УДК 342.9

Мирошниченко М. М.,
здобувач
Науково-дослідного інституту публічного права

СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ ТА ЗАХОДИ ЩОДО ЇХ МІНІМІЗАЦІЇ

CURRENT THREATS OF THE INFORMATION SECURITY OF THE STATE AND MEASURES ON THEIR MINIMIZATION

У статті проаналізовано сучасні загрози інформаційній безпеці держави. Визначено, що система загроз інформаційній безпеці державі має комплексний характер. Доведено, що найбільш ефективним методом боротьби із загрозами інформаційній безпеці держави є нейтралізація їх джерел виникнення, що забезпечить можливість повного усунення загроз.

Ключові слова: *інформаційна безпека, загрози інформаційній безпеці, мінімізація загроз, джерела загроз.*

В статье рассмотрены современные угрозы информационной безопасности государства. Определено, что система угроз информационной безопасности государству имеет комплексный характер. Доказано, что наиболее эффективным методом борьбы с угрозами информационной безопасности государства является нейтрализация их источников возникновения, что обеспечит возможность полного устранения угроз.

Ключевые слова: *информационная безопасность, угрозы информационной безопасности, минимизация угроз, источники угроз.*

The modern threats to information security are considered in the article. It was determined that the system of information security threats to the state is complex. It is proven to be the most effective method of struggle against threats to the security of the state is to neutralize their sources of origin, which will enable complete elimination of threats.

Key words: *information security, information security threats, minimization of threats, sources of threats.*

За період свого становлення та розвитку наша держава займає особливо привабливе геополітичне становище, через територію якої проходять численні торгові та транспортні шляхи. Варто погодитись, що Україна перебуває в епіцентрі як економічних, так і політичних інтересів провідних учасників міжнародних правовідносин. На сучасному етапі свого існування особливе місце серед провідних показників власного волевиявлення провідне місце займає здатність нашої держави протистояти інформаційній війні. Це явище обумовлюється масштабним значенням інформаційної сфери та її ключової ролі для всього людства. Інформаційна сфера перебуває в зоні постійного ризику, а значний посилений до неї інтерес призводить до збільшення та загострення загроз інформаційній безпеці держави. Рівень розвитку та власне безпека інформаційного середовища, які є одними з найважливіших факторів у всіх сферах державної безпеки, активно впливають на стан не тільки політичної та економічної, але й інших складових державної безпеки. Треба зазначити, що протягом усього періоду існування проблемних питань вказаної сфери як науковці, так і практики неодноразово намагалися класифікувати загрози інформаційній безпеці держави, джерела їх походження для подальшого вироблення єдиного підходу щодо мінімізації цього негативного явища. Проте однозначна думка стосовно цього питання відсутня й до сьогодні. Під час розгляду проблемних питань інформаційної безпеки держави важливим кроком є виділення саме загроз інформаційній безпеці, а також вироблення дієвого правового механізму її захисту.

Необхідно зауважити, що поняття «загроза» неодноразово згадувалося в різних доктринальних і нормативно-правових джерелах, але досі немає єдиного підходу до визначення його сутності. Наприклад, А.Б. Антонов і В.В. Балашов стверджують, що загрозою є процес настання певних змін, які можуть створити перешкоди на різних етапах реалізації їхніх інтересів [1, с. 48]. Водночас термін «загроза» в словнику С.І. Ожегова означає можливість настання небезпеки [2, с. 673]. Під загрозою також трактують невідворотність настання неприємностей чи проблем [3, с. 95]. Заслуговує на увагу наукова позиція В.П. Горбуліна та А.В. Качинського, які у своїх працях наголошують на тому, що загрозу варто розглядати як родову ознаку безпеки. За їхніми словами похідним від загрози виступає неминучість виникнення різних явищ із неконтрольованими подіями, що можуть виникнути в певний час та на певній території, наслідком яких є завдана шкода – як моральна, так і матеріальна. Окремі науковці стверджують, що загрозою є безпека на нульовому рівні [4, с. 113–114].

Варто зауважити, що законодавець на державному рівні закріпив таке поняття, як «загрози національній безпеці», роз'яснюючи, що це наявні та потенційно можливі явища й чинники, що створюють небезпеку життєво важливим національним інтересам України. Водночас Закон України «Про основи національної безпеки України» визначає загрози національним інтересам і національній безпеці України в інформаційній сфері, серед яких такі: вияви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства,

жорстокості, порнографії; комп'ютерна злочинність і комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства й держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації. Проте нормотворець обмежився лише простим перерахуванням загроз національним інтересам і національній безпеці України в інформаційній сфері, не приділяючи їм належної уваги. Також вказаний перелік загроз не є вичерпним, оскільки стрімкий розвиток інформаційних технологій перебуває у стані постійного ризику й стверджувати про конкретну кількість загроз є неможливим. Закріплення на законодавчому рівні повного переліку існуючих на сьогодні загроз інформаційній безпеці держави дасть змогу розпочати процес створення та застосування дієвого механізму щодо протидії існуючим загрозам інформаційній безпеці держави або мінімізації їх виявів.

Треба брати до уваги те, що на законодавчому рівні відсутнє правове закріплення дефініції «загрози інформаційній безпеці». Серед науковців також не вироблено єдиного загальноприйнятого підходу до тлумачення цього поняття. Але водночас більшість провідних учених вважають, що загрози інформаційній безпеці держави – це явища або процеси, через які соціальні об'єкти інформаційної безпеки частково або цілком втрачають можливість реалізувати свої інтереси в інформаційній сфері [5, с. 182–186]. Інші стверджують, що загрози інформаційній безпеці держави сприяють порушенню нормального функціонування, здійсненню руйнації або стримуванню розвитку технічних об'єктів інформаційної безпеки [6, с. 116–117].

М.В. Галамба та В.В. Петрик пропонують виділяти чотири групи інформаційних небезпек для суспільства й держави, зумовлених досягненнями науково-технічного прогресу [7, с. 133–136]. На їхній науковий погляд, перша група пов'язана з інтенсивним розвитком нового вигляду зброї – інформаційної, здатної ефективно впливати на психіку людей та інформаційну інфраструктуру держави. Друга група являє собою новий вигляд соціальних злочинів, заснований на використанні досягнень сучасних інформаційних технологій: махінації з банківськими операціями; комп'ютерне хуліганство; незаконне копіювання технологічних рішень та інше. На думку провідних дослідників, у цій сфері комп'ютер стає провідним знаряддям злочину. Третя група виявляється у вигляді електронного контролю за життям, настроєм, планами громадян, роботою політичних організацій, тотального комп'ютерного контролю за населенням країни. Інформаційні технології дають змогу накопичувати, зберігати й використовувати величезні масиви даних про здоров'я, соціальну активність, політичні думки, зв'язки, фінансові справи населення. Четверта група полягає у використанні інформаційних технологій у політичній боротьбі. Зростання впливу засобів масової інформації на хід і зміст політичних процесів, функціонування механізму влади – одна з домінуючих тенденцій сучасного суспільного розвитку.

Відтак система загроз інформаційній безпеці державі має комплексний характер і в загальному вигляді містить загрози безпеці інформації та інформаційної інфраструктури, загрози безпеці суб'єктів інформаційної сфери й соціальних зв'язків між ними від інформаційних впливів, загрози належному порядку реалізації прав та інтересів суб'єктів інформаційної сфери. Відповідно, доцільно погодитись із визначенням загроз інформаційній безпеці держави як сукупності умов і факторів, які становлять небезпеку життєво важливим інтересам держави суспільства й особи у зв'язку з можливістю негативного інформаційного впливу на свідомість і поведінку громадян, а також інформаційні ресурси та інформаційно-технічну інфраструктуру [8, с. 89]. До істотних властивостей загроз інформаційній безпеці держави при цьому належать вибірковість, передбачуваність і шкідливість [9, с. 17]. Зважаючи на динамічність суспільно-політичної обстановки та появу якісно нових небезпечних для нашої держави факторів, закріплення фіксованого переліку загроз інформаційній безпеці держави, який до того ж не має вичерпного характеру, навряд чи є доцільним. Тому пропоновані науковцями переліки зазвичай є розширеними та більш актуальними, порівняно з наведеним вище, однак і такі розгорнуті переліки загроз не можуть уважатися вичерпними та незмінними. Джерелами загроз при цьому можуть бути людина, технічні пристрої, моделі, алгоритми, програми, технологічні схеми обробки, зовнішнє середовище тощо [10, с. 67].

Чинна Стратегія національної безпеки України серед основних загроз національній безпеці, які мають безпосередній стосунок до інформаційної сфери, визначає агресивні дії Росії, що підривають суспільно-політичну стабільність із метою знищення держави Україна й захоплення її території, зокрема інформаційно-психологічну війну, приниження української мови й 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 медіакультури суспільства, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, фізична й моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [11]. Необхідно зауважити, що у Стратегії відмежовуються вияви інформаційно-психологічної війни, загрози кібербезпеці й безпеці інформаційних ресурсів від суто загроз інформаційній безпеці, що, на нашу думку, не є виправданим.

Слушними є наукові твердження науковців стосовно класифікації інформаційних загроз: економічні (система прийняття рішень, банківська інфраструктура, управління економічним станом в

умовах надзвичайних ситуацій, система управління державними комунікаціями, які мають економічний характер, корпоративні війни та промисловий шпіонаж), політичні (система державного управління, системи підготовки прийняття політичних рішень, виборчі системи, телекомунікаційні системи спеціального призначення), науково-технічні (системи накопичення ноу-хау, об'єкти інтелектуальної власності, структури фундаментальних і прикладних досліджень, структури аналізу та прогнозування тенденцій у науково-технічній сфері, бази й банки даних конфіденційного характеру), військові (інформаційні ресурси збройних сил, системи управління військами, системи постійного контролю й спостереження, канали надходження інформації стратегічного, оперативного й розвідувального характеру) та суспільні (загрози для системи формування громадської думки, системи засобів масової комунікації, структури політичних партій, громадських рухів, релігійних організацій, структури забезпечення основних прав і свобод людини) [12, с. 49–50].

Разом зі збільшенням масштабу та різновидів уже традиційних загроз процеси глобалізації також стають ключовим фактором і поштовхом до виникнення нових небезпек. В основі специфічної властивості вказаних загроз слугує характерне для глобалізації розмежування явищ і процесів, які функціонують у транскордонному просторі, відірвані від територіальної локалізації, зокрема, в умовах інформаційної війни. На думку В.П. Горбуліна [13, с. 71–73], інформаційні війни, котрі є лише елементами багатоаспектних військово-політичних протистоянь, прийнято називати інформаційними операціями. Їхніми основними методами інформаційної війни слугують блокування або перекручування інформаційних потоків і процесів прийняття рішень супротивником [14, с. 75–80].

До основних виявів інформаційної війни можна віднести й інформаційну злочинність. З огляду на сучасні тенденції до розширення мережевої архітектури організованої злочинності сьогодні відбувається формування неформальних груп хакерів у навчальних закладах і безпосередньо у віртуальному просторі [15, с. 255–257]. Також наявні відомості про залучення організованими злочинними групами хакерів до підготовки злочинів у кредитно-банківській сфері, на фондовому ринку, до протиправного заволодіння службовою інформацією. Не виключено й розроблення організованими злочинними співтовариствами планів інформаційних операцій, зокрема інформаційних диверсій. Якщо станом на 2015 рік Україна посідала 5 місце у світовому рейтингу з ризику зіткнення з веб-загрозами [16, с. 86–90], після атаки вірусу «Petya» в минулому році, від якої постраждали енергетичні компанії, банки, урядові сайти тощо, антирейтинг нашої країни в питаннях кібербезпеки відчутно зріс. За оцінками фахівців, 2017 рік загалом характеризують такі тенденції у сфері загроз інформаційній безпеці: неконтрольовані ризики, пов'язані з так званим «інтернетом речей» і поширенням мережевих з'єднань, стрімке зростання «кіберзлочинів як сервісу» – надання цифрових послуг кримінальними синдикатами, зростання правових ризиків у сфері регулювання мережевих комунікацій, хакерські атаки, спрямовані на підрив репутації брендів і політичних сил [17].

На думку Р.Р. Марутян, найсуттєвішою загрозою інформаційній безпеці держави є здійснення негативного інформаційно-психологічного впливу іноземними державами на суспільну свідомість громадян України та світову громадськість через проведення інформаційних акцій і кампаній, спеціальних інформаційних операцій. Це відбувається через систематичне поширення тенденційної, неповної або упередженої інформації про Україну та політичні процеси, що відбуваються на її теренах. Усе це впливає на зовнішню та внутрішню політику нашої держави, знижує її міжнародний імідж, має політичне та економічне підґрунтя. Метою таких інформаційних операцій є забезпечення власних національних інтересів інших держав [18, с. 465–467].

Зважаючи на численні дослідження, можна виділити такі види загроз інформаційній безпеці: загрози інформаційним правам і свободам особистості, загрози несанкціонованого доступу третіх осіб до інформації, загрози впливу недостовірної чи фальшивої інформації на особистість, суспільство, державу, технічні несправності під час роботи з обладнанням [19, с. 46–48].

Вітчизняні науковці загрози інформаційній безпеці держави схильні класифікувати за своєю загальною спрямованістю: загрози конституційним правам і свободам людини й громадянина в інформаційній сфері, загрози інформаційному забезпеченню державної політики, загрози розвитку вітчизняної індустрії інформації, загрози безпеці інформаційно-телекомунікаційних систем [20, с. 12–13]. Водночас до загроз інформаційній державній політиці можемо віднести такі: надмірне втручання держави в інформаційні процеси, низька якість інформаційних продуктів, що виробляються, застарілість методів регулювання інформаційного ринку, проблеми кадрового забезпечення. До факторів, що заважають розвитку та поширенню вітчизняних інформаційних продуктів, можемо віднести такі: недовіра до вітчизняної інформаційно-технічної продукції з боку органів державної влади та приватних суб'єктів, блокування діяльності українських виробників у світовому інформаційному просторі, протидія доступу України до нових інформаційних ринків, відсутність стимулювання та налагодження нових виробничих потужностей в інформаційній сфері, втрата цінних кадрів.

Актуальними та невирішеними проблемами сьогодні залишаються питання, які стосуються оцінки стану інформаційної безпеки держави. Сутність такої оцінки стану інформаційної безпеки держави розкривається через логічно структурований підхід на основі аналізу сучасного стану вітчизняного інформаційного простору. Результатом вказаного процесу є прогнозування ймовірних внутрішніх і зовнішніх загроз інформаційній безпеці. Отже, варто зауважити, що більшість науковців висловлюють свої наукові обґрунтування стосовно оцінки

сучасного рівня інформаційної безпеки, який можна оцінити за такими критеріями: ступінь охорони конфіденційної інформації, можливість протистояння негативним інформаційним «хвилям», професійна діяльність державних органів у сфері забезпечення інформаційної безпеки, право вільного доступу громадянина до правової інформації [21, с. 135–147].

Дотепер у науковому соціумі дискусійними залишаються питання виокремлення джерел загроз інформаційній безпеці. Зазвичай виділяють внутрішні та зовнішні [22, с. 211]. До внутрішніх загроз інформаційній безпеці держави відносять такі: відсутність правової традиції в державі, значний вплив організованої злочинності, відсутність налагодженої системи управління в державі, складна економічна ситуація, економічна неосвіченість населення. До зовнішніх джерел загроз інформаційній безпеці держави відносять такі: наявність комплексного впливу на державу, її інститути та суспільство з боку інших держав чи впливових зарубіжних структур, «конкуренція» в інформаційному просторі з іншими державами, діяльність міжнародних кримінальних структур, інформаційна експансія щодо держави чи її окремих територіальних утворень.

Як протидія масштабним негативним інформаційно-психологічним впливам, операціям і війнам пріоритетними напрямами державної інформаційної політики та важливими кроками з боку владних органів України мають бути такі: інтеграція України у світовий та регіональний європейський інформаційний простір, інтеграція в міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації, створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства, модернізація всієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики, вдосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів, розвиток національної інформаційної інфраструктури, підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг, впровадження сучасних інформаційно-комунікативних технологій у процеси державного управління, ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригування державної політики в інформаційній сфері.

З метою недопущення інформаційної експансії діяльність держави в інформаційному просторі має здійснюватися за такими напрямами: реалізація упереджувальної стратегії й тактики (превентивні заходи), здійснення реагувальної стратегії (оперативне реагування на інформаційні атаки супротивника та активний наступ), захист національного інформаційного простору. Основна мета – забезпечення переваги в інформаційному просторі. Крім того, пріоритетними завданнями інформаційних структур владних органів мають бути такі: контроль за інформаційними потоками, надання об'єктивної, вичерпної інформації, представлення фахових коментарів і пояснень щодо подій, систематичне висвітлення офіційної позиції посадових осіб і політичних лідерів.

Варто зазначити, що з метою захисту національного інформаційного простору, створення ефективної системи забезпечення інформаційної безпеки з боку української влади здійснюються певні заходи. Зокрема, 2015 року КМУ ухвалив Постанову, згідно з якою створено Міністерство інформаційної політики України, пріоритетними завданнями якого є протидія інформаційній агресії з боку РФ, розроблення ефективної стратегії інформаційної політики держави та Концепції інформаційної безпеки України, узгодженість і координація функціонування та діяльності органів державної влади й інформаційної сфери. З метою протидії негативним впливам інформаційної пропаганди та інформаційних війн, задля нейтралізації та упередження реальних і потенційних загроз в інформаційному просторі України Рада національної безпеки й оборони України ухвалила Рішення «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». У документі зазначено, що РНБО, зважаючи на необхідність вдосконалення нормативно-правового забезпечення та запобігання й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, вирішила: розробити та внести на розгляд ВРУ законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу, зокрема забороною ретрансляції телевізійних каналів; посилити контроль за додержанням законодавства з питань інформаційно-психологічної та кібернетичної безпеки; ужити заходів щодо забезпечення поширення у світі об'єктивних відомостей про суспільно-політичну ситуацію в Україні, зокрема, через створення відповідного медіахолдингу для підготовки якісного конкурентоздатного інформаційного продукту; розробити порядок аналізу інформаційних матеріалів іноземних засобів масової інформації, що мають представництва в Україні, з метою впровадження дієвого механізму акредитації журналістів; ужити заходів до активізації міжнародного співробітництва з питань протидії негативним інформаційно-психологічним впливам і кібернетичній злочинності. Крім вищезазначеного документа, основні напрями державної політики з питань національної безпеки в інформаційній сфері визначені в законах України «Про основи національної безпеки України», «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», у «Доктрині національної безпеки» та в інших нормативно-правових документах. Отже, в умовах сучасних інформаційних протистоянь, експансіоністської політики Російської Федерації національний інформаційний простір України є недостатньо захищеним від зовнішніх негативних пропагандистських інформаційно-психологічних впливів і загроз. Тому захист інформаційного суверенітету, створення потужної та ефективної системи інформаційної безпеки України, розроблення дієвих стратегій і тактик протидії медіа-загрозам повинні стати пріоритетними

завданнями органів державної влади та недержавних інститутів. Актуальність досліджуваної проблематики – незаперечна й потребує поглибленого вивчення.

Отже, для нейтралізації та мінімізації внутрішніх загроз потрібно вжити таких заходів: організаційні заходи із захисту інформації (комплекс адміністративних та обмежувальних заходів), контрольно-правові заходи (контроль за виконанням персоналом вимог відповідних інструкцій, розпоряджень, наказів, нормативних документів), профілактичні заходи (спрямовані на формування в персоналу мотивів поведінки, які спонукають їх до безумовного виконання в повному обсязі вимог режиму, правил проведення робіт, а також на формування відповідного морально-етичного стану в колективі), інженерно-технічні заходи, робота з кадрами (підбір персоналу, інструктажі, навчання персоналу з питань забезпечення захисту інформації, виховання пильності співробітників, підвищення їхньої кваліфікації), психологічні заходи (встановлення відеоспостереження, оприлюднення інцидентів із спробою винесення забороненої інформації за межі організації).

Інформаційна безпека є комплексним, глибоко структурованим явищем, на стан якого постійно здійснює вплив велика кількість факторів внутрішнього та зовнішнього походження, а також геополітичні тенденції у світі. Загрози інформаційній безпеці переважно пов'язані із ситуацією в економіці чи політиці. Також загрози можуть бути пов'язані з бажанням окремих осіб чи груп населення до розпалювання внутрішньодержавної ворожнечі, конфліктами між правоохоронною системою та впливовими суб'єктами (наприклад, олігархами та підконтрольними їм структурами). Останні за допомогою підконтрольних ЗМІ можуть займатися створенням «образу ворога», «зомбуванням» населення з метою управління свідомістю населення. Саме через такі дії виявляються реальні можливості інформаційної сфери та її здатність «проникнення» до багатьох сфер життєдіяльності суспільства. На жаль, у нашій державі з боку представників як законодавчої, так і виконавчої влади ще недостатньо усвідомлюються можливості «маніпулювання» суспільною свідомістю. Іноді такі можливості активно використовують на більш високому рівні впливові держави чи міжнародні структури, наприклад, для ведення гібридної війни, за допомогою якої може здійснюватися значний вплив на свідомість населення, його інформаційні ресурси, інформаційну інфраструктуру та, як результат, на поведінку суспільства шляхом коригування його системи цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності.

ЛІТЕРАТУРА:

1. Антонов А.Б. Основы обеспечения безопасности личности, общества и государства: учеб. пособие. М.: Институт защиты предпринимателя, 1996. № 5. С. 36–55.
2. Ожегов С.И. Словарь русского языка. М., 1988. 748 с.
3. Словник української мови: в 11 т. / АН УРСР, Ін-т мовознавства ім. О.О. Потебні; редкол.: І.К. Білодід та ін. К: Наукова думка, 1972. Т. 3. ред.: Г.М. Гнатюк, Т.К. Черторизька. 1972. 744 с.
4. Горбулін В.П., Качинський А.Б. Засади національної безпеки України. К.: Інтер-технологія, 2009. 272 с.
5. Ткачук Т.Ю. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. Підприємництво, господарство і право. 2017. № 10. С. 182–186.
6. Гуцалюк М.В. Організація захисту інформації: навч. посібник. К.: Альтерпрес, 2012. 224 с.
7. Галамба М.,В. Петрик В.В. Інформаційна безпека України: поняття, сутність та загрози. Юридичний журнал «Юстиніан». 2006. № 6. С. 133–136.
8. Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. Інформаційна безпека (соціально-правові аспекти) / За ред. Є.Д. Скулиша К.: КНТ, 2010. 776 с.
9. Дереко В.Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 2 (18). С. 16–22.
10. Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. Сучасний захист інформації. 2016. № 4. С. 65–70.
11. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про національну безпеку України»: Указ Президента України. URL: www.president.gov.ua/ documents/2872015-190.
12. Соснін О.В. Виклики і загрози при впровадженні відкритих інформаційно-комунікаційних науково-освітніх систем та технологій. Гуманітарний вісник. 2016. № 67. С. 49–58.
13. Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. К.: Інтертехнологія, 2009. 164 с.
14. Сопілко І.М. Інформаційні загрози та безпека сучасного українського суспільства. Юридичний вісник. 2015. № 1 (34). С. 75-80.
15. Юрченко И.А. Понятие и виды информационных преступлений. Российское право в Интернете. 2003. № 1. С. 255–257.
16. Платоненко А.В. Сучасні загрози інформаційної безпеки для державних та приватних установ України. Сучасний захист інформації. 2015. № 4. С. 86–90.
17. Thor Olavsrud. 4 information security threats that will dominate 2017. URL: https://cio.com/article/3153706/security/4-information-security-threats-thatwill-dominate-2017.html.
18. Марутян Р.Р. Безпека як цінність та потреба. Науковий вісник Гілея. 2013. № 75. С. 465–467.
19. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. Вісник Київського університету ім. Т. Шевченка. 1999. Вип. 14. С. 46–48.
20. Гуцалюк М.В. Інформаційна безпека України: нові загрози. Бизнес и безопасность. 2003. № 5. С. 12–13.
21. Лисенко В.В. Проблеми інформаційної незалежності держави. Політичний менеджмент. 2006. № 4. С. 135–147.
22. Інформаційна безпека суспільства і держави. Стратегічні цілі і задачі інформаційної боротьби. URL: http://www.ngo.dn.ua/doc/concept.doc.