К. Захаренко,
кандидат філософських наук,
здобувач НПУ імені М.П.Драгоманова

ЕФЕКТИВНІСТЬ ВИКОРИСТАННЯ ПОТЕНЦІАЛУ НЕДЕРЖАВНИХ СУБ'ЄКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Протидія зовнішнім і внутрішнім загрозам у сфері національної безпеки загалом та інформаційної, зокрема, неможлива без залучення недержавних суб'єктів інформаційної безпеки: громадських організацій, громадських рухів, недержавних аналітичних і наукових центрів, різноманітних об'єднань громадян − політичних, економічних, волонтерських, правозахисних, мережевих, культурно-просвітницьких тощо. Як засвідчили «Революція гідності», а також розвиток подій після неї, в Україні є нагальна необхідність інституціалізації та нового правового забезпечення діяльності громадського сектору, який виявився локомотивом суспільних змін і одним із суб'єктів у сфері національної безпеки, зокрема, інформаційної.

У науковому світі питаннями ефективності використання потенціалу недержавних суб'єктів інформаційної безпеки займалися: Ю.Бурило, Л.Борисова, В.Дем'янчук, В.Григор'єв, В.Крутов, Я.Лантінов, О.Дзьобань, М.Горєлов, О.Юдін, С.Каштелян та ін.

Фактично весь недержавний сектор, який містить об'єднання, асоціації і громадські організації, залишається поза єдиною політикою в сфері забезпечення національної безпеки [1, 162].

Дослідники В.Крутов та Г.Новицький зазначають, що аналіз законодавства і практики забезпечення національної безпеки свідчить, що в інституціональній структурі суб'єктів забезпечення національної безпеки повинне бути чітко визначене місце недержавного сектору безпеки. Забезпечення національної безпеки здійснюється не в державі взагалі, не в абстрактному просторі, а в конкретному місці. Воно безпосередньо пов'язане з безпекою конкретних людей [2, 166]. Екстраполюючи ці висновки на проблему забезпечення інформаційної безпеки держави, суспільства та людини, підкреслимо, що саме у співпраці державних та недержавних суб'єктів можливо досягти максимального результату щодо захисту вітчизняного інформаційно-культурного простору.

На думку Ю.Лісовської, включення інститутів громадянського

суспільства у систему захисту інформаційної безпеки забезпечує вирішення багатьох важливих завдань. По-перше, забезпечується участь громадськості у прийнятті рішень з питань інформаційної безпеки. По-друге, введення інститутів громадянського суспільства у механізм політики інформаційної безпеки забезпечує процес залучення громадян до розв'язання проблем інформаційної безпеки, їхню активну позицію з відповідних питань [3, 110].

Аналіз нормативно-правової бази, яка регламентує участь недержавних суб'єктів як структурних елементів системи забезпечення інформаційної безпеки, дає підстави виокремити такі її основні форми:

• участь у роботі консультативно-дорадчих органів при органах державного управління в інформаційній сфері;

• участь у публічних громадських обговореннях, що проводяться органами державного управління в інформаційній сфері;

• вивчення громадської думки, що проводиться органами державного управління в інформаційній сфері;

• направлення органам державного управління в інформаційній сфері інформаційних запитів та скарг, що надходять під час громадського контролю за їх діяльністю, а також скарг та заяв про інформаційні правопорушення в процесі громадського контролю за дотриманням законності в інформаційній сфері;

• направлення органам державного управління в інформаційній сфері заяв (клопотань) про задоволення прав та законних інтересів у цій сфері [4, 34].

Важливим недержавним суб'єктом інформаційної безпеки країни є неурядові аналітичні центри. Роль неурядових аналітичних центрів як генераторів нових ідей та альтернативних підходів є особливо важливою на перехідних етапах, коли відбуваються глибокі внутрішні трансформації в усіх сферах суспільного життя, у сфері інформаційної безпеки зокрема. Неурядові аналітичні центри є також інструментом громадського контролю, вони впливають і на визначення цілей та цінностей суспільства, формують суспільну думку, яка є основним об'єктом інформаційних атак з боку інших держав. Їх потенціал як посередників та ефективного каналу зв'язку між інтелектуальним середовищем і державними органами та суспільством важко переоцінити. Неурядові аналітичні центри − це важливий інструмент громадського контролю за діями влади. Їхня роль важлива і у визначенні цілей та цінностей суспільства, у формуванні

громадської думки з актуальних для країни питань. Як правило, неурядові аналітичні центри існують у медіа-просторі країни: їх спеціалісти виступають у ЗМІ, фахівці аналітичних центрів надають коментарі з суспільно важливих питань, попереджають про загрози у сфері національної безпеки, інформаційної зокрема.

Демократичні країни демонструють співпрацю державних та недержавних суб'єктів інформаційної безпеки, що знайшло своє відображення і на законодавчому рівні. Наприклад, 26 листопада 2003 р. Конгресом США ухвалено закон «Про внутрішню безпеку» (Home Security Act), відповідно до якого створено Міністерство внутрішньої безпеки (Department of Homeland Security), на яке покладено координацію діяльності державних органів і всіх приватних структур з питань забезпечення інформаційної безпеки. Цим законом передбачено розробку Національної стратегії із забезпечення безпеки у кіберпросторі (National Strategy to Secure Cyberspace) та Національної стратегії фізичного захисту об'єктів життєзабезпечення населення (The National Strategy for the Physical Protection of Critical Infrastructures). Цими документами передбачено створення єдиної національної системи протидії кібернетичному тероризму, в межах якої ініційовано створення територіальних, відомчих і приватних центрів протидії, визначено їхні функції та порядок взаємодії [5, 93–94].

У свою чергу, в лютому 2011 р. уряд Нідерландів ухвалив Національну стратегію кібербезпеки «Сила через співпрацю», якою передбачено створення Національної ради з кібербезпеки. Завданням цього органу є забезпечення співробітництва державного та приватного секторів, а також різних наукових центрів. Передбачено також створення Національного центру з питань кібербезпеки, завданням якого є виявлення тенденцій та загроз інформаційній безпеці, а також сприяння подоланню наслідків інцидентів і кризових ситуацій у цій сфері [6, 30–31].

Водночас, як зауважує К.Павлюк, існує загроза поширення проявів впливу неурядових громадських організацій на стан національної безпеки (інформаційної, зокрема) через дестабілізацію внутрішньополітичної ситуації. Напрями такого впливу мають переважно політичне забарвлення. Зокрема, впродовж 2006–2007 рр. об'єднання «Народний фронт «Севастополь–Крим–Росія» проводило публічну агітацію і поширювало матеріали із закликами до дій з метою зміни кордонів території та державного кордону України,

конституційного ладу України, зокрема, шляхом реалізації так званого силового сценарію возз'єднання Криму з Росією. А 18 жовтня 2007 р. на горі Говерла «Євразійський союз молоді» вчинив акт антиукраїнської спрямованості по знищенню тризуба [7, 213].

Можна констатувати, що в інформаційній війні, яка здійснювалась і здійснюється проти України, використовуються не тільки різноманітні ЗМІ, а й неурядові організації, які створюють інформаційні приводи для такої руйнівної діяльності, підривають основи національної державності. Саме тому не всі неурядові організації можна вважати потенційними суб'єктами інформаційної безпеки.

Міжнародний досвід свідчить, що активізація екстремістських неурядових громадських організацій відбувається під час важливих для країни подій (проведення виборчих кампаній, референдумів, міжнародних заходів тощо) у формі різноманітних публічних акцій (пікетів, мітингів тощо), поширення антидержавної інформаційної продукції. Так, у перший день парламентських виборів в Індії (16 квітня 2009 р.) екстремісти маоїстських організацій у штаті Джаркханд убили дев'ять осіб, у тому числі семеро солдатів, які охороняли дільниці для голосування [8].

У демократичних країнах держава створює правові, організаційні та економічні умови для розвитку недержавних суб'єктів інформаційної безпеки, сприяє їх всебічній співпраці з державними структурами у даній сфері. Крім того, державні інститути покликані забезпечити гідну життєдіяльність усіх об'єктів інформаційної безпеки – від громадян до власне держави. Відтак уся система інформаційної безпеки має бути спрямована на захист життєво важливих інтересів особистості, різних колективів, нації, суспільства та держави. На думку Л. Борисової та В. Тулупова, в інформаційній сфері України вирізняються такі стрижневі інтереси **особистості:** забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; недопущення несанкціонованого втручання у зміст, процеси оброблення, передання та використання персональних даних; захищеність від негативного інформаційно-психологічного впливу [9, 41].

Отже, система інформаційної безпеки повинна бути спрямована на захист таких інтересів особистості та сприяти нейтралізації можливих ризиків для неї, які можна класифікувати за критеріями:

1) за ступенем універсальності − загальні й специфічні;

2) за часом дії − постійні, довгострокові, короткострокові;

3) за територіальною поширеністю − глобальні, регіональні, національні (у межах певних національних кордонів), місцеві;

4) за способом дії − відкриті й приховані:

5) за джерелами виникнення − природні (природна стихія), штучні (результат людської діяльності), змішані (людська діяльність, що сприяє виникненню стихійного лиха);

6) за характером виникнення: навмисні та ненавмисні (як закономірний або непередбачений побічний результат певних дій або явищ);

7) за характером дії − такі, що проявляються поступово або раптово; такі, що спричиняють прямий (безпосередній) або побічний збиток;

8) за ступенем небезпеки − з наслідками переборними, непереборними або переборними частково;

9) за можливістю запобігання − загрози, яким можна запобігти цілком, частково і неможливо запобігти зовсім [10, 138–140].

Об'єктом інформаційної безпеки є також різноманітні колективи. Зазначимо, в законодавстві України колективи не розглядаються як об'єкти інформаційної безпеки. Це є певним недоліком. Саме в трудових, учнівських, студентських та інших колективах відбуваються процеси становлення та розвитку суспільної та національної свідомості. Тому системна робота всіх суб'єктів інформаційної безпеки з різноманітними колективами є одним із стратегічних завдань, реалізація якого потребує розроблення та впровадження відповідних програм на рівні держави, області, району, міста тощо.

Дехто з науковців наголошує на необхідності залучення колективів до системи суб'єкт-об'єктних відносин національної та інформаційної безпеки. Так, В.Українчук сутність національної безпеки (інформаційної, зокрема), розуміє як такий специфічний вид суспільних відносин, які складаються між людьми і їхніми колективами у процесі цілеспрямованої діяльності, результатом якої є досягнення стану оптимального функціонування і розвитку громадянського суспільства, правової держави та їх структурних компонентів [11, 14].

З нашого погляду, саме у колективах утверджуються політичні, правові, національні та духовні цінності, реалізація яких становить підґрунтя інформаційної безпеки. Вочевидь, колективи є полем обговорення інформаційних повідомлень, від характеру інтерпретації яких залежить рівень розвитку суспільної свідомості.

У науковій літературі набуло поширення таке поняття, як «культура безпеки» (яке вбирає в себе й інформаційну безпеку). Визначається

воно як рівень розвитку людини і суспільства, характеризується значущістю забезпечення безпеки життєдіяльності в системі особистісних і соціальних цінностей, безпечної поведінки в повсякденному житті і в умовах надзвичайних ситуацій, рівнем захищеності від загроз і небезпек в усіх сферах життєдіяльності. Культура безпеки має складові, які проявляються на певних рівнях, в тому числі й на рівні колективів. До вищеозначених рівнів культури безпеки та її складових належать такі:

- на індивідуальному рівні – це світогляд, норми поведінки, індивідуальні цінності і підготовленість людини у сфері безпеки життєдіяльності;
- на колективному рівні – корпоративні цінності, професійна етика та мораль, підготовленість персоналу у сфері безпеки;
- на суспільному рівні – традиції безпечної поведінки, суспільні цінності, підготовленість всього населення у сфері безпеки життєдіяльності [12, 42].

Таким чином, на рівні колективних об'єктів важливо формувати культуру інформаційної безпеки як ефективного засобу протистояння різноманітним інформаційним загрозам, що, у свою чергу, зміцнюватиме загальносуспільну інформаційну безпеку.

Аналізуючи сутність суспільства як об'єкта інформаційної безпеки, згадаємо тезу К. Поппера у праці «Відкрите суспільство та його вороги» − все, що заперечує існування системи, є небезпекою, і навпаки, система, існуванню якої не загрожує заперечення, перебуває у безпеці [13]. Отже, будь-яке суспільство повинно захищати всі сфери життєдіяльності, інформаційну зокрема.

Основними завданнями у забезпеченні інформаційної безпеки суспільства є захист інформаційно-культурного простору, протистояння зовнішнім руйнівним впливам, нівелювання загроз в інформаційних війнах. У нових геополітичних реаліях ці останні мають перманентний характер. Особливо вразливими в інформаційній сфері є суспільства, які перебувають на стадії системних трансформацій, українське суспільство зокрема.

Як зауважує О. Дзьобань, методи комунікативних технологій в умовах ведення «інформаційної війни» поширюються на всі сфери життя суспільства, провокуючи в транзитивній соціальній реальності нові явища: інформаційну релігійну експансію, переписування сторінок історії, свідоме перекручування норм національних мов у бік їх збідніння, введення ненормативної лексики тощо. Загроза поширення

псевдокультурних знань і цінностей сприяє створенню фіктивного людського і соціального капіталу, що не піддається кількісному виміру, але може зіграти «доленосну» роль у розвитку (деградації) суспільства. Він виявляється в низькому професіоналізмі, зниженні значущості моральних норм, створенні культу помилкових (хибних) цінностей тощо [14, 251].

У зв'язку з комерціалізацією ЗМІ (що природно для ринкової економіки) з телеекранів на особистість і суспільство обрушився потік реклами, фільмів і передач, що пропагують насильство, садизм, секс. Усе це можна класифікувати як несанкціонований доступ до свідомості. Наслідком панування принципу «рекламної паузи» на телебаченні є вплив на психіку мільйонів людей.

З метою запобігання та нейтралізації загроз інформаційній безпеці суспільства застосовуються базові методи – правові, програмно-технічні та організаційно-економічні. Правові методи передбачають розробку комплексу нормативно-правових актів та положень, що регламентують інформаційні відносини в суспільстві, керівні і нормативно-методичні документи щодо забезпечення інформаційної безпеки. Програмно-технічні методи сприяють наповненню національного інформаційного простору новітніми технологіями, що здатні істотно підвищити як адекватність відображення реальності, так і продуктивність інформаційної діяльності в суспільстві, що, у свою чергу, визначає можливості захисту національних інтересів. Застосування організаційно-економічних методів зумовлене тим, що інформаційні технології привносять в соціально-економічні процеси революційну, але, на думку деяких дослідників, не завжди безпечну хвилю, тому безпека інформаційної революції для суспільства може бути гарантована коректним управлінням інформаційними процесами [15, 54–55].

Досліджуючи сутність суб'єкт-об'єктних відносин у системі інформаційної безпеки, не можна ігнорувати її етнонаціональний вимір, а саме –базові характеристики нації та народу. Розглядаючи націю як об'єкт інформаційної безпеки, ми розуміємо її як політичну спільноту, що мешкає на певній території, має власну мову, культуру та створила (або прагне створити) державу.

Необхідно розрізняти поняття «національна безпека» та «безпека нації». Я.Лантінов вважає, що доцільно розрізняти «національну безпеку» у широкому та у вузькому розумінні. Національна безпека у широкому розумінні – це система «безпек» як усіх складових

нації України (ієрархічне поєднання безпеки держави, безпеки недержавних об'єднань (громад) та безпеки фізичних осіб), так і поєднання усіх інших аспектів безпеки (безпеки військово-політичної, економічної, енергетичної, екологічної, інформаційної тощо). Є підстави вважати, що національна безпека у широкому розумінні збігається з суспільною безпекою (не плутати з громадською безпекою). Національна безпека у вузькому розумінні – це вищий, найзагальніший рівень безпеки, який не може бути зведений до жодного з окремих аспектів. Змістом національної безпеки у вузькому розумінні є забезпечення «життя» націй України, її самобутньої життєдіяльності [16, 572].

Послуговуючись визначенням національної безпеки у вузькому значенні, зазначимо, що самобутність будь-якої нації проявляється, насамперед, в її культурі, мові, традиціях, здатності сформулювати й реалізувати національну ідею. Тому інформаційна безпека нації полягає у захисті неповторних національно-культурних цінностей, історичних традицій, історичної пам'яті тощо.

Якщо культура певної нації в усталені періоди суспільного буття була єдиним впорядкованим, ієрархізованим цілим, то в перехідних умовах культура характеризується певною мозаїчністю, яка, з одного боку, полегшує можливість нав'язувати широким верствам населення певні думки й поняття, а з іншого, − сприяє формуванню знань не через освіту, а засобами масової інформації. В результаті культурне поле соціуму стає небезпечно вразливим, соціальна комунікація втрачає таку важливу рису, як взаємопов'язаність, національно-культурна ідентичність нівелюється. Культурна безпека є надзвичайно чутливою до загроз, особливо зовнішніх. Глобальні інформаційні й комунікаційні технології створюють умови для формування нового інформаційного простору, що охоплює весь світ. Поряд з позитивним ефектом це створює ризики для культурної безпеки України, формуються передумови уніфікації культури, суспільної думки, ціннісних орієнтацій, політичної поведінки, запозичення окремих рис сторонніх культур. Системи цінностей традиційних спільнот руйнуються під дією ризиків, які створюються сучасними засобами масової інформації в умовах соціокультурного транзиту [17, 248–249].

Інформаційна політика держави повинна враховувати вищеозначені ризики, зменшувати їх негативний вплив шляхом сприяння відтворенню у суспільстві національно-культурних норм та цінностей усіма можливими засобами.

Українська політична нація є поліетнічною, до її складу входить багато народів (етнонаціональних спільнот). Саме тому розглянемо народ як об'єкт інформаційної безпеки. Етнічна структура українського суспільства характеризується, з одного боку, беззаперечним кількісним переважанням корінного автохтонного українського етносу, з іншого − багатющою палітрою національних меншин і етнічних груп, які репрезентують основні мовні сім'ї світу. При цьому розмаїта етнічна палітра не лише збагачує українське суспільство, а й висуває до кожної зі сторін (відповідно − до корінного етносу та меншин) взаємні зобов'язання щодо налагодження оптимальних умов для гармонізації міжетнічних відносин [17, 489]. Отже, заходи з інформаційної безпеки щодо окремих народів та етнонаціональних груп, які мешкають на теренах України, повинні базуватися на таких принципах, як плюралізм, толерантність, віротерпимість, гуманізм. Водночас держава повинна дбати про захист етнонаціональних утворень від зовнішніх інформаційних загроз, суб'єкти яких можуть використовувати етнічно-культурні, релігійні та мовні відмінності певних народів для дестабілізації ситуації в поліетнічній країні.

З нашої точки зору, інформаційна безпека та інформаційна політика нашої держави в етнонаціональній площині повинна базуватися на інтегральній світоглядній основі, якою є українська національна ідея. Як вважає О.Ляшенко, українська національна ідея повинна стати політичним проектом майбутньої нації, смисложиттєвим чинником національного розвитку. Національну ідею слід вважати ідеєю нації як спільноти з наступними характеристиками:

1) поліетнічна, консолідована інститутом громадянства приналежність до України як спільної Батьківщини;

2) свідома своєї політичної мети − побудови незалежної, економічно міцної та соціальної, демократичної, правової держави;

3) об'єднана спільністю історичної долі, мовою, культурними традиціями, толерантністю корінного українського етносу щодо численних етнічних груп [18, 96–97].

Будь-яка нація прагне створити (створила) державу як інститут, що повинен забезпечувати її розвиток та історичний поступ. Адже держава є одним із системоутворювальних об'єктів інформаційної безпеки. У широкому розумінні інформаційна безпека держави − це захист вітчизняного інформаційно-культурного поля та національних інформаційних ресурсів. Інформаційна безпека національних

ресурсів, складовим елементом якої є державні інформаційні ресурси, забезпечується їх власниками (для державних інформаційних ресурсів власником є державні органи управління) шляхом створення комплексної системи захисту інформації щодо несанкціонованого доступу та дотримання належного рівня їх захисту [29, 300].

Державна політика з питань захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах спрямована на:

• захист державних інформаційних ресурсів;
• створення єдиної системи антивірусного захисту інформації;
• взаємодію з органами державної влади;
• взаємодію з адміністрацією домену .ua;
• міжнародне співробітництво в галузі інформаційних ресурсів;
• визначення рівня захищеності інформаційно-телекомунікаційних систем органів державної влади [20].

Узагальнюючи різноманітні підходи щодо захисту держави як об'єкта інформаційної безпеки, можна виокремити параметри цього феномену:

− кількість і види реально існуючих джерел загроз;
− ймовірність реалізації кожної із загроз і нападу в цілому;
− розмір збитку, що завдається в результаті реалізації кожної загрози;
– ступінь стійкості об'єкта безпеки до деструктивних впливів (імунітет);
– здатність об'єкта уникати нападу (реалізації загроз);
− ступінь надійності системи захисту;
− здатність об'єкта безпеки до самовідновлювання і розміри витрат, необхідні для ліквідації наслідків нападу [21, 20].

Отже, ефективна інформаційна безпека є запорукою захисту національного інформаційного простору та національних інтересів будь-якої країни.

ЛІТЕРАТУРА

1. *Крутов В.* Щодо правового статусу структур недержавного сектору національної безпеки України // Проблеми боротьби зі злочинністю. – 2009. – №2 (57). – С. 161–168.
2. *Крутов В.* Щодо правового статусу структур недержавного сектору національної безпеки України // Проблеми боротьби зі злочинністю. – 2009. – №2 (57). – С. 161–168.

3. *Лісовська Ю.П.* Адміністративно-правова діяльність недержавних органів та організацій як структурних елементів системи забезпечення інформаційної безпеки // Наукові праці МАУП. – 2014. – Вип. 2 (41). – С.108–113.
4. *Бурило Ю.П.* Участь недержавних суб'єктів у здійсненні державного управління інформаційною сферою // Правова інформатика. – 2007. – № 4. – С.31–41.
5. *Алямкін Р.В.* Правове забезпечення національної інформаційної безпеки // Наукові записки Інституту законодавства Верховної Ради України. – 2013. – № 4. – С.91–96.
6. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/65/201) // Нью-Йорк, 2012, Организация Объединенных Наций. – 57 с.
7. *Павлюк К.* Діяльність неурядових громадських організацій у контексті забезпечення національної безпеки України // Вісник Національної академії державного управління при Президентові України. – 2012. – № 2. – С.210–218.
8. *Горєлов Д.* Аналітична записка відділу стратегій розвитку громадянського суспільства та протидії корупції. – Режим доступу : http://human-rights.unian.net/ukr/detail/187585
9. *Борисова Л.В.* Інформаційна безпека як визначальний компонент національної безпеки України // Право і безпека. – 2013. – № 1 (48). – С.39–42.
10. *Биктимирова З.З.* Безопасность в концепции развития человека // Общественные науки и современность. – 2002. – № 6. – С.135–142.
11. *Українчук В.М.* Забезпечення національної безпеки в умовах формування в Україні громадянського суспільства. – Харків: Ун-т внутр. справ. – 1996. – 164 с.
12. *Дем'янчук В.А.* Культура безпеки людини – безпека суспільства в XXI столітті // Оновлення змісту, форм та методів навчання і виховання в закладах освіти. – Наукові записки Рівненського державного гуманітарного університету. Випуск 8 (51). – Рівне, 2014. – С.42–46.
13. *Поппер К.Р.* Открытое общество и его враги. Т. 1: Чары Платона. – М., 1992. – 448 с.
14. *Дзьобань О.П.* Національна безпека України: концептуальні засади та світоглядний сенс. – Харків, 2007. – 284 с.
15. *Григор'єв В.І.* Інформаційна безпека у державному управлінні // Бібліотекознавство. Документознавство. Інформологія. – 2013. – № 4. – С.53–55.
16. *Лантінов Я.О.* Щодо визначення національної безпеки України як об'єкта кримінально-правової охорони // Форум права. – 2011. – № 1. – С.570–574.
17. *Горєлов М.Є.* Цивілізаційна історія України // М.Є.Горєлов, О.П.Моця, О.О.Рафальський. – К., – 2005. – 632 с.
18. Правосвідомість і правова культура як базові чинники державотвор-

чого процесу в Україні. – Харків, 2009. – 352 с.
19. *Юдін О.К.* Концептуальний аналіз уразливості державних інформаційних ресурсів // Наукоємні технології. – 2013. – № 3 (19). – С.299–304.
20. Біла книга Держспецзв'язку. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=49942&cat_id=49941
21. *Каштелян С.О.* Сутність та зміст поняття «безпека» у контексті забезпечення національної безпеки України у прикордонній сфері // Честь і закон. – 2013. – № 1 (44). – С.17–21.

Захаренко К. Ефективність використання потенціалу недержавних суб'єктів інформаційної безпеки.

Максимальний результат щодо захисту вітчизняного інформаційно-культурного простору забезпечується співпрацею його державних і недержавних суб'єктів. Демократичні країни мають значний досвід використання потенціалу недержавних суб'єктів інформаційної безпеки різних громадських об'єднань, асоціацій та організацій. Так само, як і державні інститути, ці суб'єкти є генераторами нових ідей та альтернативних підходів у сфері інформаційної безпеки. Неурядові організації є інструментами громадського контролю, знаряддями впливу на визначення цілей і цінностей суспільства, засобами формування суспільної думки. Але не всі неурядові організації можна вважати потенційними суб'єктами інформаційної безпеки. Адже навіть ті серед них, які діють легально, іноді використовуються в інформаційній війні проти України. Саме тому держава має створювати правові, організаційні та економічні умови для розвитку недержавних суб'єктів інформаційної безпеки, а також сприяти їх усебічній співпраці з різними державними структурами.

Ключові слова: інформаційна безпека, культура безпеки, суб'єкт інформаційної безпеки.

Захаренко К.Эффективность использования потенциала негосударственных субъектов информационной безопасности.

Максимальный результат по защите отечественного информационно-культурного пространства обеспечивается сотрудничеством его государственных и негосударственных субъектов. Демократические страны имеют значительный опыт использования потенциала негосударственных субъектов информационной безопасности различных общественных объединений, ассоциаций и организаций. Так же, как и государственные институты, они являются генераторами новых идей и альтернативных подходов в сфере информационной безопасности. Неправительственные организации являются инструментами общественного контроля, орудиями влияния на определение целей и ценностей общества, средствами формирования общественного мнения. Но не все неправительственные органи-

зации можно считать потенциальными субъектами информационной безопасности. Даже те из них, которые действуют легально, иногда используются в информационной войне против Украины. Именно поэтому государство должно создавать правовые, организационные и экономические условия для развития негосударственных субъектов информационной безопасности, а также способствовать их всестороннему сотрудничеству с различными государственными структурами.

Ключевые слова: информационная безопасность, культура безопасности, субъект информационной безопасности.

Zakharenko K. Efficiency of use of potential of non-state actors of information security.

Maximum result for the protection of domestic information-cultural space is provided by cooperation of its state and non-state actors.However, democratic countries have significant experience in the using the potential of non-state actors of various information security societies, associations and organizations.As well as state institutions, they are generators of new ideas and alternative approaches in the field of information security. NGOs are also tools of social control, instruments of influence on setting goals and values of society, means of the formation of public opinion. But not all NGOs can be considered as potential actors of information security.Even those among them who are legal, sometimes are used in the information war against Ukraine. Therefore the state should create legal, organizational and economic conditions for the development of non-state actors of information security, and promote their comprehensive cooperation with various government agencies.

Key words: information security, safety culture, actor of information security.