УДК 343.326:004

ІРХА Ю.Б., науковий консультант судді Конституційного Суду України

ВИКОРИСТАННЯ ЕКСТРЕМІСТАМИ МЕРЕЖІ ІНТЕРНЕТ: ПРАВОВІ ПРОБЛЕМИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ В УКРАЇНІ

Анотація. *У статті висвітлюються проблеми використання екстремістами мережі Інтернет для пропаганди своєї діяльності в Україні. Звертається увага на недосконалість національного правового регулювання інформаційної діяльності у віртуальному середовищі, що перешкоджає вчасному виявленню та нейтралізації екстремістських проявів. У результаті аналізу досвіду зарубіжних держав у цій сфері вироблено пропозиції та рекомендації щодо вдосконалення українського законодавства, функціонування органів державної влади та інститутів громадянського суспільства.*

Ключові слова: *екстремізм, екстремістські матеріали, Інтернет, інформаційно-психологічний вплив, національна безпека.*

Аннотация. *В статье освещаются проблемы использования экстремистами сети Интернет для пропаганды своей деятельности в Украине. Обращается внимание на несовершенство национального правового регулирования информационной деятельности в виртуальной среде, которое препятствует своевременному выявлению и нейтрализации экстремистских проявлений. В результате анализа опыта зарубежных государств в этой сфере выработаны предложения и рекомендации по усовершенствованию украинского законодательства, функционирования органов государственной власти и институтов гражданского общества.*

Ключевые слова: *экстремизм, экстремистские материалы, Интернет, информационно-психологическое воздействие, национальная безопасность.*

Summary. *The article deals with the problem of use of the Internet by extremists for propaganda of their activities in Ukraine. Attention is drawn to the insufficiency of national legal regulation of information activities in a virtual environment that prevents timely detection and neutralization of extremist activity. After analyzing the experience of foreign countries in this area, author made suggestions and recommendations for improving Ukrainian legislation, functioning of public authorities and civil society.*

Keywords: *extremism, extremist material, the Internet, information and psychological impact, national security.*

Постановка проблеми. Еволюція соціуму завжди супроводжується як позитивними, так і негативними зрушеннями. Нові знання, уміння і технології відкривають численні додаткові можливості для забезпечення потреб індивідів, їх захисту від внутрішніх та зовнішніх загроз. Водночас багато змін несе явну або приховану небезпеку, яку не всі здатні адекватно оцінити, а тим більше – вчасно виявити, відвернути або нейтралізувати.

Стрімкий розвиток інформаційних технологій наприкінці XX – на початку XXI століття суттєво вплинув на життя людини, суспільства і держави. Завдяки новим способам обміну інформацією став простішим доступ до відомостей наукового, художнього, енциклопедичного, довідкового характеру тощо, зросли ступінь і якість поінформованості різних суб’єктів права, розширилися можливості для комунікації, реалізації та захисту прав і свобод, а також контролю за виконанням відповідних обов’язків. Крім того, деякі правовідносини набули нового змісту не тільки на національному, але й на міжнародному рівні.

Перехід до нової моделі соціальних відносин ознаменувався появою і ряду негативних явищ. Комп’ютерні технології та Інтернет надали фактично необмежені можливості й ресурси для вільного створення, розповсюдження і зберігання інформації деструктивного спрямування, вдосконалення форми і методів маніпулювання інформацією з метою неправомірного впливу на свідомість та поведінку як окремих громадян чи їх груп, так і соціуму в цілому. Інтернет став середовищем, за допомогою якого екстремісти, терористи, представники організованої злочинності здійснюють явний або, як правило, прихований обмін інформацією, грошовими коштами, зброєю, наркотиками та іншими забороненими товарами і послугами.

Не оминула названа проблема й Україну. У нашій державі інформаційна діяльність в Інтернеті не отримала належного нормативно-правового регулювання, тому екстремісти широко використовують віртуальне середовище у своїх цілях, чим завдають значної шкоди національним інтересам.

Аналіз останніх досліджень і публікацій. Функціонування Інтернету та регулювання діяльності у цій мережі, використання її можливостей зі злочинною метою різними категоріями осіб, а також забезпечення інформаційної безпеки України є предметом багатьох досліджень. Ці питання розкриваються у працях, зокрема, О. Доброжанської, В. Іванова, Р. Марутян, А. Новицького, В. Панченко, В. Петрика, Н. Савінової, Є. Скулиша, Д. Стровського, О. Присяжнюка, К. Шурупової, Н. Юдіна.

Фахівці визнають, що міжнародне і національне законодавство не встигають належно унормовувати відносини, які виникають внаслідок стрімкого розвитку інформаційних технологій. Більше того, на нашу думку, чимало користувачів мережі Інтернет, здобуваючи вигоду з переваг інформаційного суспільства, не усвідомлює характеру та ступеня небезпек, які виникають через надто вільний обіг інформації у цій мережі. У той же час екстремісти й інші девіантні особи дуже швидко зорієнтувалися у ситуації, що склалася, і намагаються максимально ефективно використовувати віртуальний простір для своєї протиправної діяльності.

Метою статті є з’ясування основних способів та наслідків використання екстремістами мережі Інтернет за кордоном та в Україні, вироблення пропозицій щодо вдосконалення українського законодавства у сфері протидії інформаційній діяльності екстремістів у віртуальному середовищі.

Виклад основного матеріалу. Інформаційна революція стала одним із ключових факторів утворення глобального інформаційного суспільства, яке О. Проскуріна розглядає як суспільство нового типу, що формується в результаті нової глобальної соціальної революції, основою якої є інтенсивний розвиток і конвергенція інформаційних і телекомунікаційних технологій; суспільство знання, у якому головною умовою благополуччя кожної людини і кожної держави стають знання, отримані завдяки безперешкодному доступу до інформації, та вміння працювати з цією інформацією [1, с. 73]. Хоча в Окінавській хартії глобального інформаційного суспільства визнано необхідність узгодження зусиль міжнародного співтовариства, спрямованих на створення безпечного і вільного від злочинності кіберпростору [2], однак дієвих універсальних, регіональних чи навіть національних демократичних “правил гри” для реалізації вказаного задуму досі не розроблено.

Глобалізаційні перетворення у поєднанні зі світовою фінансово-економічною кризою призвели до загострення значної кількості внутрішніх проблем у багатьох державах, наслідком чого стало розв’язання або активізація економічних, етнічних, культурних, політичних, релігійних та інших конфліктів між представниками різних соціальних груп. У багатьох випадках насильницькі способи й методи вирішення цих

конфліктів стали переважати існуючі демократичні стандарти узгодження розбіжностей і протиріч. У державах почали активно з’являтися екстремістські угруповання різного спрямування. При цьому саме Інтернет став первинним, а в окремих випадках і пріоритетним майданчиком для агітації та пропаганди екстремістських ідеологій, пошуку однодумців, посібників, спільників, спонсорів екстремізму, поширення паніки, страху, чуток у суспільстві, радикалізації населення, руйнування та дискредитації традиційних ціннісних засад, соціальних інститутів, делегітимізації органів державної влади та органів місцевого самоврядування.

В Інтернеті створено велику кількість інформаційних ресурсів (сайтів), які не тільки розповсюджують матеріали екстремістського характеру, але й сприяють розвитку екстремізму. На думку фахівців, такі сайти умовно можна поділити на чотири основні групи: 1) сайти, які безпосередньо поширюють ідеї екстремізму, сепаратизму і тероризму; 2) інформаційні ресурси, що здійснюють інформаційну та фінансову підтримку представників міжнародних екстремістських та терористичних організацій; 3) сайти, що розпалюють ксенофобію на основі расової чи національної приналежності; 4) інформаційні ресурси довідкового характеру, які побічно закликають до протиправної діяльності [3].

Незважаючи на те, що Інтернет вільно використовується для розробки, передачі, отримання та зберігання інформації екстремістського характеру, органи державної влади не завжди мають правові можливості для перешкоджання екстремістській діяльності у віртуальному середовищі, а також для вчасного запобігання використанню Інтернету для планування та реалізації екстремістських проявів у реальному житті. Насамперед це зумовлено тим, що Інтернет є екстериторіальним утворенням. У багатьох державах Інтернет-контент, який вважається незаконним або шкідливим, надходить із джерел за межами їхньої територіальної юрисдикції. У зв’язку з цим виникають серйозні проблеми, адже те, що в одній державі законно, в іншій – заборонено або суттєво обмежено. Крім того, органи державної влади, як правило, не мають правових підстав для втручання у роботу сайтів, які розміщені на іноземних серверах, особливо у державах “другого” та “третього” світу.

Різноманіття політичних, культурних, моральних, релігійних цінностей та підходів до забезпечення національної безпеки створює умови за яких відсутність цензури, свобода слова та інформації, свобода віросповідання, свобода мирних зібрань і політичний плюралізм використовуються одними для побудови і зміцнення демократії та її інститутів, а іншими – для екстремістської чи терористичної діяльності, руйнування основ конституційного або суспільного ладу.

У світі не існує універсального, закріпленого у законодавстві визначення екстремізму, яке охоплювало б усі його прояви та давало б можливість органам державної влади певної країни звертатися до міжнародної спільноти по всебічну підтримку у протидії екстремістській діяльності на її території чи поза нею. Лише деякі форми екстремізму однозначно засуджуються світовим співтовариством. До них належать ті, що пов’язані зі скоєнням особливо тяжких злочинів, наприклад тероризм (бомбовий, ядерний) та його фінансування.

Звичайно поняття “екстремізм” визначається, виходячи з його сутності. У той же час інколи без спеціальної експертизи дуже важко чітко визначити правовий статус інформації, поширюваної як у друкованому, так і в електронному вигляді, адже не всі матеріали та висловлювання мають відвертий екстремістський, расистський, ксенофобський, дискримінаційний або антидержавний зміст. Існує безліч матеріалів, що містять начебто нейтральну інформацію, однак вона подається у спосіб, який спонукає до

розпалювання або підтримки незаконних протестних настроїв, міжгрупової ворожнечі, насильницьких дій щодо опонентів, дискредитації органів публічної влади тощо.

Головною особливістю поширення ідей екстремізму у віртуальному середовищі, зокрема у соціальних мережах, як зазначає І. Галицький, є можливість швидкого й оперативного контакту з багатомільйонною аудиторією без значних фінансових затрат та спеціальних засобів, що дозволяє екстремістам не лише пропагувати свої ідеї, але й організовувати масові акції у реальному житті [4, с. 81].

Управління Організації Об’єднаних Націй з наркотиків та злочинності наголошує, що екстремістська риторика все частіше переноситься до мережі Інтернет. Відповідний контент поширюється через спеціалізовані веб-сайти, віртуальні чати і форуми, Інтернет-журнали, соціальні мережі (Twitter і Facebook), відео- і файлообмінники (YouTube і Rapidshare). Екстремістська пропаганда охоплює широкий спектр завдань. Її цільову аудиторію становлять, з одного боку, потенційні та реальні прихильники екстремістів, а з іншого – їх жертви та супротивники. Окрім пропаганди, Інтернет активно використовується екстремістами для налагодження контактів, організації злочинів. Комунікації відбуваються з використанням спеціального програмного забезпечення, яке встановлює технологічні бар’єри для входу на відповідні платформи. Захищені паролями веб-сайти значно ускладнюють вчасне виявлення, відстеження та нейтралізацію правоохоронними органами протиправної діяльності екстремістів [5].

На значне зростання випадків використання екстремістами та терористами Інтернету в останні роки звертає увагу і Європейське поліцейське управління (Європол). Спеціалісти цього міждержавного правоохоронного органу виявили, наприклад, що прихильники джихаду у процесі використання у своїх цілях соціальних мереж демонструють глибоке розуміння принципів їх роботи. За допомогою вказаних ресурсів вони організовують узгоджені кампанії щодо пошуків послідовників та пропаганди своєї діяльності. З метою протидії екстремістській діяльності в Європі з 1 липня 2015 року започатковано функціонування спеціального підрозділу – European Union Internet Referral Unit, який уповноважений на співпрацю з правоохоронними органами не лише держав – членів Європейського Союзу, але й інших держав, а також із приватним сектором. Головною функцією вказаного підрозділу є виявлення шкідливого онлайн-контенту, надання оперативної та стратегічної аналітичної допомоги державам-членам Європейського Союзу [6].

Під егідою Організації з безпеки та співробітництва в Європі в період з 21 вересня по 2 жовтня 2015 року у місті Варшаві (Республіка Польща) відбулася Нарада з розгляду виконання зобов’язань, присвячених людському виміру, на якій порушувалися, зокрема, питання щодо протидії екстремістській діяльності у Інтернеті. За результатами цієї наради встановлено, що Інтернет вніс революцію у саму природу соціального конфлікту, адже створено нові канали розповсюдження фундаменталістських та інших не толерантних ідеологій, які виправдовують насильство. Фахівці зазначили, що упродовж чотирьох місяців прихильники Ісламської держави використали більш ніж 46000 акаунтів у Twitter, при цьому кожного дня було зроблено близько 90000 “твітів” на підтримку відповідної екстремістської ідеології. Експерти також звернули увагу на значну Інтернет-активність правих екстремістів у Європі та російських екстремістських угруповань в Україні [7].

За даними Федерального відомства з охорони Конституції Німеччини протягом 2014 року екстремістські організації різного спрямування широко використовували можливості Інтернету для пропаганди у німецькій державі насильницьких ідеологій і розширення своєї соціальної бази. Ліві та праві екстремісти поширювали у соціальних

мережах та інших сегментах Інтернету музику, відеозаписи та текстові матеріали з метою мобілізації своїх прихильників, генерування правильної атмосфери на публічних заходах, ідеологічного обґрунтування своїх вчинків. Такі дії розглядаються як важливий фактор радикалізації суспільства та вербуванні громадян, збільшення потенціалу екстремістів. Сучасні комунікативні технології також використовуються терористами для публічного демонстрування своїх “досягнень”, причому воно здійснюється на досить високому професійному рівні [8].

На думку керівника Федерального відомства з охорони Конституції Німеччини Ганса-Ґеорґа Маасена, світова спільнота має виробити міжнародні правила для кібервійни. Він стверджує, що радикальна пропаганда дедалі частіше здійснюється шляхом надсилання користувачам індивідуальних повідомлень у соціальних мережах та за допомогою сервісів миттєвих повідомлень. Очільник названої спецслужби зауважив, що з використанням сервісів Twitter, WhatsApp тощо масштаби пропаганди джихадистів збільшилися і зміна цього тренду наразі не очікується. Він закликає Інтернет-провайдерів бути відповідальними у своїй роботі та налагоджувати довірчу співпрацю з правоохоронними органами з метою недопущення використання їхньої інфраструктури для розповсюдження екстремістських ідей [9].

В умовах проведення широкомасштабної антитерористичної операції на Сході України активна інформаційна діяльність екстремістських угруповань, у тому числі міжнародних, або екстремістів-одинаків у мережі Інтернет серйозно загрожує інформаційному суверенітету держави та інформаційно-психологічній безпеці індивідів, під якою розуміють стан захищеності психіки людини від негативного впливу, що здійснюється шляхом упровадження деструктивної інформації у свідомість і (або) у підсвідомість людини та призводить до неадекватного сприйняття нею дійсності [10, с. 136]. Оскільки гарантування і захист інформаційної безпеки особи й суспільства є складовими національної безпеки України, то, очевидно, держава не може залишити поза увагою питання протидії інформаційним загрозам з боку екстремістів та інших суб’єктів інформаційних відносин.

За даними дослідження, проведеного компанією Factum Group Україна на замовлення Інтернет-асоціації України, у 2015 році загальна чисельність Інтернет-аудиторії по всій території України, без урахування Автономної Республіки Крим, зросла до 21,8 млн. користувачів і становить 59 % (у 2014 році – 18,8 млн). У сільській місцевості з 2012 по 2015 рік частка регулярних Інтернет-користувачів зросла більше ніж удвічі (з 21 % до 45 %) [11]. Наведені відомості дають підстави стверджувати, що за відсутності дієвих механізмів протидії, екстремісти, маніпулюючи Інтернет-аудиторією, можуть суттєво впливати на внутрішню та зовнішню політику України.

Навіть після анексії Автономної Республіки Крим та міста Севастополя, тимчасової окупації окремих районів Донецької та Луганської областей в українському законодавстві не розроблено ефективних механізмів нагляду за діяльністю в Інтернеті, своєчасного виявлення і нейтралізації реальних та потенційних загроз національним інтересам в цій мережі. Окремі екстремістські угруповання скористалися цією ситуацією і збільшили свою присутність у віртуальному інформаційному полі України, намагаючись посилити свої позиції, здобути певні економічні чи політичні дивіденди, вплинути на стан справ у державі.

У Воєнній доктрині України визначено, що до воєнно-політичних викликів, які можуть перерости в загрозу застосування воєнної сили проти України, належать, зокрема, цілеспрямований інформаційний (інформаційно-психологічний) вплив з використанням сучасних інформаційних технологій, спрямований на формування

негативного міжнародного іміджу України, а також на дестабілізацію внутрішньої соціально-політичної обстановки, загострення міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин [12]. Такий вплив здійснюється не тільки ззовні іноземними державами, зокрема їхніми збройними силами або спеціальними службами, але й зсередини через контрольовані ними екстремістські та терористичні угруповання, а це безпосередньо загрожує незалежності та суверенітету нашої держави.

Проаналізувавши зміст праворадикальних сайтів в Україні, Р. Пасічний вивив, що на всіх сайтах, де висловлюються ідеї расизму та ксенофобії, автори і лідери воліють залишатися анонімними. Деякі сайти містять контакти лише у вигляді адрес електронних поштових скриньок або номерів мобільних телефонів. Водночас юридично зареєстровані та легалізовані організації, а також організації, які претендують на участь у політичному житті, не розміщують на своїх Інтернет-сторінках висловлювань расистського та ксенофобського характеру. Дослідник звертає увагу на те, що роз’яснення всіх ідеологічних засад найчастіше міститься в матеріалах різної форми – книгах, статтях, новинах та що на проаналізованих сайтах широко представлені філософські твори, праці теоретиків націоналізму або фашизму, публіцистика, художня література, зокрема, поезія, тощо.

Науковець зазначає, що, трактуючи ті чи інші події, автори часто вдаються до різноманітних маніпуляцій із інформацією, перекручуючи її відповідно до власної ідеології чи роблячи на її основі висновки, які узгоджуються з цією ідеологією. Новини отримують необхідне “забарвлення” та подаються в такий спосіб, щоб слугувати підтвердженням ідеології сайту. Окремим пропагандистським напрямом роботи сайтів Р. Пасічний визначає розміщення зображень, плакатів та стікерів (наклейок, трафаретів), та зауважує, що найчастіше пропаганда розроблена самими авторами сайтів (такі матеріали мають низьку якість), іноді – на основі плакатів подібних або навіть конкуруючих закордонних організацій. Частина сайтів містить аудіо- та відеоматеріали або посилання на них на загальнодоступних медіаресурсах [13, с. 83-84].

Аналіз доступної широкому загалу інформації, яка поширюється у глобальній мережі, а також у вітчизняних та зарубіжних засобів масової інформації, дав фахівцям Служби безпеки України підстави стверджувати про систематичне втручання міжнародних терористичних і релігійних екстремістських організацій у внутрішні справи України, поширення на території держави діяльності право- та ліворадикальних політичних організацій, різноманітних націоналістичних рухів екстремістської спрямованості.

Так, розпалювання сепаратистських настроїв у регіонах держави, де проживають мусульманські громади, та пропаганда створення на їх основі державних утворень ісламського типу є основною метою експансії в інформаційний простір України окремих терористичних та релігійних екстремістських організацій, адже постійне розширення сфери впливу є одним із принципів ісламського фундаменталізму. Право- та ліворадикальні політичні організації активно застосовують у своїй діяльності екстремістські націоналістичні лозунги та гасла, засновані на образах “ворога” та ідеї меншовартості представників інших рас і національностей, поширюють у мережі Інтернет інформацію відповідного змісту. Націоналістичні рухи екстремістської спрямованості, неофашистські організації розповсюджують екстремістські відеоролики через Інтернет-сервіс Youtube, а також розміщують такі матеріали на закритих “торрентах” і “підкастах” [14, с. 89-90].

Українські правоохоронні органи та спецслужби мають можливості для виявлення протиправної діяльності в Інтернеті шляхом проведення відповідних оперативно-розшукових, розвідувальних та контррозвідувальних заходів. Вони здатні попередити конкретний екстремістський, у тому числі терористичний акт, про наміри щодо скоєння якого, екстремісти та їх лідери повідомляють у мережі Інтернет. Водночас дуже важко запобігти діянням екстремістського спрямування, заклики до скоєння яких, розміщені на сайтах чи у соціальних мережах та не містять чіткої вказівки на час, місце, спосіб їх здійснення. Ця інформація адресується невизначеному колу осіб, тому майже неможливо встановити усіх, хто реально відгукнеться на такі заклики.

В Україні не існує належного правового механізму оперативного реагування на виклики та загрози з боку екстремістів, які містяться у віртуальному середовищі та стосуються суспільства і держави. У національному законодавстві відсутня дефініція поняття “екстремізм” та його похідних. У зв’язку з цим виникає багато правових проблем у випадку необхідності невідкладного блокування роботи сайту чи недопущення поширення контенту екстремістського характеру, який становить реальну загрозу об’єктам національної безпеки України.

Чимало осіб, які вільно та безвідповідально поширюють інформацію в Інтернеті, виправдовують свої дії конституційним правом на інформацію, міжнародними стандартами у цій сфері, а також законодавством, яке регулює, як правило, функціонування друкованих засобів масової інформації та роботу журналістів. Проте, ми вважаємо, що за своєю природою та наслідками інформаційна діяльність у віртуальному середовищі відрізняється від інформаційної діяльності у реальному світі. Інтернет має вагомий вплив на людину, її психіку та поведінку, а тому держава зобов’язана посилено охороняти й захищати громадян від деструктивних інформаційно-психологічних впливів, зокрема з боку екстремістів, у цій мережі.

Європейський суд з прав людини у рішенні у справі “Редакція газети “Правоє дело” та Штекель проти України” вказав (пункт 63 у [15]): “Інтернет як інформаційний і комунікаційний інструмент дуже відрізняється від друкованих засобів масової інформації, особливо у тому, що стосується здатності зберігати та передавати інформацію. Електронна мережа, яка обслуговує мільярди користувачів у всьому світі, не є і потенційно не буде об’єктом такого ж регулювання та засобів контролю. Ризик завдання шкоди здійсненню та використанню прав людини і свобод, зокрема права на повагу до приватного життя, який становлять інформація з Інтернету та комунікація в ньому, є безумовно вищим, ніж ризик, який походить від преси. Таким чином, підходи, які регулюють відтворення матеріалу з друкованих засобів масової інформації та Інтернету, можуть відрізнятися. Останній, безперечно, має коригуватися з урахуванням притаманних цій технології рис для того, щоб забезпечити захист зазначених прав і свобод та сприяння їм”.

В Україні парламент досі не прийняв закон про кібербезпеку, на якому наполягає багато експертів. Хоча ще у 2005 році було ратифіковано Конвенцію про кіберзлочинність, у 2006 році – Додатковий протокол до неї, а з 30 червня 2014 року втратила чинність Доктрина інформаційної безпеки України. Крім того, законодавство у сфері боротьби з тероризмом, а також здійснення оперативно-розшукової, розвідувальної та контррозвідувальної діяльності не дозволяє повною мірою реагувати на небезпеки, які існують у віртуальному середовищі.

Незважаючи на те, що у Верховній Раді України зареєстровано проект Закону України “Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби

з кіберзлочинністю” від 19 червня 2015 року № 2133а [16], в якому пропонується вдосконалити функціонування відповідних органів державної влади в аспекті сучасних інформаційних викликів та загроз, можливість його швидкого розгляду та прийняття викликає сумніви.

Окрім органів державної влади, інформаційну безпеку України та її громадян мають забезпечувати й інститути громадянського суспільства. Соціум не може покладати на державу виключний обов’язок щодо забезпечення його безпеки. Громадяни індивідуально чи колективно повинні також залучатися до протидії інформаційно-психологічному впливу екстремістів у національному інформаційному просторі. Самостійно або за підтримки держави саме громадянське суспільство має не допустити появи та поширення екстремізму в Україні.

Погоджуємося з пропозицією В. Панченко та С. Семчишина щодо необхідності визначення суб’єкта, який би виконував функцію експертного оцінювання інформаційної продукції, що містить заклики до порушення конституційного ладу, територіальної цілісності, пропаганду війни, фашизму, національної та релігійної ворожнечі, або запровадження з метою недопущення поширення такої інформації механізму самоцензури шляхом створення міжвідомчого консультативного комітету, до складу якого доцільно включити представників виконавчої влади, правоохоронних органів, а також провідних журналістів і власників засобів масової інформації (на зразок британського Defence, Press and Broadcasting Advisory Committee – DPBAC – консультативного комітету з оборони, преси і теле-, радіомовлення [17, с. 84].

У цьому аспекті слушними є також твердження В. Петрика про необхідність створення експертної комісії на базі Координаційного центру інформаційно-психологічної безпеки Міністерства інформаційної політики України, яка перевіряла б сайти на предмет наявності протиправного контенту, зокрема такого, що містить загрози державній безпеці. Крім того, заслуговують на увагу і твердження науковця про те, що для захисту від шкідливих інформаційно-психологічних впливів можливим і необхідним є введення до навчальних планів підготовки усіх фахівців із вищою освітою обов’язкової (нормативної) навчальної дисципліни “Соціально-психологічні основи інформаційної безпеки”, а для формування критичного мислення у дітей та вироблення у них навичок розпізнавання прихованих інформаційно-психологічних впливів – вдосконалення структури й змісту навчальної дисципліни “Безпека життєдіяльності” [18, с. 89, 92].

Вважаємо, що саме через підвищення обізнаності рівня громадян із сучасними та перспективними способами й методами впливу на їхню свідомість, формування у них навичок критичного мислення, поглиблене вивчення релігійного, культурного, політичного становища в державі, а також причин появи та розповсюдження радикалізму й екстремізму, наслідків їх впливу на людину, суспільство і державу вдасться значно зменшити соціальну базу екстремістів. Відсутність підтримки екстремістської діяльності серед населення значно дезорганізовує екстремістські угруповання та позбавляє їх стимулу для подальшої протиправної діяльності як у віртуальному середовищі, так і у реальному житті.

Висновки.

Україна як складова частина глобального інформаційного суспільства не може залишати свій інформаційний простір без належного захисту. Національне інформаційне середовище має бути безпечним та сприяти розвитку Українського народу. З метою захисту громадян від деструктивних інформаційно-психологічних впливів екстремістів,

особливо у віртуальному середовищі, у державі мають бути створені відповідні правові механізми. Для реалізації цієї мети пропонуємо:

1. Прийняти закон України про кібербезпеку.

2. Ухвалити нову Доктрину інформаційної безпеки України;

3. Закріпити у Законі України “Про боротьбу з тероризмом” дефініції таких понять, як: “екстремізм”, “екстремістська діяльність”, “екстремістські матеріали”.

На нашу думку, національна система протидії екстремізму, у тому числі в мережі Інтернет, має охоплювати не тільки контрольно-наглядові та репресивні заходи. Важливо також підвищувати інтелектуальний рівень населення. Це допоможе сформувати у громадян установки для самостійного відторгнення екстремістських ідеологій і практик, що сприятиме забезпеченню національної безпеки України, відновленню її суверенітету та територіальної цілісності.

Використана література

1. Проскуріна О. Глобальне інформаційне суспільство: ідеї та реалії // Вісник Севастопольского НТУ : зб. наук. пр. – Вип. 136/2012. – (Серія : Політологія). – Севастополь, 2012. – С. 70-74.

2. Окинавская хартия глобального информационного общества : принятая 22 июля 2000 г., г. Окинава. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/998_163

3. Костихин А. Интернет как инструмент террористических и экстремистских организаций в психологической войне. – Режим доступа : //www.iimes.ru/?p=4737

4. Галицький І. Екстремізм в соціальних мережах: організаційно-правові заходи протидії // Альманах міжнародного права. – 2014. – Вип. 4. – С. 74-83.

5. The use of the Internet for terrorist purposes // United Nations Office on Drugs and Crime. – New York, 2012. – Режим доступу : //www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

6. Europols internet referral unit combat terrorist and violent extremist propaganda. – Режим доступу : //www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda

7. Participating States of OSCE must counter extremist narrative on social media. – Режим доступу : //www.osce.org/odihr/183786

8. 2014 Annual Report on the Protection of the Constitution Facts and Trends // Federal Ministry of the Interior. – Режим доступу : //www.verfassungsschutz.de/embed/annual-report-2014-summary.pdf

9. Грабська А. Німецькі спецслужби вимагають правил для кібервійн. – Режим доступу : //www.dw.com/uk/німецькі-спецслужби-вимагають-правил-для-кібервійн/a-18333761

10. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України // Політичний менеджмент. – 2008. – № 4(31). – С. 135-141.

11. 165 населених пунктів підключено до безлімітного Інтернету від Укртелекому в першому півріччі 2015 року. – Режим доступу : //www.ukrtelecom.ua/presscenter/news/pressrelease?id=134727

12. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року “Про нову редакцію Воєнної доктрини України” : Указ Президента України від 24.11.15 р. № 555/2015. – Режим доступу : //www.president.gov.ua/documents/5552015-19443

13. Пасічний Р. Толерантність : Інтернет-джерела праворадикальних рухів України // Українська національна ідея : реалії та перспективи розвитку. – 2010. – Вип. 22. – С. 82-86.

14. Мельник Д. Мережа Інтернет як засіб поширення інформації екстремістського змісту зб. матеріалів “круглого столу” [“Запобігання радикалізації і тероризму : міжнародний досвід і національний вимір”] : за ред. М.Г. Гуцало. – К. : НІСД, 2012. – С. 88-91.

15. Рішення Європейського суду з прав людини у справі “Редакція газети “Правоє дело” та Штекель проти України” від 5 серпня 2011 року. – (Заява № 33014/05). – Режим доступу : http://zakon3.rada.gov.ua/laws/show/974_807/print1444740902222308

16. Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю : проект закону України від 19.06.15 року № 2133а. – Режим доступу : http://w1.c1.rada.gov.ua /pls/zweb2/webproc4_1?pf3511=55668

17. Панченко В., Семчишина С. Тактичні пріоритети України у сфері забезпечення інформаційної безпеки у сучасних умовах : зб. матер. наук.-практ. конф. [Актуальні проблеми управління інформаційною безпекою держави], (Київ, 19 березня 2015 року). – К. : Центр навчальних наукових. та періодичних видань НА СБ України, 2015. – С. 83-85.

18. Петрик В. Пропозиції щодо підготовки фахівців з інформаційної безпеки держави та формування критичного мислення населення для захисту від шкідливих інформаційно-психологічних впливів зб. матер. наук.-практ. конф. [Актуальні проблеми управління інформаційною безпекою держави], (Київ, 19 березня 2015 року). – К. : Центр навчальних, наукових та періодичних видань НА СБ України, 2015. – С. 89-93.

Рецензент: Скуліш Є.Д., доктор юридичних наук, професор

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~