ФП 2017-5
ISSN 1995-6134

УДК 659.4:327.88(477)
DOI: http://doi.org/10.5281/zenodo.1206228

А.О. ЯФОНКІН,
доцент кафедри військової підготовки
Університету державної фіскальної служби України, кандидат юридичних наук, доцент,
м. Ірпінь, Україна;
ORCID: http://orcid.org/0000-0001-9143-6122

В.А. ШЕВЧУК,
завідувач кафедри військової підготовки
Університету державної фіскальної служби України, кандидат юридичних наук,
м. Ірпінь, Україна;
ORCID: http://orcid.org/0000-0002-6950-4827

ІНФОРМАЦІЙНА ВІЙНА ПРОТИ ДЕРЖАВИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

A.A. YAFONKIN,
Ass. Professor, Chair of military training,University of the State Fiscal Service of Ukraine,
Ph.D. in Law, Associate Professor, Irpin, Ukraine;
ORCID: http://orcid.org/0000-0001-9143-6122

V.A. SHEVCHUK,
Head, Chair of military training, University of the State Fiscal Service of Ukraine,
Ph.D. in Law, Irpin, Ukraine;
ORCID: http://orcid.org/0000-0002-6950-4827

INFORMATION WAR AND INFORMATION SECURITY OF UKRAINE

З прагненням України до повноцінного членства у Європейському Союзі в умовах проведення масштабних реформ, майже у всіх сферах суспільного життя, посилюється роль і значення інформації та забезпечення інформаційної безпеки держави.

Незважаючи на великі зусилля щодо захисту інформації та інформаційних ресурсів, актуальною задачею є та залишаються вирішення питань вдосконалення українського інформаційного законодавства у сфері створення, поширення, використання та ефективного захисту інформації відповідно до сучасних потреб і викликів, ефективного законодавчого забезпечення захисту інформаційного простору України від внутрішніх і зовнішніх загроз та запровадження ефективних механізмів їх реалізації.

Крім вищевказаних актуальних задач, які постають перед суспільством та державою, негативний вплив для досягнення визначеної мети в усіх сферах суспільного життя має так звана «інформаційна війна», яка потребує своєчасного вирішення.

Теоретичною основою даного дослідження є наукові праці вітчизняних та зарубіжних вчених А.Л. Еремина, М.І. Зубка, Г.Г. Почепцова, А.А. Поляруша, П.С. Прибутька, Б.А. Кормича, В.В. Крутова, І.Б. Лук'янця , А.Г. Міщенка, І.Г. Муковського, В.М. Петрика, В.В. Остроухова, А.А. Штоквиша, О.В. Нестеренка, А.М. Юрченко, М.М. Шевченка та інших, вітчизняне законодавство у зазначеній сфері та передовий досвід іноземних держав, які досягли значного прогресу у сфері забезпечення інформаційної безпеки держави. Тому метою статті є висвітлення напрямів забезпечення інформаційної безпеки держави, як складової національної безпеки України, діяльності спецслужб щодо збору інформації із соціальних мереж для її подальшого використання, шляхів забезпечення безпеки інформаційних систем держави та протидія «інформаційним війнам».

Ніколо Макіавеллі в творі «Государ» позначив проблематику проведення інформаційних війн, де сформулював поради для політичних та військових лідерів щодо здійснення ефективної інформаційної політики для здійснення успішних війн та управління державою. Розглядаючи специфіку розвитку монархічної та республіканської форми правління, автор надав поради, як

ISSN 1995-6134

потрібно вибудовувати комунікацію між народом та правлячою елітою, а також як вибудовувати міждержавні стосунки [1, с.28].

Враховуючи, що антитерористична операція в Україні продовжується вже четвертий рік, слід констатувати, що інформаційний компонент став набагато сильнішим, нових можливостей додали соціальні мережі. Тому держава потребує відповідної підтримки як з боку військових, так і з боку цивільного населення.

Не можна не погодитись з думкою Г.Г. Почепцова, який стверджує,що армія більше орієнтована на дії у фізичному просторі, тому для неї важко розвивати інформаційний інструментарій та інформація не потрібна, якщо вона не підсилює військову дію. Однак, у сучасних умовах активізації інформаційних війн необхідно особливу увагу приділити активній інформаційній роботі саме з цивільним населенням, яке не зовсім правильно розуміє цю війну. Враховуючи, що власне відношення населення, представниками якого є люди зі своїми проблемами, зі своїм рівнем освіти і своїм рівнем сприйняття, до споживання інформації є досить суттєвим фактором, відроджується інтерес до війни ідей.

Сьогодні сучасні засоби комунікації у поєднанні з науковими методами надають інструменти, якими воно раніше не володіло. Ключова роль застосування технологій масових маніпуляцій зі свідомістю населення країни, «ненасильницької зміни режиму» тощо, відведена ЗМІ і мережі Інтернет [2].

Однак, в умовах перебування майже усіх засобів масової інформації у приватній власності олігархічних груп, кланів, об'єднань та окремих фізичних осіб-олігархів, відсутність достовірної інформації внаслідок її обмеженості або закритості відіграє негативну роль для подальшого розуміння громадянами шляхів та напрямів розвитку держави, невизначеності перспектив їхнього гідного існування та самовдосконалення, викликає почуття незахищеності [3].

Так, за результатами моніторингу у 2018 році Національної ради з питань телебачення і радіомовлення, присвяченого висвітленню ситуації на сході України, в ефірі шести загальнонаціональних інформаційно-розважальних каналів (ICTV, «1+1», «UA: Перший», «Інтер», НТН, «Україна») – відбувалось тільки 22 години, які становлять лише 2,2 % з 1008 годин від тижневого обсягу ефіру

За словами медіа експерта Діани Дуцик, наприкінці 2016 року «Детектор медіа», Інститут масової інформації також робили схожий моніторинг. Цифри були приблизно такі ж самі. Ситуація за цей період часу не змінилася. Інформаційні потреби та очікування людей на сході та в усій Україні зовсім інші, ніж те, що дають їм телеканали. Люди дуже потребують більше інформації про те, що відбувається в нас на фронті або просто в Луганській та Донецькій областях, на окупованих територіях; також вони потребують інформації й про те, що відбувається в Криму. Моніторинг показав, що найбільша частка інформації про події на сході – це офіційні зведення: були обстріли – не було, є поранені – нема, є загиблі – нема. Навіть до цієї інформації люди ставляться з недовірою. Тому що особливо ті, хто живе на лінії розмежування, отримують такого роду інформацію безпосередньо на місці – від військових. Або вони є свідками того, що там відбувається. Але вони, наприклад, кажуть: нам ніхто не пояснює, чому приймаються ті чи інші рішення [4].

Аналіз діяльності сучасних різноманітних суспільних організацій, союзів, засобів масової комунікації та висловлювання окремих політиків, представників окремих партій та чиновників високого рангу свідчить, що у всіх сферах – ідеології, релігії, історії, освіти, символів ведуться інформаційні війни: один проти іншого, один проти усіх, усі проти одного, усі проти усіх та в інших формах.

Слід констатувати, що великий резонанс в українському суспільстві та світі викликала заборона в Україні соціальних мереж. Генеральний секретар Ради Європи заявив, що «блокування соціальних мереж, пошукових систем, поштових служб та інформаційних веб-сайтів суперечить нашому спільному розумінню свободи висловлювання та свободи засобів масової інформації». «Більше того, такі загальні широкі заборони не відповідають принципу пропорційності», – заявив генсек РЄ [5]. Необхідно нагадати, що принцип пропорційності застосовується у законодавстві для визначення балансу між обмежувальними заходами та загрозою, яку становить те, на що було накладено заборону.

Загальновідомо, що за допомогою соціальних мереж можна не тільки впливати на суспільну свідомість, збирати людей на масові акції і «кольорові революції», але й вербувати найманців в бандформування, планувати і координувати їх дії, організовувати теракти і диверсії, проводити масштабні операції, завдаючи ворожій державі неприйнятного збитку. Так, наприклад, найпопулярнішу серед українців соцмережу «ВКонтакте» використовують 16 мільйонів

ISSN 1995-6134

людей, а в «Одноклассниках» зареєстровано 9,5 мільйонів українців [6].

Тому слід погодитись з висловлюванням відомого публіциста і політолога Анатолія Вассермана, який стверджує, що «соціальні мережі – це найкращий з наявних зараз інструментів збору найрізноманітніших відомостей, оскільки люди викладають ці відомості самостійно і викладають навіть те, що ніякий розвідник не додумався б запитати» [7]. Такою неймовірною можливістю для збору інформації із соціальних мереж та пропаганди своїх ідей серед багато мільонної аудиторії скористалися окремі передові країни. Так, для просування своїх ідей і пропаганди в соціальних мережах ще 05.05.2009 року в США було сформовано кібервійська як спеціальний підрозділ Стратегічного командування. Нині військові США обговорюють створення принципово нової структури управління інформаційними операціями (неієрархічної), яка за інноваційними можливостями буде схожою на Google, Facebook чи Apple. В РФ також створено війська інформаційних операцій та внесені відповідні зміни до діючого законодавства щодо вдосконалення правових механізмів, спрямовані на протидію поширенню в державі забороненої інформації в Інтернеті.

В Україні Постановою Кабінету Міністрів від 14.01.2015 року № 2 було утворено Міністерство інформаційної політики України (далі – Міністерство), що забезпечує формування та реалізує державну політику у сферах інформаційного суверенітету України, державного іномовлення та інформаційної безпеки. В рамках виконання покладених на нього основних завдань Міністерство має вживати заходів до захисту прав громадян на вільний збір, зберігання, використання і поширення інформації [8]. При цьому, Указом Президента України № 133/2017, який набув чинності 17.05.2017 року, було застосовано санкції щодо 468 російських і українських компаній, а також 1228 фізичних осіб [9].

Немає сенсу сперечатися з тим фактом, що соціальні мережі дуже спростили життя людей для спілкування, бізнесу. Однак, використання системи Інтернет має свої негативні сторони, оскільки інформація, що з'явилася в соціальних мережах одного разу, залишається там назавжди; соціальні мережі відстежують IP користувачів або ж сторінки, з яких вони зайшли на їх сервера, в режимі персональної прив'язки; державні органи, спеціальні служби тісно взаємодіють з соціальними мережами.

Підтвердження цього є приклади, коли британські спецслужби ще в 2008 році домовилися з Google змінити ранжирування результатів пошуку на деякі ключові слова, пов'язані з терористичним угрупуванням «Аль-Каїда». В Китаї Google погодився на деякі поступки владі, коли вона взялася за регулювання Інтернету в країні. Характерним є й скандал, пов'язаний з так званими «російськими тролями», яких звинуватили в тому, що вони через політичну рекламу в Facebook вплинули на вибори президента США. Тоді глава американської соціальної мережі без будь-яких питань пішов на співпрацю зі спецслужбами та виклав їм всю необхідну інформацію [10].

Постановою Уряду РФ «Про внесення змін до Правил взаємодії організаторів поширення інформації в інформаційно-телекомунікаційній мережі Інтернет із уповноваженими державними органами, які проводять оперативно-розшукову діяльність або забезпечення безпеки Російської Федерації». Відповідно до неї, власники інтернет-месенджерів зобов'язані забезпечувати нерозголошення будь-якої інформації про конкретні факти і зміст їх взаємодії з органами, які проводять оперативно-розшукову діяльність або забезпечення державної безпеки. Віддалений доступ до інформаційної системи власників інтернет-месенджерів, для отримання інформації про переданих повідомленнях та іншої інформації користувачів, надається уповноваженому підрозділу ФСБ Росії в строк не пізніше 3 місяців з дати отримання відповідного повідомлення.

Слід зазначити, що в сучасних умовах високих інформаційних технологій заборонити щось в Інтернеті повністю неможливо як би цього хтось не хотів. Треба констатувати, що українська влада мало зробила для того, щоб роз'яснити населенню, яку загрозу становлять ці ресурси. На нашу думку, головною зброєю українського суспільства у боротьбі із будь-якою пропагандою, має стати навчання громадян країни критичному осмисленню отриманої інформації та усвідомленню, що інформація, отримана у соціальних мережах або з інших, сумнівних джерел, може не відповідати дійсності та бути недостовірною.

З іншої сторони, для боротьби з сепаратизмом та тероризмом потрібно використовувати різні джерела інформації, в тому числі і соціальні мережі, як це роблять спецслужби передових країн світу. Це приносить свої ефективні результати та допомагає ще на рівні підготовки до терористичних актів або виникнення антидержавних настроїв завчасно їх виявляти, нейтралізувати та ліквідовувати. Однак, слід мати на увазі, що в окремих випадках державні інтереси

ISSN 1995-6134

не збігаються з інтересами тих, хто управляє тими державами.

Заборона доступу громадян до соціальних мереж, на нашу думку, для вітчизняних спецслужб відіграє негативну роль, яка полягає в обмеженості для збору та аналізу інформації, що циркулює в мережі Інтернет. Наслідком такого обмеження може стати відсутність або недостатність ефективних результатів діяльності відповідних спецслужб. Заборона використання інформаційної зброї держави агресора на своїй території не означає відсутність контролю за цією зброєю спецслужбами України.

Слід зазначити, що інформаційні війни за метою носять той самий характер, що й збройні конфлікти, економічна експансія або інші види агресивних впливів. У деяких випадках результати ведення інформаційної війни більш ефективні ніж бойові дії. Прикладів тому можна навести безліч, що відбувались та відбуваються зараз у світі.

Як відомо, країна не може здійснювати організований опір збройній агресії, якщо знищено 40 відсотків населення або 60 відсотків промислових об'єктів. Сьогодні, за оцінками деяких іноземних експертів, відключення комп'ютерних систем в результаті хакерської атаки призведе до руйнування 20 відсотків середніх компаній і третини банків протягом декількох годин, а за кілька діб зупиниться половина всіх підприємств. В результаті економіка держави впаде.

Прикладом такої атаки можна навести масштабну атаку влітку 2017 року вірусу-вимагача NotPetya, який вразив IT-системи компаній в декількох країнах світу, в більшій мірі торкнувшись України. Атаки зазнали комп'ютери нафтових, енергетичних, телекомунікаційних, фармацевтичних компаній, а також державних органів. Результати атаки відчув на собі майже кожний другий громадянин України.

У книзі «Мистецтво війни» великий китайський стратег і мислитель Сунь-Цзи писав: «Щоб бути невідомим для супротивника, треба всіма можливими способами шукати й добувати інформацію про нього» [11]. Мислитель розвинув теорію, що для безпеки держави необхідно мати таку розвідувальну систему, яка би давала інформацію як про друзів, так і про ворогів. За його словами, цілісний підхід до ведення війни глибоко аналітичний, вимагає ретельної підготовки і формулювання загальної стратегії перед початком військової кампанії.

Проведена паралель між цим висловлюванням та сучасними реаліями надає можливості дійти висновку, що моніторинг спеціальними суб'єктами соціальних мереж дозволив би виявляти як друзів, нейтральних так й недругів. Підтвердженням плідної співпраці спецслужб України із IT-компаніями, дозволило працівникам Служби Безпеки України під час проведення комплексу контррозвідувальних та антитерористичних заходів виявити та заблокувати тридцять один сайт, на яких пропагандувалась діяльність терористичних організацій, які заборонені в Україні.

Слід зазначити, що велика кількість прихованої інформації видобувається шляхом систематичного збору, обробки та аналізу публічної відкритої інформації, серед яких відрізняють відкриті джерела – інформація, що надана особою чи групою без сподівань на конфіденційність; доступна для громадськості інформація – дані, факти, інструкції, або інші матеріали, опубліковані чи передані широкому загалу, доступні на вимогу будь-якої людини, законно побачені або почуті будь-яким випадковим спостерігачем, чи розголошені на зустрічах відкритих широкій публіці [12].

Треба констатувати, що в окремих випадках розвіддані з відкритих джерел не лише не відрізняються від таємниць, а часто перевершують секретну інформацію за цінністю.

Аналіз діяльності засобів масової комунікації в Україні, особливо прямих трансляцій різних заходів на телевізійних каналах за участю відомих політиків, експертів, військових, «діячів» та інших запрошених, дозволяє досвідченому розвіднику-аналітику виявляти завчасно наміри держави, уряду або військових формувань ще на стадії їх розробки та отримати інформацію, яка має належати до конфіденційної, таємної або цілком таємної. Але, навіть за наявності відкритого порушення законів України про нерозголошення вищевказаної інформації, в Україні немає офіційно оприлюднених випадків притягнення таких осіб до юридичної відповідальності.

На нашу думку, для вирішення згаданої проблеми необхідно ввести відповідні зміни до діючого законодавства в зазначеній сфері. Іншою проблемою у сфері інформаційної безпеки держави залишається стан її інформаційних систем, розвиненість стратегічно важливих галузей науки, загальний культурно-освітній та життєвий рівень населення, рівень його соціальної захищеності тощо.

Необхідно зазначити, що функціонування інформаційної системи має здійснюватися з урахуванням дотримання законодавства України в

ISSN 1995-6134

сфері поширення інформації. При цьому, необхідно прийняти заходи щодо недопущення використання інформаційної системи з метою неправомірної обробки інформації, розміщення забороненої інформації, протиправної інформації та інформації, поширюваної з порушенням закону.

Дуже важливо, щоб інформаційна система функціонувала в безперервному режимі, має бути забезпечена безперебійна цілодобова робота інформаційної системи, а також цілісність, стійкість функціонування і безпека системи відповідно до вимог, встановлених законодавством України до інформаційних систем загального користування.

При розробці структури інформаційної системи і застосовуваних технологічних рішень необхідно передбачити забезпечення можливості розширення її функціональних можливостей. Особливо важливе значення має забезпечення безпеки інформаційних систем від незаконного зовнішнього або внутрішнього втручання «зацікавлених» суб'єктів.

Одночасно, користувачам інформаційної системи на підставі запитів повинен бути забезпечений автоматичний пошук необхідної інформації, а також надання результатів пошуку в доступній формі. Програмне забезпечення та технологічні засоби інформаційної системи мають забезпечувати доступ користувачів до ознайомлення з загальнодоступною інформацією, розміщеною в інформаційній системі.

На нашу думку, доступ до інформаційної системи має надаватися без обов'язкової установки на електронні обчислювальні пристрої користувачів, спеціально створених для перегляду сайтів програмних і технологічних засобів, а також програм для електронних обчислювальних машин.

Для забезпечення користування інформаційною системою повинні використовуватися такі технологічні засоби, як: оперативне відновлення працездатності системи і її частин в разі відмови їх роботи; моніторинг подій і поточного стану інформаційної системи та її частин, що дозволяє безперервно відстежувати доступність програмно-апаратного комплексу інформаційної системи і поточний стан використання обладнання, а також оперативно інформувати оператора інформаційної системи про відмову роботи інформаційної системи і її частин; контроль і аналіз поточної продуктивності і працездатності інформаційної системи і її частин, оперативне виявлення загроз, що обмежують її продуктивність і стійкість; резервне копіювання програмного забезпечення та інформації, що міститься в інформаційній системі, а також безстрокове зберігання всієї інформації, що розміщується в інформаційній системі; дотримання встановлених законодавством України вимог інформаційної безпеки та захисту персональних даних, розміщених в інформаційній системі; ведення електронних журналів обліку операцій, що дозволяють забезпечувати облік всіх дій з розміщення, зміни і видалення інформації в інформаційній системі, в тому числі фіксації точного часу здійснення таких дій, а також інформації, що дозволяє ідентифікувати користувачів, їх уповноважених осіб, оператора інформаційної системи, які здійснили операції в інформаційній системі [13].

Враховуючи вищевикладене слід розуміти, що державна інформаційна система інформаційних ресурсів, інформаційно-телекомунікаційних мереж, доступ до яких обмежений на території України, відповідно до Указу Президента України № 133/2017, який набув чинності 17.05.2017 року, повинна відповідати визначеним технологічним вимогам.

Необхідно посилювати боротьбу з впливом іноземних спецслужб через соціальні мережі. Для усунення негативних наслідків від впливу соціальних мереж на громадян Україні необхідно не забороняти, а ефективно взаємодіяти з розробниками соціальних мереж щодо виконання ними законодавства нашої країни задля перетворення їх з інструменту політичної пропаганди в інструмент обміну достовірною інформацією.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник. Київ : ВІКНУ, 2016. 286 с.
2. Присяжнюк М. М., Бєлошевич Я. С. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки.* 2013. Вип. 30. С. 37–41.
3. Яфонкін А. О. Обіг неправдивої інформації у засобах масової комунікації в Україні. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2017. Вип. 2–3 (6–7). С. 153–158.
4. Дуцик Д. Інформаційний вакуум: як українські телеканали висвітлюють події на Донбасі та в Криму. URL: https://hromadskeradio.org/programs/kyiv-donbas/informaciynyy-vakuum-yak-ukrayinski-telekanaly-vysvitlyuyut-podiyi-na-donbasi-ta-v-krymu.

5. Власенко В. Генсек Ради Європи: Блокування соціальних мереж не відповідає принципу свободи ЗМІ. URL: http://p.dw.com/p/2d5iH.
6. Бердинских Х. Заборона російських соціальних мереж – це безпека країни чи обмеження демократичних свобод. URL: https://24tv.ua/zaborona_rosiyskih_sotsialnih_merezh__tse_bezpeka_krayini_chi_obmezhennya_demokratichnih_svobod_n819269.
7. Вассерман А. А. Социальные сети и дезинформация. URL: http://plaza152.ru/video/jXccNMj2MIA.
8. Питання діяльності Міністерства інформаційної політики України : Постанова Кабінету Міністрів України від 14.01.2015 № 2. *Офіційний вісник України*. 2015. № 6. Ст. 124.
9. В Україні набув чинності указ про блокування ВКонтакте і Одноклассников. URL: https://www.unian.ua/politics/1926399-v-ukrajini-nabuv-chinnosti-ukaz-pro-blokuvannya-vkontakte-i-odnoklassnikov.html.
10. Социальные сети, как оружие пропаганды западных спецслужб. URL: http://x-true.info/61865-socialnye-seti-kak-oruzhie-propagandy-zapadnyh-specsluzhb.html.
11. Сунь-цзы. Искусство войны. Київ : Центрполиграф, 2014. 192 с.
12. Ржевська Н. Ф., Кожушко О. О. Розвідка відкритих джерел. URL: http://ena.lp.edu.ua/bitstream/ntb/19232/1/53-Rzhevska-257-261.pdf.
13. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навчальний посібник. Х. : Вид. ХНЕУ, 2013. 476 с.

REFERENCES

1. Kurban, O. V. (2016). *Suchasni informatsiyni viyny v merezhevomu on-layn prostori: navchal'nyy posibnyk* [Modern information wars in the on-line network space: tutorial]. Kyiv: VIKNU (in Ukr.).
2. Prysyazhnyuk, M. M., & Byeloshevych, YA. S. (2013). Informatsiyna bezpeka Ukrayiny v suchasnykh umovakh [Information security of Ukraine in modern conditions]. *Visnyk Kyyivs'koho natsional'noho universytetu imeni Tarasa Shevchenka. Viys'kovo-spetsial'ni nauky,* (30). 37–41 (in Ukr.).
3. Yafonkin, A. O. (2017). Obih nepravdyvoyi informatsiyi u zasobakh masovoyi komunikatsiyi v Ukrayini [The circulation of false information in mass media in Ukraine]. *Mizhnarodnyy yurydychnyy visnyk: aktual'ni problemy suchasnosti (teoriya ta praktyka),* (2–3). 153–158 (in Ukr.).
4. Dutsyk, D. *Informatsiynyy vakuum: yak ukrayins'ki telekanaly vysvitlyuyut' podiyi na Donbasi ta v Krymu* [Information vacuum: how Ukrainian TV channels cover events in the Donbass and Crimea]. Retrieved from: https://hromadskeradio.org/programs/kyiv-donbas/informaciynyy-vakuum-yak-ukrayinski-telekanaly-vysvitlyuyut-podiyi-na-donbasi-ta-v-krymu (in Ukr.).
5. Vlasenko, V. *Hensek Rady Yevropy: Blokuvannya sotsial'nykh merezh ne vidpovidaye pryntsypu svobody ZMI* [Secretary General of the Council of Europe: Blocking social networks does not comply with the principle of freedom of the media]. Retrieved from: http://p.dw.com/p/2d5iH (in Ukr.).
6. Berdynskykh, KH. *Zaborona rosiys'kykh sotsial'nykh merezh – tse bezpeka krayiny chy obmezhennya demokratychnykh svobod* [The prohibition of Russian social networks is the security of the country or the restriction of democratic freedoms]. Retrieved from: https://24tv.ua/zaborona_rosiyskih_sotsialnih_merezh__tse_bezpeka_krayini_chi_obmezhennya_demokratichnih_svobod_n819269 (in Ukr.).
7. Vasserman, A. A. *Sotsial'nyye seti i dezinformatsiya* [Social networks and disinformation]. Retrieved from: http://plaza152.ru/video/jXccNMj2MIA (in Ukr.).
8. Pytannya diyal'nosti Ministerstva informatsiynoyi polityky Ukrayiny [Questions of activity of the Ministry of Information Policy of Ukraine]. Postanova Kabinetu Ministriv Ukrayiny (14.01.2015 № 2). *Ofitsiynyy visnyk Ukrayiny,* (6). 124 (in Ukr.).
9. *V Ukrayini nabuv chynnosti ukaz pro blokuvannya VKontakte i Odnoklassnykov* [In Ukraine, a decree on the blocking of VKontakte and Odnoklassniki came into force]. Retrieved from: https://www.unian.ua/politics/1926399-v-ukrajini-nabuv-chinnosti-ukaz-pro-blokuvannya-vkontakte-i-odnoklassnikov.html (in Ukr.).
10. *Sotsial'nyye seti, kak oruzhiye propagandy zapadnykh spetssluzhb* [Social networks, as a weapon of propaganda of Western special services]. Retrieved from: http://x-true.info/61865-socialnye-seti-kak-oruzhie-propagandy-zapadnyh-specsluzhb.html (in Russ.).
11. Sun'-tszy. (2014). *Iskusstvo voyny* [Art of War]. Kyiv: Tsentrpoligraf (in Russ.).
12. Rzhevs'ka N. F., & Kozhushko O. O. *Rozvidka vidkrytykh dzherel* [Exploration of open sources]. Retrieved from: http://ena.lp.edu.ua/bitstream/ntb/19232/1/53-Rzhevska-257-261.pdf (in Ukr.).
13. Ostapov, S. E., Yevseyev, S. P., & Korol', O. H. (2013). *Tekhnolohiyi zakhystu informatsiyi: navchal'nyy posibnyk* [Information security technologies: tutorial]. Kharkiv: Vyd. KHNEU (in Ukr.).

Надійшла 16.11.2017

ISSN 1995-6134

Яфонкін А. О., Шевчук В. А. Інформаційна війна проти держави та інформаційна безпека України. Форум права: електрон. наук. фахове вид. 2017. № 5. С. 466–472. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2017_5_73.pdf

DOI: http://doi.org/10.5281/zenodo.1206228

Увагу приділено аналізу нормативно-правових актів у сфері інформаційної безпеки та наслідків заборони використання соціальних мереж. Досліджено досвід використання соціальних мереж спецслужбами деяких держав для своєчасного виявлення, нейтралізації та ліквідації терористичних загроз або інших антидержавних настроїв. Зазначені позитивні та негативні сторони використання мережі Інтернет.

Ключові слова: *інформаційна війна, інформаційні системи, маніпуляції зі свідомістю, заборона, спецслужби, тероризм, сепаратизм*

***

Яфонкин А.А., Шевчук В.А. Информационная война и информационная безопасность Украины

Внимание уделено анализу нормативно-правовых актов в сфере информационной безопасности и последствий запрета использования социальных сетей. Исследован опыт использования социальных сетей спецслужбами некоторых государств для своевременного выявления, нейтрализации и ликвидации террористических угроз или других антигосударственных настроений. Указаны положительные и отрицательные стороны использования сети Интернет.

Ключевые слова: *информационная война, информационные системы, манипуляции с сознанием, запрет, спецслужбы, терроризм, сепаратизм*

***

Yafonkin A.A., Shevchuk V.A. Information War and Information Security of Ukraine

Given that the antiterrorist operation in Ukraine has been going on for the fourth year, the state should pay more attention to active information work with the civilian population. According to the results of the analysis of the mass media of Ukraine, it is indicated that insufficient attention is paid to the coverage of the situation in the east of Ukraine. It is stated that the big resonance in the Ukrainian society and the world has caused a ban in Ukraine of social networks.

The role of social networks in the lives of people, the positive and negative aspects of using the Internet system are noted. Particular attention is paid to the interaction of special services with social networks to combat terrorism, separatism and other anti-state manifestations. It is noted that in modern conditions of high information technologies to ban anything on the Internet is completely impossible. It is noted that the Ukrainian authorities have done little to explain to the population the threat posed by information resources.

The main weapon of Ukrainian society in combating any kind of propaganda should be to educate the citizens of the country on the critical understanding of the information received and to realize that information received from social networks or from other questionable sources may not be true and unreliable. The conclusion is made of the need to strengthen the fight against the negative impact of foreign intelligence services through social networks on Ukrainian citizens. It is proposed to interact with social networking developers to implement the Ukrainian legislation in order to transform into reliable information exchange tools.

Key words: *information warfare, information systems, manipulation with consciousness, prohibition, special services, terrorism, separatism*