ISSN 2518-1521 (Online), ISSN 2226-2830 (Print)
ВІСНИК МАРІУПОЛЬСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ
СЕРІЯ: ІСТОРІЯ. ПОЛІТОЛОГІЯ, 2022, ВИП. 33-34

ПОЛІТИЧНІ НАУКИ

УДК 94(477.75)

В. В. Легкодух

АНАЛІЗ ЗОВНІШНЬОГО ВПЛИВУ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ НА ВІЙСЬКОВОСЛУЖБОВЦІВ ЗБРОЙНИХ СИЛ УКРАЇНИ ЧЕРЕЗ ЗАСОБИ МОБІЛЬНОГО ЗВ'ЯЗКУ

У статті досліджено зовнішній вплив Російської Федерації (РФ) на військовослужбовців Збройних Сил України (ЗСУ) через засоби мобільного зв'язку. Виокремлено основні форми впливу на військовослужбовців ЗСУ через засоби мобільного зв'язку. Розглянуто основні шляхи використання мобільних мереж противником, які дають доступ спецслужбам РФ до інформації про місцезнаходження абонента. Окреслено роботу командирів підрозділів ЗСУ щодо упередження впливу противника через засоби мобільного зв'язку на українських воїнів.

Ключові слова: *антитерористична операція, засоби мобільного зв'язку, військовослужбовці, Збройні Сили України, інформаційно-психологічний вплив.*

DOI 10.34079/2226-2830-2022-12-33-34-60-70

Російська агресія на Донбасі диктує нову реальність. Небезпека полягає не лише у можливості фізичного поранення, але й у потенційній загрозі інформаційно-психологічного впливу. Російська Федерація (РФ) з 2014 року веде інформаційну наругу над військовослужбовцями України. З цією метою активно використовуються засоби мобільного зв'язку. 22 лютого 2017 року на засіданні Державної думи РФ міністр оборони Росії С. Шойгу підтвердив наявність у збройних силах (ЗС) РФ військ інформаційних операцій (Міністерство оборони України, 2016а), що є черговим оприлюдненням факту їхнього реального існування і логічним доказом активних дій проти України.

Обмежимо наше дослідження вивченням впливу підрозділів військ інформаційних операцій ЗС РФ на військовослужбовців Збройних Сил України (ЗСУ) засобами мобільного зв'язку.

У сучасному світі способи і швидкість поширення інформації відіграє важливу роль в інформаційній війні. Від форми і швидкості надходження інформації залежить хід бойових дій, психологічний стан військовослужбовців і час проведення тієї чи іншої спецоперації. На відміну від усного оповіщення чи телефонного дзвінка, SMS-розсилка менш ніж за секунду може охопити велику кількість людей.

У німецькій газеті «Bild» зазначалося, що для імітації сигналів із мобільного телефону і масової розсилки SMS-повідомлень у 2015 році в Донецькому регіоні розміщено хай-тек обладнання (ГЛАВКОМ, 2017).

Проблема використання на війні різноманітних засобів зв'язку, в тому числі й мобільних мереж, відображена в численних наукових публікаціях сучасних дослідників. Зокрема, В. Конах (2004) вивчав роль інформаційних операцій та інформаційних воєн у

державній політиці США. І. Руснак (2000) дослідив генезу популяризації форм і способів ведення інформаційної боротьби на сучасному етапі. Г. Пєвцов, С. Залкин та А. Феклістов (2011) виокремили концептуальні підходи до забезпечення інформаційної безпеки у воєнній сфері. В. Пєвцов, А. Гордієнко, С. Залкін та ін. (2017) на основі проведеного аналізу інформаційного протиборства у воєнних конфліктах останнього часу запропонували основні підходи до проведення інформаційно-психологічних операцій ЗСУ. У напрацюваннях Г. В. Пєвцова та ін. (2014, 2014b, 2015, 2016, 2016a) розглянуто особливості проведення інформаційно-психологічної операції РФ в АР Крим, моделі впливу та напрями протидії інформаційно-психологічним операціям РФ в Україні, запропоновано методику оцінювання ефективності виконання заходів протидії негативному інформаційно-психологічному впливу противника. В. Горбулін (2015) дослідив зміст «гібридної війни» як ключового інструменту російської геостратегії реваншу.

Але попри численні дослідження інформаційного впливу з боку Росії на населення та ЗСУ, мало є інформації про використання з цією метою мобільних телефонів. До того ж вона розпорошена за джерелами розміщення та іншими матеріалами, що висвітлюють російсько-українську війну (з 2014 по теперішній час).

Мета статті – систематизувати відомості про застосування засобів мобільного зв'язку у рамках проведення РФ інформаційно-психологічного впливу на українських військовослужбовців у зоні проведення АТО (ООС).

В інформаційно-психологічних операціях активну участь беруть: воєнно-політичне керівництво РФ, спецслужби, підрозділи психологічних операцій ЗС РФ, цивільні державні і недержавні структури, залучені до проведення інформаційних операцій, релігійні організації, проросійські сили в українському суспільстві й політикумі, проросійськи налаштовані політичні діячі окремих країн.

Для того, щоб донести до населення і українських військових російський інформаційний продукт задіяні такі канали: періодична преса (газети «Комсомольская правда», «Известия», «Российская газета», «Московский комсомолец», «КоммерсантЪ» та ін.), радіо (радіостанція «Эхо Москвы»), телебачення (телеканали «Вести», «Россия», «РТР-Планета», «Россия-24», «НТВ-Мир» та ін.), Інтернет (зокрема, соцмережі «ВКонтакте» та «Одноклассники»), чутки (Туранський, 2020, с. 153).

Основними формами впливу на військовослужбовців ЗСУ через засоби мобільного зв'язку є: розсилка повідомлень деморалізуючого характеру; визначення місцезнаходження підрозділів ЗСУ для подальшого вогневого ураження; порушення роботи системи стільникового зв'язку з використанням засобів радіоелектронної боротьби; використання мобільних телефонів як додаткового джерела витоку службової інформації; збір інформації про організаційно-штатну структуру підрозділів ЗСУ.

Через мобільні телефони окупаційні війська намагаються ідентифікувати українських військових, визначити місце розташування підрозділів ЗСУ та зброї (Дорош, 2018), а, розсилаючи українським військовослужбовцям та їх родичам SMS-повідомлення деморалізуючого змісту, здійснюють провокації у власних інтересах. Російські спецслужби прослуховували мобільні телефони українських військових в Криму і продовжують надалі це робити на сході України (Міністерство оборони України, 2014).

Російський генштаб створив спеціальний інформаційний підрозділ «Сапфір», який здійснював розсилку українським військовим листівок та SMS-повідомлень провокаційного змісту. Щоденно розсилалось понад 300 повідомлень. Розсилка таких SMS-листівок мала на

меті дискредитацію українських військових (повідомлення зі звинуваченнями командування ЗСУ у нібито приховуванні бойових втрат).

Для поширення фейкових повідомлень використовували також спеціально розроблені сайти, задіювали месенджери та електронні поштові скриньки. Було встановлено акаунти у соціальних мережах, які дана група використовувала для проникнення в інтернет-спільноти підрозділів ЗСУ, де систематично поширювала вигідні ворожій стороні фейкові матеріали, що дискредитували владу. Для розповсюдження відверто антиукраїнських позицій серед відповідної аудиторії було створено 14 відверто проросійських акаунтів і понад 70 соціальних груп (Картер, 2019).

Шляхи використання мобільних мереж противником.

Деякі компанії (МТС, Life та ін.), що надають послуги мобільного зв'язку, повністю або частково належать громадянам Росії, тому спецслужби РФ мають вільний доступ до інформації про місцезнаходження абонента та зміст переговорів.

Мали місце факти передавання інформації МТС прямо ФСБ. З жовтня 2015 року МТС уклала договір із британським телеком-оператором Vodafone. Керівництво так званої ДНР планувало захопити обладнання компанії. «Перепрошити» обладнання Vodafone під себе місцевий оператор зв'язку «Фенікс» не зміг, тому картки для «Фенікса» виготовлялися на підприємстві у Московській області. За особистим рішенням «міністра міністерства зв'язку ДНР» для оператора встановлений український код-префікс +38071 (ДОБА, 2018). Зауважимо, що оператори українського зв'язку після 2014 року не припинили свою діяльність в окупованих Донецьку і Луганську. SIM-карти Vodafone продаються без паспорта і доступні для придбання в продовольчих магазинах і кіосках (Королев, 2019).

Іншим важливим каналом використання РФ мобільних телефонів у зоні військових дій є засоби радіоелектронної боротьби. У травні 2015 року на інтернет-платформі «Informnapalm» розміщена інформація про те, що Росія направила в Донецьк ультрасучасну військову систему РБ-341В «Леєр-3», яка з 2015 року перебуває на озброєнні російської армії (ГЛАВКОМ, 2017). «Леєр-3» – це система придушення GSM-зв'язку за допомогою перешкод, що передаються з безпілотного літального апарату. Безпілотні апарати у зоні їх дії мають можливість визначати координати користувача мобільного телефону і пригнічувати мобільний зв'язок. Система передає координати та іншу інформацію для ураження артилерійськими засобами. Місцеві сепаратисти не в змозі обслуговувати таку систему. Це свідчить, що високотехнологічне озброєння не тільки надійшло з Росії, але й обслуговується їхніми військовими фахівцями (Міністерство оборони України, 2015, 2015a, 2015c, 2016).

Таким чином, «Леєр-3» не тільки може отримувати доступ до мобільних телефонів, а й визначає їх місцезнаходження з точністю до метра. Мобільні телефони пов'язуються не з однією щоглою мобільного оператора, а з емулятором, встановленим на спеціальній вантажівці (Міністерство оборони України; ГЛАВКОМ, 2017).

Під час активізації бойових дій поблизу Авдіївки з її допомогою на мобільні телефони українських захисників розсилалися провокаційні антиукраїнські SMS-повідомлення. Також через SMS-розсилки російські фахівці здійснювали інформаційно-психологічні атаки на українських військових в зоні АТО. Про це з посиланням на матеріали «InformNapalm» у 2017 році писало інформаційне агентство «AssociatedPress».

Спектр використання засобів мобільного зв'язку.

1. SMS-повідомлення. За допомогою спеціальних технічних пристроїв для поширення інформації через мобільні мережі зв'язку військовослужбовці ЗСУ періодично отримували

повідомлення, які могли впливати на них психологічно: «На Вас чекають вдома», «Залишайте позиції» (Міністерство оборони України, 2016; INSIDER, 2015). З початку бойових дій військовослужбовцям ЗСУ з невідомих телефонних номерів тисячами надходили SMS-повідомлення з погрозами та образами. Багато військовослужбовців фотографували їх, а потім розміщували у соціальних мережах. У німецькій газеті «Bild» зазначалося, що у повідомленнях, написаних виключно українською мовою, йшлося про те, що «українські солдати є лише м'ясом для своїх командирів», що «вони немов німці під Сталінградом» і «їх знайдуть тільки тоді, коли розтане сніг» (ГЛАВКОМ, 2017).

Враховуючи, що пріоритетним завданням російських спецслужб є вербування українських бійців (Картер, 2019), соціальні мережі та засоби телефонного зв'язку використовувалися як особливий канал комунікації з військовиками. Військовослужбовці ЗСУ отримували SMS-повідомлення від терористів з пропозицією високооплачуваної роботи (ЕСПРЕСО, 2015).

2. Телефонні дзвінки. З метою дестабілізації морального стану родичів бійців, почастішали випадки телефонних дзвінків їм з окупованих територій. Наприклад, дружина майора А. Кизила, який загинув у січні 2017 року, тривалий час отримувала «новини» про обставини загибелі її чоловіка. Непоодинокими є також випадки вимагання грошей за бійця, який нібито перебуває в полоні (АРМІЯ INFORM, 2020).

Розглянуті випадки інформаційного впливу на військовослужбовців ЗСУ є непоодинокими, вони пов'язані з початком АТО на території Донецької та Луганської областей і продовжуються по теперішній час з метою деморалізації військовослужбовців Збройних Сил України та зриву виконання поставлених перед ними завдань.

Робота командирів підрозділів ЗСУ щодо упередження впливу противника через засоби мобільного зв'язку на підлеглий особовий склад.

Зважаючи на можливі інформаційні загрози, окремі командири після прибуття свого підрозділу у зону АТО, забороняли особовому складу користуватися мобільними телефонами, усвідомлюючи, що смартфони здатні надсилати інформацію про географічну позицію з точністю до 5–6 метрів (Шрамович, 2015). Якщо радіоелектронна розвідка запеленгує підрозділ, то зможе побачити, де боєць несе чергування, де проходить лінія переднього краю та отримати інші відомості.

Використання засобів мобільного зв'язку в зоні проведення АТО загрожувало також прослуховуванням розмов, ознайомленням з листуванням військовослужбовців, нав'язуванням неправдивої інформації військовослужбовцям та їх родичам.

Враховуючи це, українське військове командування зосередило увагу на дотриманні режиму невикористання особовим складом, що перебував у зоні АТО (ООС), гаджетів. Під час бойових дій військовослужбовцям заборонялося мати при собі індивідуальні засоби зв'язку (мобільні пристрої). Дозволялось використовувати їх у строго відведений час і у визначеному місці під контролем командирів. В іншому випадку, для забезпечення не тільки інформаційно-психологічної, але й фізичної безпеки, дані пристрої підлягали вилученню.

У ЗСУ немає юридичної заборони на користування мобільними телефонами, водночас статтею 143 Статуту внутрішньої служби ЗСУ визначено, що порядок користування засобами мобільного зв'язку та передачі інформації військовослужбовцями, які виконують обов'язки військової служби, встановлюється командиром військової частини (Закон України…, 2015). Отже, командирам ЗСУ дозволено самостійно ухвалювати рішення про можливість користуватися мобільними телефонами в зоні АТО (Міністерство оборони України, 2015, 2016).

Якщо з певних причин неможливо відмовитися від використання мобільного телефона у зоні бойової операції, то, як радять досвідчені військові, у крайньому випадку як виняток можна придбати SIM-карту безпосередньо в зоні проведення АТО (ООС). Це не дозволить встановити, звідки приїхав військовослужбовець, оскільки за номером можна дізнатися лише, в якій області активований мобільний телефон (Міністерство оборони України, 2015а). Водночас, приховати своє місцезнаходження шляхом зміни телефону або SIM-карти після прибуття в зону АТО (ООС) неможливо, оскільки мобільний телефон постійно надсилає сигнали на базову станцію. Достатньо однієї вечірньої розмови з рідними чи близькими, прослуханої противником, щоб ідентифікувати військовослужбовця (Пєвцов та ін. 2014а). Неможливо приховати маршрут пересування або місцезнаходження базового табору чи скупчення військових. Тому ворогу зовсім нескладно здійснити прицільний артобстріл.

Досвід проведення АТО (ООС) дозволяє виокремити основні причини неефективної протидії негативному інформаційному та психологічному впливу на особовий склад ЗСУ:

– неготовність командирів військових частин організовувати бойову діяльність в умовах негативного інформаційно-психологічного впливу, проводити масштабні інформаційно-психологічні операції, пропагандистські компанії та, як результат, низька психологічна готовність особового складу (перш за все, того, який прибув з резерву) до виконання службових обов'язків;

– недостатня підготовка та психологічна готовність особового складу діяти у нестандартних умовах і, як результат, відсутність рішучості, ініціативи, здатності мислити і діяти у складних умовах;

– слабка система захисту особового складу та населення від негативного інформаційного і психологічного впливу ворога, відсутність ефективної ієрархічної структури планування та здійснення інформаційно-психологічної протидії;

– відсутність позитивної взаємодії із правоохоронними органами в кризових регіонах України;

– неефективне вирішення соціально-побутових проблем персоналу та їх сімей через недосконаліть нормативно-правової бази та цільового фінансування.

За результатами проведеного дослідження можна зробити такі висновки:

Одним із напрямків зовнішнього впливу РФ на військовослужбовців ЗСУ є інформаційно-психологічний вплив через засоби мобільного зв'язку шляхом розсилки повідомлень деморалізуючого характеру; визначення місцезнаходження підрозділів ЗСУ для подальшого вогневого ураження; порушення роботи системи стільникового зв'язку з використанням засобів радіоелектронної боротьби; використання мобільних телефонів як додаткового джерела витоку службової інформації; збір інформації про організаційно-штатну структуру підрозділів ЗСУ. Під час бойових дій військовослужбовцям заборонялося мати при собі індивідуальні засоби зв'язку (мобільні пристрої) й інформації. Ці засоби використовувались під контролем командирів у строго відведений час і у визначеному місці.

У подальших наукових розвідках доцільно дослідити роботу всіх мобільних операторів, які діють на тимчасово непідконтрольній Україні території, їх вплив на інформаційний простір у зоні бойових дій та морально-психологічний стан військовослужбовців.

Бібліографічний список

АРМІЯ INFORM, 2020. *Мобільні телефони для військовослужбовців: заборонити не можна користуватися* [online]. Доступно: <https://armyinform.com.ua/2020/07/mobilni-telefony-dlya-vijskovosluzhbovcziv-zaboronyty-ne-mozhna-korystuvatysya/> [Дата звернення 28 січня 2022].

ГЛАВКОМ, 2017. *Розсилати українським військовим на Донбасі СМС з погрозами могли тільки російські фахівці – Bild* [online]. Доступно: <https://glavcom.ua/news/rozsilati-ukrajinskim-viyskovim-na-donbasi-sms-z-pogrozami-mogli-tilki-rosiyski-fahivci-bild-396192.html> [Дата звернення 3 лютого 2022].

Горбулін, В., 2015. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. *Дзеркало тижня Україна*, 23 січня, с. 2.

ДОБА, 2018. *Військовим на Сході погрожують в СМС, мобільний оператор зливає інформацію (фотофакт)* [online]. Доступно: <https://doba.te.ua/post/12946> [Дата звернення 3 лютого 2022].

Дорош, С., 2018. Дзвонити в Донецьк через Ростов: що зі зв'язком на Донбасі? [online]. *BBC News Україна.* Доступно: <https://www.bbc.com/ukrainian/features-43556986> [Дата звернення 1 лютого 2022].

ЕСПРЕСО, 2015. *Бойовики пропонують через SMS українським військовим високооплачувану роботу*. [online] Доступно: <https://espreso.tv/news/2015/10/22/boyovyky_proponuyut_cherez_sms_ukrayinskym_viyskovym_vysokooplachuvanu_robotu> [Дата звернення 28 січня 2022].

Закон України «Про внесення зміни до статті 143 Статуту внутрішньої служби Збройних Сил України» від 1 липня № 568-VIII, 2015. *Верховна Рада України* [online]. Доступно: <https://zakon.rada.gov.ua/laws/show/568-19#Text> [Дата звернення 25 січня 2022].

Картер, С., 2019. *«Сапфір» розсилав українським військовим фейки та погрози* [online]. *УНН.* Доступно: <https://www.unn.com.ua/uk/news/1785786-sapfir-rozsilav-ukrayinskim-viyskovim-feyki-ta-pogrozi> [Дата звернення 1 лютого 2022].

Конах, В., 2004. Роль інформаційних операцій та інформаційних воєн у державній політиці США. *Стратегічна панорама*, 1, с. 164–169.

Королев, И., 2019. Как ДНР построила себе «российский 4G», и почему ЛНР держится за украинский CDMA. *CNews* [online]. Доступно: <https://www.cnews.ru/news/top/2019-05-02_kak_dnr_postroila_sebe_rossijskij_4gi_pochemu> [Дата звернення 3 лютого 2022].

Міністерство оборони України, 2014. *Спецслужби РФ розсилають українським військовим провокаційні SMS*. [online] Доступно: <https://www.mil.gov.ua/news/2014/04/15/speczsluzhbi-rf-rozsilayut-ukrainskim-vijskovim-provokaczijni-sms/> [Дата звернення 3 лютого 2022].

Міністерство оборони України, 2015. *Аналіз бойових дій в районі Іловайська після вторгнення російських військ 24-29 серпня 2014 року*. [online] Доступно: <http://www.mil.gov.ua/news/2015/10/19/analiz-illovausk--14354/> [Дата звернення 1 лютого 2022].

Міністерство оборони України, 2015а. *Аналіз бойових дій на сході України в ході зимової кампанії 2014-2015 років.* [online] Доступно: <http://www.mil.gov.ua/news/2015/12/23/analiz-bojovih-dij-na-shodi-ukraini-v-hodi-

zimovoi-kampanii-2014%E2%80%932015-rokiv--16785/> [Дата звернення 1 лютого 2022].

Міністерство оборони України, 2016. *Кібербезпека. Аспект 2: мобільні телефони*. [online] Доступно: <https://www.mil.gov.ua/ukbs/> [Дата звернення 1 лютого 2022].

Міністерство оборони України, 2016a. *Правила інформаційної та кібернетичної безпеки в зоні проведення АТО*. [online] Доступно: <https://www.mil.gov.ua/ukbs/pravila-informaczijnoi-ta-kibernetichnoi-bezpeki-v-zoni-provedennya-ato.html> [Дата звернення 1 лютого 2022].

Пєвцов, Г., Гордієнко, А., Залкін, С., Сідченко, С. та Хударковський, К., 2016. Методика оцінювання ефективності виконання заходів протидії негативному інформаційно-психологічному впливу противника. *Збірник наукових праць Харківського університету Повітряних Сил*, 1(46), с. 23–28. Харків: ХУПС.

Пєвцов, Г., Гордієнко, А., Залкін, С., Сідченко, С., Феклістов, А. та Хударковський, К., 2017. *Інформаційно-психологічна боротьба у воєнній сфері : монографія.* Харків: Вид. Рожко С. Г.

Пєвцов, Г., Залкін, С., Сідченко С., Хударковський, К.І. та Гордієнко, А.М., 2014a. Реалізація підходів інформаційної війни Російською Федерацією в сучасному інформаційному просторі України. *Наука і техніка Повітряних Сил*, 2(15), с. 10–13.

Пєвцов, Г., Залкін, С., Сідченко, С. та Хударковський, К., 2014b. *Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення.* Харків: Цифрова друкарня № 1.

Пєвцов, Г., Залкін, С., Сідченко, С. та Хударковський, К., 2015. Інформаційно-психологічні операції Російської Федерації в Україні: моделі впливу та напрями протидії. *Наука і оборона*, 2, с. 28–32. Київ : Видавничий дім “Стилос”

Пєвцов, Г., Залкін, С., Сідченко, С. та Хударковський, К., 2016a. Методичний підхід до аналізу інформаційно-психологічної операції противника. *Наука і оборона*, 3, с. 27–31. Київ : Видавничий дім “Стилос”

Пєвцов, Г. В., Залкін, С. В., Сідченко, С. О., Хударковський, К. І., Феклістов, А. О. та Антонов, А. В., 2014. Основні особливості ознак проведення інформаційно-психологічної операції Російської Федерації в автономній республіці Крим. *Наука і техніка Повітряних Сил*, 1(14), с. 35–37.

Пєвцов, Г.В., Залкин, С.В. та Феклістов, А.О., 2011. Концептуальні підходи щодо забезпечення інформаційної безпеки у воєнній сфері. *Системи обробки інформації,* 2(92), с. 57–59.

Руснак, І.С. та Телелим, В.М., 2000. Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі. *Наука і оборона*. 2, с. 18–23.

Туранський, М.О., 2020. *Інформаційно-психологічне забезпечення операції з анексії Криму Російською Федерацією: історичні передумови та практична реалізація*. Доктор наук. Дисертація. Національна академія сухопутних військ імені гетьмана Петра Сагайдачного. Інститут українознавства імені Івана Крип’якевича Національної академії наук України. Львів.

Шрамович, В., 2015. Чому солдатам заборонили користуватися телефонами [online]. *BBC News Україна.* Доступно: <https://www.bbc.com/ukrainian/society/2015/07/150701_cell_phones_ato_zone_ban_vs> [Дата звернення 1 лютого 2022].

INSIDER, 2015. *Сепаратисти шлють бійцям ЗСУ на передовій провокативні СМСки*. [online] Доступно: <http://www.theinsider.ua/politics/54d7571740015/> [Дата звернення 28 січня 2022].

References

ARMIIA INFORM, 2020. *Mobilni telefony dlia viiskovosluzhbovtsiv: zaboronyty ne mozhna korystuvatysia* [*Mobile phones for servicemen: can not be banned]* [online] Available at: <https://armyinform.com.ua/2020/07/mobilni-telefony-dlya-vijskovosluzhbovcziv-zaboronyty-ne-mozhna-korystuvatysya/> [Accessed 28 January 2022] (in Ukrainian).

DOBA, 2018. *Viiskovym na Skhodi pohrozhuiut v SMS, mobilnyi operator zlyvaie informatsiiu (fotofakt) [The military in the East is threatened by SMS, the mobile operator is leaking information (photo fact)]* [online]. Available at: <https://doba.te.ua/post/12946> [Accessed 3 February 2022]. (in Ukrainian).

Dorosh, S., 2018. Dzvonyty v Donetsk cherez Rostov: shcho zi zviazkom na Donbasi? [Calling Donetsk via Rostov: what about communication in Donbass?] [online]. *BBC News Ukraina*. Available at: <https://www.bbc.com/ukrainian/features-43556986> [Accessed 1 February 2022]. (in Ukrainian).

ESPRESO, 2015. *Boiovyky proponuiut cherez SMS ukrainskym viiskovym vysokooplachuvanu robotu [Militants offer high-paying jobs to the Ukrainian military via SMS]*. [online] Available at: <https://espreso.tv/news/2015/10/22/boyovyky_proponuyut_cherez_sms_ukrayinskym_viyskovym_vysokooplachuvanu_robotu> [Accessed 28 January 2022]. (in Ukrainian).

GLAVKOM, 2017. *Rozsylaty ukrainskym viiskovym na Donbasi SMS z pohrozamy mohly tilky rosiiski fakhivtsi – Bild [Only Russian specialists could send threatening SMS to the Ukrainian military in Donbass – Bild]* [online]. Available at: <https://glavcom.ua/news/rozsilati-ukrajinskim-viyskovim-na-donbasi-sms-z-pogrozami-mogli-tilki-rosiyski-fahivci-bild-396192.html> [Accessed 3 February 2022] (in Ukrainian).

Horbulin, V., 2015. «Hibrydna viina» yak kliuchovyi instrument rosiiskoi heostratehii revanshu ["Hybrid War" as a key tool of n geostrategy of revenge]. *Dzerkalo tyzhnia Ukraina*, 23, p.2 (in Ukrainian).

INSIDER, 2015. *Separatysty shliut biitsiam ZSU na peredovii provokatyvni SMSky [Separatists send provocative text messages to the Armed Forces on the front line]* [online]. Available at: <http://www.theinsider.ua/politics/54d7571740015/> [Accessed 28 January 2022]. (in Ukrainian).

Karter, S., 2019. «Sapfir» rozsylav ukrainskym viiskovym feiky ta pohrozy [Sapphire sent fakes and threats to the Ukrainian military] [online]. *UNN*. Available at: <https://www.unn.com.ua/uk/news/1785786-sapfir-rozsilav-ukrayinskim-viyskovim-feyki-ta-pogrozi> [Accessed 1 February 2022]. (in Ukrainian).

Konakh, V., 2004. Rol informatsiinykh operatsii ta informatsiinykh voien u derzhavnii politytsi SShA [The role of information operations and information wars in US public policy]. *Stratehichna panorama,* 1, pp. 164–169. (in Ukrainian).

Korolev, I., 2019. Kak DNR postroyla sebe «rossyiskyi 4G», y pochemu LNR derzhytsia za ukraynskyi CDMA [How the DNR built itself a "Russian 4G", and why the LNR is holding on to the Ukrainian CDMA] [online]. *CNews.* Available at: <https://www.cnews.ru/news/top/2019-05-

02_kak_dnr_postroila_sebe_rossijskij_4gi_pochemu> [Accessed 3 February 2022]. (in Ukrainian).

Ministerstvo oborony Ukrainy, 2016. *Kiberbezpeka. Aspekt 2: mobilni telefony [Cybersecurity. Aspect 2: mobile phones]* [online]. Available at: <https://www.mil.gov.ua/ukbs/> [Accessed 1 February 2022]. (in Ukrainian).

Ministerstvo oborony Ukrainy, 2016a. *Pravyla informatsiinoi ta kibernetychnoi bezpeky v zoni provedennia ATO [Rules of information and cyber security in the area of anti-terrorist operation]* [online]. Available at: <https://www.mil.gov.ua/ukbs/pravila-informaczijnoi-ta-kibernetichnoi-bezpeki-v-zoni-provedennya-ato.html> [Accessed 1 February 2022] (in Ukrainian).

Ministry of Defense of Ukraine, 2014. *Russian special services send provocative SMS to the Ukrainian military*. [online] Available at: <https://www.mil.gov.ua/news/2014/04/15/speczsluzhbi-rf-rozsilayut-ukrainskim-vijskovim-provokaczijni-sms/> [Accessed 3 February 2022]. (in Ukrainian).

Ministry of Defense of Ukraine, 2015. *Analysis of hostilities in the Ilovaisk region after the invasion of Russian troops on August 24-29, 2014*. [online] Available at: <http://www.mil.gov.ua/news/2015/10/19/analiz-illovausk--14354/> [Accessed 1 February 2022]. (in Ukrainian).

Ministry of Defense of Ukraine, 2015a. *Analysis of hostilities in eastern Ukraine during the winter campaign of 2014-2015*. [online] Available at: <http://www.mil.gov.ua/news/2015/12/23/analiz-bojovih-dij-na-shodi-ukraini-v-hodi-zimovoi-kampanii-2014%E2%80%932015-rokiv--16785/> [Accessed 1 February 2022]. (in Ukrainian).

Pievtsov, H., Hordiienko, A., Zalkin, S., Sidchenko, S. and Khudarkovskyi, K., 2016. Metodyka otsiniuvannia efektyvnosti vykonannia zakhodiv protydii nehatyvnomu informatsiino-psykholohichnomu vplyvu protyvnyka [Methods for evaluating the effectiveness of measures to counter the negative information and psychological influence of the enemy]. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl*, 1(46), pp.23–28. Kharkiv: KhUPS. (in Ukrainian).

Pievtsov, H., Hordiienko, A., Zalkin, S., Sidchenko, S., Feklistov, A. and Khudarkovskyi, K., 2017. *Informatsiino-psykholohichna borotba u voiennii sferi [Information and psychological struggle in the military sphere]*. Kharkiv: Rozhko S.H. (in Ukrainian).

Pievtsov, H., Zalkin, S., Sidchenko, S. and Khudarkovskyi, K., 2014b. *Informatsiina bezpeka u voiennii sferi: problemy, metodolohiia, systema zabezpechennia [Information security in the military sphere: problems, methodology, support system]*. Kharkiv: Tsyfrova drukarnia № 1. (in Ukrainian).

Pievtsov, H., Zalkin, S., Sidchenko, S. and Khudarkovskyi, K., 2016a. Metodychnyi pidkhid do analizu informatsiino-psykholohichnoi operatsii protyvnyka [Methodical approach to the analysis of information and psychological operation of the enemy]. *Nauka i oborona*, 3, pp. 27–31. Kyiv : Vydavnychyi dim “Stylos” (in Ukrainian).

Pievtsov, H. V., Zalkin, S. V., Sidchenko, S. O., Khudarkovskyi, K. I., Feklistov, A. O. ta Antonov, A. V., 2014. Osnovni osoblyvosti oznak provedennia informatsiino-psykholohichnoi operatsii Rosiiskoi Federatsii v AR Krym [The main features of the signs of the information and psychological operation of the Russian Federation in the

Autonomous Republic of Crimea]. *Nauka i tekhnika Povitrianykh Syl*, 1(14), pp. 35–37 (in Ukrainian).

Pievtsov, H., Zalkin, S., Sidchenko, S. and Khudarkovskyi, K., 2015. Information and psychological operations of the Russian Federation in Ukraine: models of influence and directions of counteraction [Informatsiino-psykholohichni operatsii Rosiiskoi Federatsii v Ukraini: modeli vplyvu ta napriamy protydii]. *Nauka i oborona*, 2, pp. 28–32. Kyiv : Vydavnychyi dim "Stylos" (in Ukrainian).

Pievtsov, H., Zalkin, S., Sidchenko, S., Khudarkovskyi, K.I. ta Hordiienko, A.M., 2014a. Realizatsiia pidkhodiv informatsiinoi viiny Rosiiskoiu Federatsiieiu v suchasnomu informatsiinomu prostori Ukrainy [Implementation of information warfare approaches by the Russian Federation in the modern information space of Ukraine]. *Nauka i tekhnika Povitrianykh Syl*, 2(15), pp.10–13. (in Ukrainian).

Pievtsov, H.V., Zalkyn, S.V. ta Feklistov, A.O., 2011. Kontseptualni pidkhody shchodo zabezpechennia informatsiinoi bezpeky u voiennii sferi [Conceptual approaches to information security in the military sphere]. *Systemy obrobky informatsii*, 2(92), pp.57–59. (in Ukrainian).

Rusnak, I.S. ta Telelym, V.M., 2000. Rozvytok form i sposobiv vedennia informatsiinoi borotby na suchasnomu etapi [Development of forms and methods of information struggle at the present stage]. *Nauka i oborona*, 2, pp.18–23 (in Ukrainian).

Shramovych, V., 2015. Chomu soldatam zaboronyly korystuvatysia telefonamy [Why soldiers were forbidden to use telephones] [online]. *BBC News Ukraina*. Available at: <https://www.bbc.com/ukrainian/society/2015/07/150701_cell_phones_ato_zone_ban_vs > [Accessed 1 February 2022]. (in Ukrainian).

Turanskyi, M.O., 2020. *Informatsiino-psykholohichne zabezpechennia operatsii z aneksii Krymu Rosiiskoiu Federatsiieiu: istorychni peredumovy ta praktychna realizatsiia [Information and psychological support of the operation for the annexation of Crimea by the Russian Federation: historical background and practical implementation]*. Ph.D. Dissertation. Hetman Petro Sagaidachny National Academy of Land Forces, Ivan Krypyakevych Institute of Ukrainian Studies of the National Academy of Sciences of Ukraine. (in Ukrainian).

Zakon Ukrainy «Pro vnesennia zminy do statti 143 Statutu vnutrishnoi sluzhby Zbroinykh Syl Ukrainy» vid 1 lypnia № 568-VIII [*Law of Ukraine "On Amendments to Article 143 of the Statute of the Internal Service of the Armed Forces of Ukraine" of July 1 № 568-VIII]* [online], 2015. *Verkhovna Rada Ukrainy*. Available at: <https://zakon.rada.gov.ua/laws/show/568-19#Text> [Accessed 25 January 2022] (in Ukrainian).

Стаття надійшла до редакції 18.02.2022 р.

V. Lehkodukh

ANALYSIS OF THE EXTERNAL INFLUENCE OF THE ENEMY ON THE MILITARY SERVANTS OF THE ARMED FORCES OF UKRAINE THROUGH MOBILE

The article examines the external influence of the Russian Federation (RF) on servicemen of the Armed Forces of Ukraine (AFU) through mobile communications. The purpose of the article

is to systematize information on the use of mobile communications in the framework of the Russian Federation information and psychological impact on Ukrainian servicemen in the area of the Anti-Terrorist Operation (ATO). It was emphasized that the active influence on the servicemen of the Armed Forces of Ukraine by the units of the information operations of the Armed Forces of the Russian Federation is connected with the beginning of the Anti-Terrorist Operation (ATO) in Donetsk and Luhansk regions and continues to this day. The main forms of influence on the servicemen of the Armed Forces of Ukraine through the means of mobile communication are highlighted: sending messages of a demoralizing nature; determining the location of units of the Armed Forces for further fire damage; disruption of the cellular communication system with the use of electronic warfare; use of mobile phones as an additional source of leaks of official information; collecting information on the organizational and staffing structure of the Armed Forces. In order to demoralize the servicemen of the Armed Forces of Ukraine and disrupt the tasks assigned to them, SMS messages with threats and insults and telephone calls to the military and their relatives are actively used. The main ways of using mobile networks by the enemy, which give access to the intelligence services of the Russian Federation to information about the location of the subscriber: through the activities of companies providing mobile services that are wholly or partly owned by Russian citizens; through means of electronic warfare (military system RB-341V "Leer-3", which suppresses GSM communications through interference transmitted from unmanned aerial vehicles). The work of the commanders of the units of the Armed Forces of Ukraine on preventing the influence of the enemy through the means of mobile communication on Ukrainian soldiers is outlined. It was found out that during the fighting in the ATO (OOS) zone, servicemen were forbidden to carry individual means of communication (mobile devices) and information. These tools were used under the control of commanders at a strictly allotted time and place.

Key words: *anti-terrorist operation, means of mobile communication, servicemen, Armed Forces of Ukraine, information and psychological influence.*