МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
Національний університет оборони України
Інститут стратегічних комунікацій

СТРАТЕГІЧНІ КОМУНІКАЦІЇ У СФЕРІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ: ПРОБЛЕМИ, ДОСВІД, ПЕРСПЕКТИВИ

IV МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

27 вересня 2023 року

ТЕЗИ ДОПОВІДЕЙ

Київ – 2023

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
Національний університет оборони України

Інститут стратегічних комунікацій

СТРАТЕГІЧНІ КОМУНІКАЦІЇ У СФЕРІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ: ПРОБЛЕМИ, ДОСВІД, ПЕРСПЕКТИВИ

IV Міжнародна науково-практична конференція
27 вересня 2023 року

ТЕЗИ ДОПОВІДЕЙ

Видання університету
2023

УДК: 355.451

Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи : IV міжнар. наук.-практ. конф., 27 верес. 2023 р.: тези доповідей / Міністерство оборони України, НУОУ. К.: НУОУ, 2023. 406 с.

До збірника увійшли тези доповідей, що містять теоретичні та практичні результати наукових досліджень і розробок учасників міжнародної науково-практичної конференції, присвячені проблемам інформаційної безпеки та розбудови стратегічних комунікацій.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Голова організаційного комітету:
ВОЙТКО О.В., кандидат військових наук, доцент
Заступник голови організаційного комітету:
ЄРГІДЗЕЙ К.В., кандидат педагогічних наук
Члени організаційного комітету:
ФЕДОРІЄНКО В.А., кандидат технічних наук *(головний модератор конференції)*
ІЖУТОВА І.В., кандидат наук з державного управління *(модератор конференції)*
КАМИШЕНЦЕВ Г.В., доктор технічних наук
СІВОХА І.М.
Секретар:
ТЮТЮННИК Л.Л. доктор філософії
Технічне супроводження:
ЛАШИН Я.О.
ТУРЧЕНКО Д.В.

Затверджено протоколом та схвалено до друку на засіданні інституту стратегічних комунікацій Національного університету оборони України (протокол № 12 від 29 вересня 2023 року).

За достовірність наданого матеріалу, фактів, цитат та інших відомостей відповідальність несуть автори.

ЗМІСТ

ВСТУПНЕ СЛОВО
генерал-полковника Михайла КОВАЛЯ,
начальника Національного університету оборони України,
доктора військових наук

Вельмишановні учасники конференції!

Щиро вітаємо вас з початком роботи четвертої міжнародної науково-практичної конференції *"Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи"*.

Сучасні реалії нелінійної війни, яку розв'язала російська федерація проти України, щоразу висувають нові вимоги до організації системи стратегічних комунікацій. Вістря цієї війни спрямоване насамперед в інформаційний простір нашої країни з метою впливу на всі сфери життєдіяльності нашої держави, зокрема: суспільно-політичну та економічну. Це потужний інструмент дестабілізації українського суспільства з боку агресора.

Сьогодні інформація є головною зброєю міжнаціонального та міждержавного протистояння, що відкриває величезні можливості для ефективного маніпулювання людьми, їх цінностями, нормами та настановами, здатна розпалювати міжрелігійні та міжнаціональні конфлікти, викликати ненависть за мовною, етнічною, релігійною та іншими ознаками, спонукати до порушення територіальної цілісності держави та поширювати сепаратистські заклики.

Воєнні події останніх десяти років стали досить повчальними для України й позначились безцінним досвідом у сфері розбудови системи стратегічних комунікацій, яким ми маємо змогу обмінятися з колегами в межах роботи конференції.

Дуже приємно, що наше запрошення прийняли визнані експерти з питань стратегічних комунікацій держав-членів НАТО і партнерів та високоповажні фахівці з різних куточків України.

Шановні колеги! Ми раді вітати кожного з вас на цьому заході і впевнені, що сьогодні ми визначимо та обговоримо основні проблемні питання щодо розвитку системи стратегічних комунікацій та інформаційної безпеки, а також запропонуємо конструктивні та ефективні напрями їх вирішення.

Щиро вітаємо вас з початком роботи IV міжнародної науково-практичної конференції. Бажаємо усім нам плідної співпраці, творчого натхнення, продуктивного обміну досвідом, позитивних вражень, цікавих ідей та найшвидшої реалізації результатів досліджень!

Слава Україні! Glory to Ukraine!

ВСТУПНЕ СЛОВО
полковника Олександра ВОЙТКА,
начальника інституту стратегічних комунікацій
кандидата військових наук, доцента

Шановні учасники конференції!

Щиро вітаємо вас на міжнародній науково-практичній конференції *"Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи",* яку ми традиційно, уже вчетверте, проводимо у Національному університеті оборони України. Цей захід проходить на базі нашого підрозділу, який ще зовсім недавно був Навчально-науковим центром стратегічних комунікацій у сфері забезпечення національної безпеки та оборони, а зараз трансформувався в Інститут стратегічних комунікацій. Це вкотре доводить значимість стратегічних комунікацій для забезпечення національної безпеки та оборони нашої держави.

Сьогодні, коли в умовах відбиття широкомасштабної збройної агресії росії Сили оборони України ведуть героїчну боротьбу щодо захисту суверенітету, територіальної цілісності нашої держави та звільнення тимчасово окупованих територій, наша держава та весь цивілізований світ стоять перед загрозами, зокрема, породженими навалою російської пропаганди та дезінформації. Ця проблематика набуває все більших масштабів, а засоби, які застосовує ворог, стають більш витонченими, підступними і завуальованими.

Як говорив канадський дослідник Herbert Marshall McLuhan: "Істинно тотальна війна – це війна за допомогою інформації" яку и й спостерігаємо сьогодні. А успішна боротьба в ній потребує ефективних методів протидії російським інформаційним і психологічним операціям та дієвих інструментів комунікування з власним суспільством.

Дуже приємно, що на наше запрошення відгукнулось багато закордонних та вітчизняних визначних науковців, політиків, військовослужбовців, цивільних. Ваш досвід наразі є надзвичайно потрібним і важливим.

Ми віримо в те, що робота конференції буде цікавою і продуктивною. Бажаємо усім плідної роботи, ефективного обміну безцінним досвідом, нових важливих знайомств та позитивних вражень.

СЕКЦІЯ 1: ПУБЛІЧНА ДИПЛОМАТІЯ

Sergiy GERASYMCHUK
Foreign Policy Council "Ukrainian Prism"
Deputy Executive Director
E-mail: gerasymchuk@prismua.org

THE ROLE OF THINK TANKS IN PUBLIC DIPLOMACY: OPPORTUNITIES AND CHALLENGES AT THE TIME OF WAR

Amidst the crucible of geopolitical turmoil, the role of think tanks has emerged as an increasingly vital force shaping the narratives and strategies that underpin international relations. As the world grapples with the complexities of modern warfare, the influence wielded by these intellectual powerhouses extends far beyond the confines of academia. Think tanks have evolved into dynamic agents of public diplomacy, acting as crucial intermediaries between governments, civil society, and the global public. Their profound impact on shaping public opinion, policy agendas, and diplomatic initiatives cannot be overstated. From shaping policy to fostering dialogue, think tanks have assumed a pivotal role in the pursuit of peaceful resolutions and the advancement of diplomatic efforts amid turbulent times.

For the sake of the fulfillment of their mission think tanks use a number of channels to make their findings public, to deliver them to the target audience of the decision makers and to convert them into the political decisions. In certain cases they refer directly to the policy-makers, but also in some cases they use media and society as the mediators and channels of influence. As correctly summarized by James G. McGann [1], think tanks employ a wide range of methods to accomplish the vital goal of effectively propagating information, including:

a) In times of war, platforms like think tanks play a pivotal role in delivering crucial messages, persuading foreign partners regarding the necessity of their assistance, and bringing together decision-makers, media, and academia. One prominent avenue for this engagement is through seminars, conferences, and briefings. These public events serve as invaluable opportunities for think tanks to present their research findings and disseminate them to a wider audience. This dissemination, in turn, serves to shape public opinion, providing a lever of influence aimed at decision-makers and policy shapers. Furthermore, public events offer a platform for constructive dialogue among various stakeholders, including academicians, interest groups, and politicians. At times, they even serve as independent arenas for the exchange of opinions that might not find expression through official channels.

b) Publications: in times of war, the information provided by think tanks garners greater trust and often commands more attention, owing to the reputable standing they

hold. Some think tanks extend their influence through specialized information services distributed via emails or tweets, offering insightful commentary on the day's political and economic developments. Furthermore, most think tank websites feature an array of resources including speeches, commentaries authored by their fellows, comprehensive conference reports, and increasingly, multimedia content such as video and audio clips, as well as various visualizations. These diverse channels serve as vital conduits for disseminating critical knowledge and shaping public discourse during times of war.

c) The media: Journalists often profit from the expertise of think tank employees. In turn, the think tank and the expert concerned gain a wide forum for the opinion expressed – and sometimes even certain renown because of the direct media exposure. Think tank analysts are quoted as experts in the print media and appear on television and radio news programs as well as on talk shows. Their access to the foreign media in the time of war is an asset for the state.

d) Relations with government agencies: In case of the US think tanks are particularly concerned with maintaining lines of communication to members of Congress and their staff, administration officials, federal judges, and representatives from state and local bodies. In turn, government officials and members of Congress are invited to speak at think tank events, which provide them with opportunities to test out political ideas or initiatives on "neutral ground" in front of an audience of experts. (This seems to be the direct and the most efficient channel of communication with the decision-makers and government. However, it should be noted that such a channel is affordable mostly for the influential think tanks with high budgets and prevailingly in the US whereas in the European Union such a pattern of communication is used seldom and foresees a number of conditions (e.g. office in Brussels is desperately needed to set the channel of influence on the European decision-makers [2]).

Resuming the abovementioned channels and features of think tanks we may come to the conclusion that the think tank is an independent organization, which focuses primarily on the policy research related to the public needs (mostly but not exclusively in the field of economics, international relations etc.) and by different channels (including some sort of shaping public opinion on the issue by means of public events, publications and media coverage) makes the outcomes of this research/policy oriented solution available to the policy-makers to be considered while elaborating the respective policies and further makes the assessment of this policy through the lens of its relevance to the initial public need.

n times of geopolitical turmoil and modern warfare, think tanks have emerged as influential forces shaping international relations beyond the realms of academia. Serving as intermediaries between governments, civil society, and the global public, their impact on public opinion, policy agendas, and diplomatic initiatives is profound. This article explores the multifaceted role of think tanks in navigating international conflicts, illuminating their pivotal contribution to peaceful resolutions and diplomatic efforts amid turbulent times.

To fulfill their mission, think tanks employ various channels to disseminate findings, influence decision-makers, and shape political decisions. They utilize platforms such as seminars, conferences, and briefings, acting as crucial conduits for delivering crucial messages and persuading foreign partners to provide necessary assistance. These public events not only present research findings but also foster constructive dialogues among stakeholders, including academicians, interest groups, and politicians. Furthermore, think tanks leverage publications, harnessing their reputable standing during times of war to disseminate information via specialized services, emails, or tweets, offering insightful commentary on political and economic developments.

The media also plays a vital role, as journalists often seek expertise from think tank employees, providing a wide forum for opinions. Think tank analysts are quoted as experts in various media outlets, enhancing their visibility and influence. Additionally, think tanks maintain essential lines of communication with government agencies, enabling them to engage with members of Congress, administration officials, and other key figures. This two-way interaction allows for the exchange of political ideas and initiatives on neutral ground, providing valuable insights for policy-makers.

In summary, Ukrainian think tanks operate as independent organizations focused on policy research, primarily addressing public needs, particularly in areas like economics and international relations In the time of war. Through a diverse array of channels, including public events, publications, media coverage, and government relations, think tanks bridge the gap between research outcomes and policy-making, ensuring that policies align with the initial public needs, in particular emerging in the times of war and are continually assessed for their relevance. During times of war, their role becomes even more indispensable, serving as instrumental instruments for promoting national interests on the international stage and establishing alternative diplomatic tracks in regions overlooked by the government.

Список використаних джерел:

1. James G. McGann, Think Tanks and Policy Advice in The US. www.kas.de/wf/doc/kas_7042-544-1-30.pdf.

2. NOTRE EUROPE, Etudes & Recherchers, Studies and Research n°35, Europe and its think tanks : a promise to be fulfilled. An analysis of think tanks specialised in European policy issues in the enlarged European Union, Directed by Stephen BOUCHER.

Михайло БЛАВІЦЬКИЙ
E-mail: m_blav@tntu.edu.ua
Валерій ЛАЗАРЮК, канд. техн. наук, доц.,
доцент кафедри МТ
ТНТУ ім. Івана Пулюя
ORCID: 0000-0003-3731-2828
E-mail: lazaryuk@gmail.com

ГРОМАДСЬКА ДИПЛОМАТІЯ ЯК ІНСТРУМЕНТ ПРОТИДІЇ РОСІЙСЬКІЙ ГІБРИДНІЙ АГРЕСІЇ

Причина злочинної діяльності російської федерації є збереження її колоніальної політики загарбання та експлуатації за допомогою військового, політичного та економічного примусу народів. Жорстокість російсько-української війни обумовлюється намаганням монополізувати вільний світовий ринок через власну гегемонію шляхом прямого грабунку, вбивства та викрадення населення.

Гібридний характер російської агресії тривалий час мав прихований характер передусім у соціальному, фінансово-економічному та інформаційному вимірах з чисельними пропагандистськими та інформаційно-психологічними операціями для впливу на громадську думку як на локальному рівні та і в світі.

Сучасний розвиток економіки світових наддержав засновано на інформаційних технологіях, на глобальному цілодобовому механізмі ведення бізнесу. Розвиток засобів комунікації привів до того, що інформаційні технології стали новим ресурсом держав для отримання конкурентних переваг та вигод при завоюванні нових ринків збуту та споживачів. Проте стирання кордонів створило широкі можливості і для маніпулятивного впливу на свідомість населення, передусім країн з близькими мовними та культурними ознаками. Вразливість інформаційного процесу при цьому привело до створення інформаційних засобів боротьби з будь-ким за будь-які ідеї. Основним інструментом гібридної війни є ініціювання та підтримання державою-агресором в іншій державі, обраній для агресії, внутрішніх протиріч і конфліктів. При цьому сторона-агресор зазвичай публічно заперечує свою причетність до розв’язаного конфлікту, ретельно маскує його справжній перебіг та ініціаторів.

Міжнародний інформаційний обмін включає не лише засоби офіційної дипломатії, але і недержавні форми відносин дипломатії. Такі недержавні форми проведення міжнародного співробітництва, більш послідовні та вільні у виборі способів комунікації у своїй країні. Функціями для здійснення громадської дипломатії потенційно наділений будь-який суб’єкт, який має право на міжнародне співробітництво. Суб’єктами громадської дипломатії можуть бути окремі громадяни, громадські організації, заклади вищої освіти. Перші дії у визнанні України, як держави на міжнародній арені, були зроблені саме через

активну підтримку української діаспори, та з боку підтримки тих країн, етнічні представники яких проживають на території нашої держави.

Станом на 2010 рік за межами України мешкало до 10 млн. українців. Серед розвинутих країн багатих на українську діаспору, таких як США та Канада, додалися також Чехія, Португалія, Польща, Франція, Латвія, Естонія, Литва, Велика Британія, Австрія та Хорватія.

Порівняно з іншими світовими діаспорами, українські громади мали найбільшу кількість різних громадських об'єднань (за приблизними підрахунками – близько 3 тисяч). Авторитетною міжнародною українською організацією є Світовий Конгрес Українців, який об'єднує близько 300 громадських організацій закордонних українців з більше, ніж 30 країн світу. Серед міжнародних об'єднань українських громад слід назвати Європейський конгрес українців та Світову федерацію українських жіночих організацій.

Розвиток глобального інформаційного простору з допомогою засобів народної дипломатії, подальше включення українських громад в усьому світі до протидії гібридним виявам російської агресії стало адекватною, дійовою відповіддю на глобальні виклики нової гуманітарної катастрофи XXI століття.

Громадянське суспільство у країнах розвинених демократій відіграє важливу роль у вирішенні багатьох загальнополітичних аспектів, особливо тих, що пов'язані з порушеннями прав людини та принципів свободи. Прозора, відкрита та соціально-орієнтована система державного управління західної розвиненої демократії включає в себе вирішальну роль громадської думки у прийнятті та ухваленні рішень. Колективний опір світового співтовариства масовим жорстоким порушенням російською федерацією права людини на життя та людську гідність у російсько-українській війні привів не лише до введення західними урядами політичних, економічних та юридичних санкцій проти російської федерації, але і до зняття обмежень щодо надання зброї Україні.

Після свідчень жорстоких вбивств цивільних у Бучі та інших міст Київської області ЄС затвердив, на той час, п'ятий пакет санкцій проти рф, що включав запровадження вугільного ембарго, обмеження для російських та білоруських транспортних компаній, заборону суднам під російськими прапорами заходити в порти країн Євросоюзу. Показово, що у даному пакеті було враховано акцію громадськості блокади вантажівок на пункті пропуску Козловичі-Кукурики на кордоні Польщі та білорусі. Співорганізаторами вказані півдесятка громадських організацій та об'єднань, у тому числі "Євромайдан-Варшава", "Український світ", "Українці в Польщі", "Загальнопольський страйк жінок", Фундація "Відкритий діалог". Блокада розпочалася 12 березня 2022 року, та створила затор із вантажівок, довжиною 55 км. Як результат, з 16 квітня 2022 року російські та білоруські перевезення на всій території ЄС були припинені [1].

У відповідь на безпрецедентну агресію проти України ЄС на середину травня 2023 року ухвалив 10 пакетів жорстких санкцій проти Росії. Вони націлені на

основи російської економіки й позбавляють її критично важливих та сучасних технологій і ринків, значно урізуючи її здатність вести війну. Санкції спланованo з намірами підірвати здатність Кремля фінансувати війну, накласти помітні економічні й політичні витрати на політичну еліту Росії, відповідальну за вторгнення, вибити з під Росії опору.

Практично від початку війни 24 лютого 2022 року світова громадськість звернулася до урядів усіх країн з вимогою закрити небо над Україною. Заклики у мережах до громадськості світу надали можливість усім отримувати прямі фото та відео докази злочинів безпосередньо з місць їх скоєння російськими військовими в Україні та дозволили підписати петицію громадськості більше мільйона осіб за короткий час. Постійні демонстрації у світових мегаполісах Лондоні, Парижі, Нью-Йорку, Амстердамі, Торонто, Варшаві, Берліні, Мілані, Турині та багатох інших збирають тисячі небайдужих громадян із закликами до своїх урядів надати необхідний захист українцям [2]. Як результат, в першу чергу урядами Великобританії, США, Канади, Польщі, Чехії, Словаччини було надано озброєння українським захисникам. Список країн, що долучаються до допомоги надалі розширюється [3]. Значним досягненням дипломатії є обладнання протиповітряної оборони України зенітно-ракетними системами "Patriot". Переломним аспектом для всієї архітектури безпеки у Європі стане поява сучасних літаків у повітряному щиті України.

Продовження порушення прав людини та принципів свободи в Україні, через ракетні обстріли жилих будинків, укриттів, вокзалів, знищення Маріуполя, Бахмута, Маріїки, Вугледара, Волновахи, Лиману, Рубіжного, Соледару, Сєвєродонецька, Щастя, Попасної, руйнування житлових масивів Харкова, Ізюма, Ірпіня, Бучі, Гостомеля, викриття жорстоких вбивств та насильства над цивільними, розстріл місць евакуації, застосування хімічної зброї, заяви російського керівництва про можливість застосування ядерної зброї є надзвичайною та впливовою підставою до дій світового фронту громадської дипломатії, щодо термінового надання важкої зброї та авіації українським військовим та зміни підходів до організації безпеки у світі на найближче майбутнє.

Чисельні приклади взаємодії закордонного громадянського суспільства та влади довели ефективність недержавних форм громадської дипломатії як важливого інструменту протидії гібридним формам ведення агресії проти України та потребують подальшої підтримки з боку державних організацій.

Список використаних джерел:

1. Ukraine conflict hurts Russian science, as West pulls funding, Reuters, https://www.reuters.com/lifestyle/science/ukraine-conflict-hurts-russian-science-.

2. Як світ протестує проти війни в Україні у фото, BBC, https://www.bbc.com/ukrainian/features-60730413>.

3. Зброя – головне, чого зараз потребує Україна: підсумки Ради ЄС, https://www.dw.com/uk/zbroia-dlia-ukrainy-bytva-za-donbas-i-nafta-pidsumky-rady-yes/a-61441361.

Юрій ГЕЛЕМЕЙ
НУ "Львівська політехніка"
ORCID: 0009-0008-0869-9713
E-mail: utkeveq@ukr.net

ПРАВОВИЙ СТАТУС ВІЙСЬКОВОПОЛОНЕНИХ ТА ПУБЛІЧНА ДИПЛОМАТІЯ

Питання правового статусу військовополонених дуже актуалізується в сучасній українській військово-політичній реальності. Один із основних принципів гуманізму стосовно ставлення до учасників військових конфліктів позиціоновано у забороні будь-якого жорстокого, недостойного чи принижуючого поводження з ними.

Норми міжнародного гуманітарного права, ще з минулого століття розглядають проблеми захисту комбатантів, цивільних осіб та інших учасників збройного конфлікту, формують механізм їх статусу та захисту. Правила захисту військовополонених є специфічними і вперше були детально описані в Женевській конвенції 1929 року. Вони були уточнені в третій Женевській конвенції 1949 року [1], враховуючи уроки Другої світової війни, а також у Додатковому протоколі I 1977 року.

Ця конвенція надає права як військовополоненим, так і учасникам опору та цивільному населенню борються з ворогом. Військовополоненими, у розумінні Конвенції, є декілька категорій осіб: особовий склад збройних сил; члени інших ополчень та добровольчих загонів; особи, які супроводжують збройні сили, але фактично не входять до їхнього складу; члени екіпажів суден торговельного флоту; жителі неокупованої території, які під час наближення ворога озброюються, щоб чинити опір силам загарбника.

Проте, саме стан війни характеризується суттєвим дисонансом між нормами права, які встановлені на державному чи міжнародному рівнях та практикою їх реалізації. IV Женевські конвенції та ряд інших актів чітко поставили стандарти, які зобов'язують сторони конфлікту поважати гідність полонених і утримувати їх у гідних умовах. Але враховуючи сучасні особливості, це питання потребує оновлення через такі фактори: наявність військового конфлікту на території України та зростання числа військовополонених з обох сторін; ефективного

механізму забезпечення належної поваги до військовослужбовців, обмеженість міжнародних інституцій у цьому аспекті; прийняття нормативно-правових актів після Другої світової війни, що може вказувати на їх соціально-політичну "застарілість" та потребу оновлення в контексті інформаційного суспільства, глобалізації та змін у життєдіяльності держави, міжнародних інституцій та соціуму, зокрема їх уточнення для розробки ефективної політики в цьому напрямку.

У сфері гуманізації суспільного розвитку значний крок вперед був зроблений шляхом прийняття міжнародних норм, зокрема тих, які регулюють обробку військовополонених. Основна концепція захисту та забезпечення гідного становища цієї категорії учасників збройних конфліктів вже визначена. Однак важливо відзначити серйозну, а навіть величезну проблему: недостатня дієвість міжнародних зобов'язань, неефективність міжнародних установ. У цьому контексті актуальним є міжнародне оновлення гуманітарного права загалом, а також у контексті поводження з військовополоненими.

Публічна дипломатія – це стратегічний підхід до міжнародних відносин, який передбачає використання комунікаційних засобів та взаємодії з громадськістю для досягнення мети в рамках міжнародної політики.

Становище українських військовополонених зумовлене тим, що держава-агресор не виконує міжнародних вимог у цій сфері, проводить політику принизливого становища українських військових, що потрапили в полон. Тому фактори дипломатії є не настільки дієвими, проте це єдина можливість зберегти життя наших воїнів, тому вагомо досліджувати проблеми в цій сфері.

Неефективність публічної дипломатії щодо захисту військовослужбовців може також бути пов'язана з низьким рівнем свідомості та обізнаності громадськості цих питань, а також недостатньою мобілізацією суспільства для впливу на владу та формування відповідної політики. Важливим аспектом є також ефективність комунікаційних стратегій та ресурсів, вкладених у публічну дипломатію для досягнення конкретних результатів у цій сфері.

Низька результативність публічної дипломатії у справі визначення статусу військовополонених може бути підкреслена низьким рівнем досягнутих цілей та відсутністю конкретних досягнень у цій сфері, що демонструє війна росії проти нашої держави. Деякі причини цього можуть включати недостатню міжнародну підтримку, зниження ефективних механізмів впливу на пошкодження та недоліки в координації зусиль. У цьому контексті важливо шукати шляхи покращення ефективності публічної дипломатії та впровадження більш ефективних стратегій для вирішення питань щодо статусу військовополонених.

Список використаних джерел:

1. Женевська конвенція про поводження з військовополоненими URL: https://zakon.rada.gov.ua/laws/show/995_153#Text.

Богдан ГОЛЯНИЧ, канд. політ. наук
ВА ім. Євгенія Березняка
ORCID: 0000-0003-0921-6142
E-mail: holjanuch@ukr.net

ПОБУДОВА МЕРЕЖІ ПУБЛІЧНОЇ ДИПЛОМАТІЇ З КИТАЙСЬКОЮ СПЕЦИФІКОЮ: ДОСВІД ДЛЯ УКРАЇНИ

Публічна дипломатія займає важливе місце в дипломатичних стратегіях різних країн та спрямована на іноземні уряди та зарубіжну громадськість з метою покращення іміджу країни. Здійснення публічної дипломатії – це неминучий вибір відповідності світовим тенденціям і розвитку часу, це об'єктивна необхідність створення доброго м'якого середовища для власного розвитку країни та зовнішньої співпраці, це важливий напрямок розвитку дипломатичної роботи.

Тенденція розвитку публічної дипломатії Китаю тісно пов'язана з національною політикою. Під час проведень з'їздів Комуністичної партії Китаю, неодноразово в доповідях звучали наступні фрази: "рішуче сприяти публічній дипломатії та міжлюдським обмінам, розбудові можливостей міжнародної комунікації, розповідати історію Китаю, представляти справжній Китай і покращувати культурну м'яку силу країни".

Після того, як у 2013 році президент Сі Цзіньпін запропонував ініціативу співпраці для будівництва "Нового економічного поясу Шовкового шляху" та "Морського Шовкового шляху 21 століття", публічна дипломатія Китаю досягла нового розвитку. Китай поглибив свої відносини з сусідніми країнами відповідно до концепцій "дружелюбності, щирості та взаємної вигоди".

Розвиток нових медіа породив нову медіа-публічну дипломатію, а також створив більш зручні умови для реалізації ініціативи "Один пояс, один шлях". Вчені Китаю вважають, що для досягнення нової медіа-публічної дипломатії "Один пояс і один шлях" необхідно зміцнювати побудову офіційних онлайн медіа, використовувати платформи соціальних медіа для ознайомлення з громадською думкою, посилювати комунікацію з громадськістю, проводити двостороннє інтерактивне спілкування, водночас створюючи механізм екстреного реагування на поширення негативної інформації.

ЗМІ є потужним інструментом публічної дипломатії та незамінним ключовим елементом у прийнятті дипломатичних рішень. У дослідженні публічної дипломатії Китаю вчені провели поглиблене дослідження та дискусії щодо співвідношення між ЗМІ та аналітичними центрами, нових можливостей і викликів медіа дипломатії в новому медіа-середовищі та ролі місцевих ЗМІ в публічній дипломатії.

Результатами дослідження встановлено, що в останні роки через національні виклики, технологічні зміни, зміни в бізнесі, інтелектуальну інтеграцію ЗМІ та

інші причини, ЗМІ перетворились на мозкові центри. Також доведено, що публічна дипломатія аналітичних центрів може формувати та впливати на громадську думку, а інтегрований розвиток "мозкового центру + ЗМІ" також допоможе здійснювати публічну дипломатію та посилювати ідеологічну силу країни в міжнародному просторі громадської думки.

Зі швидким розвитком нових медіа технологій, представлених мобільним Інтернетом, технологією великих даних і штучним інтелектом, публічна дипломатія ЗМІ також продемонструвала багато нових змін. Публічна медіа може досягти "точної доставки" цільовій аудиторії на основі інтерактивності та двостороннього характеру поширення інформації та отримання кращих результатів. Реальний інформаційний зворотній зв'язок може зробити відповідні дипломатичні рішення більш науковими та цілеспрямованими.

Також слід згадати і про культурну дипломатію, яка є ранньою формою публічної дипломатії, і її важлива роль у публічній дипломатії стає дедалі помітнішою. Питання про те, як просувати китайську культуру до "виходу на глобальний рівень" і досягнення "зв'язку між людьми" в рамках ініціативи "Один пояс, один шлях" також викликає занепокоєння в академічних колах в останні роки. Основна пропозиція нинішньої побудови публічної дипломатії Китаю – це проведення розповідей про історію Китаю та створення іміджу Китаю, як в середині країни, так і за її межами. Також це інноваційний прогрес у побудові публічної дипломатії Китаю.

На сьогоднішній день існують наступні шляхи поширення китайської культури за кордоном: Інститути Конфуція, храм Шаоліня, китайські компанії, сексуальне спілкування, культурне спілкування, засноване на економічних намірах, таких як експортна торгівля культурними продуктами (такими як анімація та ігри), публічні бібліотеки, музика, спорт.

Взагалі публічна дипломатія Китаю має глибоке історичне коріння. Публічна дипломатія з китайською специфікою керується теорією соціалізму. Основні стратегічні ідеї, такі як теорія Ден Сяопіна, важлива думка "Трьох представників" і науковий погляд на розвиток, а також дипломатичні концепції з китайською специфікою, такі як спільні зусилля для побудови гармонійного світу тривалого миру та спільного процвітання є керівною ідеологією публічної дипломатії Китаю та мають великий вплив на публічну дипломатію.

Публічна дипломатія з китайською специфікою спрямована на сприяння спільному розвитку та процвітанню між Китаєм і світом. Китай не має наміру експортувати ідеології та цінності, а також впливати на шляхи розвитку внутрішньої та зовнішньої політики інших країн. Діяльність Китаю в галузі публічної дипломатії спрямована на те, щоб наблизити Китай до світу, представити зовнішньому світу справжній Китай, Китай, який прагне підтримувати міцний світовий мир і сприяти спільному процвітанню для всіх країн.

Публічна дипломатія з китайською специфікою зосереджується на органічному поєднанні просування китайської цивілізації та вивчення досвіду інших цивілізацій. Сприяння взаємним обмінам і навчанню між китайською цивілізацією та іншими цивілізаціями світу також є правильним просуванням публічної дипломатії. Протягом багатьох років, особливо після проведення реформ, Китай постійно зміцнював діалог і обміни з різними цивілізаціями, закладаючи хорошу основу для публічної дипломатії.

Публічна дипломатія з китайською специфікою не тільки успадковує традиції, але і йде в ногу з часом. Після заснування Китайської Народної Республіки, голова Мао Цзедун і прем'єр-міністр Чжоу Еньлай встановили основні принципи політики, які не тільки прорвали західну блокаду та стримування Нового Китаю, але й встановили важливу роль у нормалізації дипломатичних відносин між Японією та встановленні дипломатичних відносин між Китаєм і США, а також призвели до великого розвитку "народної дипломатії" і "дипломатії між людьми".

Формування позитивного сприйняття України вимагає скоординованої державної політики з метою підняття міжнародного іміджу і репутації країни, поширення власних наративів з використанням усіх доступних форматів комунікації.

Досвід використання Китаєм ЗМІ та китайської культури в публічній дипломатії може слугувати прикладом для України. Адже на сьогоднішній день через збройну агресію Росії проти України, багато українців були вимушені виїхати за кордон. За кордоном українці можуть активно просувати українські традиції та звичаї, цінності української культури що і є проявом публічної дипломатії.

Юрій МІХЄЄВ, к.т.н., с.н.с.
ORCID: 0000-0002-6239-2324
E-mail: yuramiheev@ukr.net
Владислава САВЧУК, Ph. D.
ORCID: 0000-0002-0624-2284
E-mail: vladaahtytseva@gmail.com
Вероніка ЛОБОДА
ЖВІ ім. С.П. Корольова
ORCID: 0000-0002-3535-0233
E-mail: veronichkaloboda@gmail.com

БЕЗПЕКОВІ ПРІОРИТЕТИ ЗОВНІШНЬОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ

Разом із намаганням росії захопити територію України ворог продовжує впливати на процеси управління військами та об'єкти критичної інфраструктури нашої держави. Проведений аналіз кібератак, які були спрямовані на Україну з

боку російських спецслужб, свідчить про те, що більша частина інцидентів мала на меті деструктивну мету, а загальна кількість зареєстрованих кіберінцидентів у 2022 році в порівнянні з 2021 збільшилася у 2,8 рази [1]. Ці атаки спричинили суттєві негативні наслідки, зокрема витік інформації з обмеженим доступом та порушення функціонування критично важливих об'єктів державної інфраструктури.

Протистояти ворогу, який веде активні дії, в таких умовах можна завдяки розвитку державної системи кібербезпеки, що передбачає розвиток існуючих спроможностей суб'єктів кібербезпеки та кібероборони, а також удосконалення процесу координації їх спільної діяльності. Одним з пріоритетних завдань у рамках розвитку державної системи кібербезпеки є впровадження підходів провідних держав світу, які стосуються ряду організаційно-технічних заходів щодо вдосконалення оборонних спроможностей та забезпечення національних інтересів у кіберпросторі.

Враховуючи наявний стан державної системи кібербезпеки та характеристики кіберзагроз головними пріоритетами зовнішньої політики України у сфері кібербезпеки мають бути:

розроблення та впровадження нормативно-правової бази в сфері кібероборони, яка відповідала б міжнародним стандартам та була сумісною з нормативно-правовими базами держав – членів Європейського Союзу та НАТО;

нарощування спроможностей Збройних Сил України та інших складових сил оборони щодо забезпечення обороноздатності у кіберпросторі;

підготовка та навчання інструкторів з кібербезпеки на міжнародних навчальних платформах та підвищення кваліфікації фахівців і впровадження сучасних підходів у сфері кібербезпеки;

організація та проведення спільних наукових проєктів, спрямованих на розвиток системи кібербезпеки;

розширення військової співпраці з НАТО щодо забезпечення безпеки в кіберпросторі та спільних операцій, а також участь у міжнародних багатонаціональних навчаннях, таких як Cyber Flag, Locked Shields, Cyber Coalition, Cyber Endeavor.

Запропоновані пріоритети можуть стати підґрунтям для формування тем форумів Національного Кластеру Кібербезпеки.

Список використаних джерел:

1. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, 2022. URL: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf (дата звернення: 19.09.2023).

Андрій РУДИК, д.ф. з галузі спн
ННІ ПУДС КНУ ім. Тараса Шевченка
ORCID: 0000-0002-7291-4341
E-mail: andronikimpaler@gmail.com

МІСЦЕ І РОЛЬ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ У СИСТЕМІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Перш за все, починаючи розгляд даної проблеми, варто дати визначення понять "система забезпечення національної безпеки" та "стратегічні комунікації".

Отже, система забезпечення національної безпеки – це сукупність взаємопов'язаних та взаємообумовлених механізмів (інституційних, організаційних, правових та інших) та суб'єктів забезпечення національної безпеки (посадові особи держави, органи державної влади та місцевого самоврядування, державні установи та заклади, сили та засоби сектору безпеки, інститути громадянського суспільства, окремі громадяни), які на основі чинного законодавства трансформують політику національної безпеки у цілеспрямовану скоординовану діяльність (заходи політичного, правового, організаційного, воєнного та іншого характеру) щодо реалізації національних інтересів (передусім щодо виявлення, прогнозування, попередження та нейтралізації загроз безпеці особи (громадянина), суспільству та державі) [2, с. 293].

У Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України зазначається, що стратегічні комунікації – це скоординоване і належне використання комунікативних можливостей держави: публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави [1].

В обох визначеннях варто зафіксувати перегукування таких термінів як "національні інтереси держави" та "цілі держави". Очевидно, що перший є більш ширшим, оскільки національні інтереси лежать в основі системи забезпечення національної безпеки. Тоді як другий – вужчий, оскільки цілі держави виступають в якості уречевлення національних інтересів.

Стратегічні комунікації є різновидом інформаційних механізмів системи забезпечення національної безпеки. Водночас стратегічні комунікації є безпосередньою складовою системи забезпечення інформаційної безпеки. Остання входить до національної безпеки в якості її складника [4, с. 104]. Отже, місце стратегічних комунікацій у системі забезпечення національної безпеки визначається через інформаційну безпеку як складника національної безпеки.

Відповідно, це зумовлює специфічну роль стратегічних комунікацій у системі забезпечення національної безпеки, яка проявляється в наступних особливостях. По-перше, вона є опосередкованою. Стратегічні комунікації, всупереч популярній

в наукових колах думці, нездатні самостійно здійснювати вирішальний вплив на процес забезпечення національної безпеки. За своєю природою вони мають інформаційне спрямування, а отже, охоплюють лише одну сферу національної безпеки – інформаційну.

Безумовно, не варто забувати, що стратегічні комунікації не зовсім коректно відносити лише до інформаційної сфери суспільного буття. Звідси випливає друга особливість – універсальність, тобто, здатність проникати в інші сфери суспільного буття. Наприклад, така складова стратегічних комунікацій як публічна дипломатія є проявом політичної сфери за своєю сутністю. Тому, належачи до інформаційної сфери, стратегічні комунікації можуть реалізовуватися в інших складових суспільного буття. Однак, повторюючись, суто з методологічної точки зору, на забезпечення національної безпеки вони впливають лише через інформаційну сферу. Оскільки наслідки тієї ж публічної дипломатії для забезпечення національної безпеки матимуть політичне, а не інформаційне оформлення. Наприклад, український дослідник С. Соловйов прямо зауважує, що у стратегічних комунікаціях засоби інформаційного впливу скоординовано застосовуються на кожному етапі вироблення політики [5, с. 169].

Третьою особливістю специфічної ролі стратегічних комунікацій у системі забезпечення національної безпеки є їхня масштабність. Як зауважує українська вчена Т. Сивак, стратегічні комунікації не мають часових та просторових обмежень, всі дійові особи (суб'єкти стратегічних комунікацій) прямо чи опосередковано є комунікаторами [3, с. 80]. Фактично дана особливість зумовлюється вище описаними опосередкованістю та універсальністю. За умов повної приналежності стратегічних комунікацій суто до інформаційної сфери і відсутності здатності проникати/реалізовуватися в інших складових суспільного буття, вони не набували б масштабності. Перш за все, це проявлялося б у чітких обмеженнях і у визначеному наборі комунікаторів. Власне на масштабність стратегічних комунікацій вказують їхні складові: публічна дипломатія, зв'язки із громадськістю, військові зв'язки, інформаційні та психологічні операції.

Четвертою особливістю специфічної ролі стратегічних комунікацій у системі забезпечення національної безпеки є їхня трансформативність. Словник термінів і визначень НАТО AAP-06 трактує стратегічні комунікації (у військовому розумінні) як інтеграцію комунікаційних спроможностей та інформаційної функції штабу з іншими військовими видами діяльності для того, щоб зрозуміти та сформувати інформаційне середовище на підтримку стратегічних цілей і завдань НАТО [6, с. 123]. Важливо, що в Альянсі під час здійснення стратегічних комунікацій акцентують увагу саме на формуванні/перетворенні інформаційного середовища. Стратегічні комунікації у системі забезпечення національної безпеки мають виконувати не суто інформативну функцію, наприклад, просування наративів чи доведення конкретних повідомлень. Це лише один з елементів стратегічних комунікацій. По-факту вони повинні трансформовувати

інформаційну, політичну, соціальну та навіть економічну сфери суспільного буття (як держави-суб'єкта, так і держав-об'єктів) з метою забезпечення власної національної безпеки.

Отже, стратегічні комунікації займають важливе місце у системі забезпечення національної безпеки. Вони є інформаційним механізмом у структурі останньої. Водночас специфічність ролі стратегічних комунікацій у системі забезпечення національної безпеки зумовлюється наступними особливостями:

- опосередкованість;
- універсальність;
- масштабність;
- трансформативність.

Варто зауважити, що це лише ключові особливості ролі стратегічних комунікацій у системі забезпечення національної безпеки. Їхній перелік не є вичерпним, оскільки, як мінімум, можна вдаватися до поглиблення та деталізації окремих аспектів стратегічних комунікацій. У будь-якому разі, стратегічні комунікації повинні бути тим містком, який поєднує інформаційну безпеку з іншими складовими національної безпеки, і тим механізмом, який поєднує інші механізми системи забезпечення національної безпеки.

Список використаних джерел:

1. Про Затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України: наказ Міністерства оборони України від 22.11.2017 №612. База даних "Законодавство України" / Верховна Рада України. URL: https://zakon.rada.gov.ua/rada/show/v0612322-17#Text (дата звернення: 15.09.2023).
2. Публічне управління та адміністрування у сфері національної безпеки: (системні, політичні та економічні аспекти): словник-довідник / С. П. Завгородня, М. Г. Орел, Г. П. Ситник [уклад.] / за заг. ред. Д. В. Неліпи, Є. О. Романенка, Г. П. Ситника, Київ: Видавець Кравченко Я. О., 2020. 380 с.
3. Сивак Т. В. Стратегічні комунікації у системі публічного управління України : монографія. Київ: НАДУ, 2019. 338 с.
4. Ситник Г. П., Орел. М. Г. Публічне управління у сфері національної безпеки: підручник. Київ: ВПЦ "Київський університет", 2022. 464 с.
5. Соловйов С. Г. Основні характеристики стратегічних комунікацій. Вісник Національного університету цивільного захисту України. Серія: Державне управління, 2016. Вип. 1. С. 165-170.
6. AAP-06 Edition 2021. NATO Glossary of terms and definitions (English and French). North Atlantic Treaty Organization. NATO Standardization Office (NSO), 2021. 276 p.

Олександр САМПІР, д.ф.
ORCID: 0000-0002-3564-1997
E-mail: sampir1984@ukr.net
Ілона САМПІР
НУОУ
ORCID: 0000-0003-3194-893X
E-mail: Ilonasampir@ukr.net

БЕЗПЕКОВИЙ ПРІОРИТЕТ ЗОВНІШНЬОЇ ПОЛІТИКИ УКРАЇНИ

Український народ споконвічно відзначався своїм мирним характером та прагненням до спокійного життя. Але наявність історично – ворожого сусіда до суверенітету та цілісності України, в особі російської федерації, не дає змогу спокійно розвиватись та продовжувати впроваджувати європейські цінності в нашу буденність.

У 2014 році росія анексією Криму та введенням терористів на територію Донецької та Луганської областей розпочала неоголошену війну з Україною. Ця війна є складною та багатогранною, має багато площадок де розгортаються бойові дії, як на полі бою так і на політичній, економічній та торгівельній аренах. Ця війна носить затяжний характер та є місце експериментального впровадження нових методів ведення війни та нових технологій. В будь-якому випадку, ця війна буде широко висвітлена в світовій історії. Беззаперечно, що героїчна боротьба українського народу, після початку повномасштабного вторгнення, оцінені на найвищому рівні Світовою спільнотою.

Проте кожна війна має закінчуватись, а нашій державі маючи такого агресора поруч, як росія, необхідно шукати рішення для превенції в майбутньому спроб знищення нашого суверенітету та захоплення наших територій. Пошук та впровадження ефективних рішень у такій ситуації є складним завданням.

За роки війни з нащадком “московського князівства” ми можемо проаналізувати вплив основних міжнародних безпекових організацій на їх змогу врегулювання війни в Україні та прийняти рішення, яке буде кращим для майбутнього нашої держави.

Для цього, розглянемо наступні основні безпекові організації, як Організація об’єднаних націй (далі – ООН), Організація з безпеки та співробітництва в Європі (далі – ОБСЄ) та Північно-атлантичний альянс (далі – НАТО).

Першим необхідно розглянути ООН. Отже, ООН, як глобальна міжнародна організація заснована 1945 року, має на меті підтримання й зміцнення миру й міжнародної безпеки, розвиток співробітництва між державами світу, а також захист прав людини та розвиток економіки та соціальної сфери [1].

ООН в війні між Україною та росією, виявилася неефективною з наступних причин:

ООН не має достатньої влади і ресурсів для примусового вирішення конфлікту. Відповідальність за вирішення конфлікту лежить на державах-членах. ООН може діяти тільки, як посередник або сприяти вирішенню конфлікту;

ООН є складною системою з дорадчими органами та агенціями, які працюють незалежно один від одного, що може затримувати прийняття ефективних рішень;

члени Ради Безпеки мають право накладати вето ООН, яке може блокувати всі важливі рішення щодо конфлікту;

у разі невиконання рішень Ради Безпеки ООН державами-членами відповідальність за їх виконання лежить на самій Раді Безпеки та державах-членах.

Конфлікт між Україною та росією стався в межах їх території, тому рішення про втручання з боку ООН мають обмеження.

У підсумку, ООН може допомогти у вирішенні конфлікту між Україною та росією тільки, як посередник або сприяти вирішенню конфлікту. Щоб ООН могла виконувати свої функції, необхідно, щоб держави дійсно дотримувалися принципів, закладених в Уставі ООН та виконували рішення, прийняті ООН.

Слід враховувати, що у війні між Україною та росією ООН прийняла декілька резолюцій, які закликали до припинення насильства та повного виконання міжнародного права. Однак росія продовжила свою агресію проти України, а самі резолюції не були виконані. Також росія має можливість використовувати вето, як постійний член Ради Безпеки ООН, що ускладнює вирішення конфліктів у цій раді.

Ці твердження також були озвучені президентом України Володимиром Зеленським на засіданні Ради Безпеки ООН [2].

Президент в своїй промові на Раді Безпеки ООН 20.09.2023 року сказав:

“Мені шкода, що Рада Безпеки ООН зараз – це лише найбільш помітна у світі трибуна. Я вірю, що ООН здатна… Я знаю, що ООН здатна на більше. Я впевнений, що Статут ООН може реально працювати заради миру, заради безпеки у глобальному масштабі. Але для цього багаторічні розмови та проекти щодо реформування ООН повинні стати конкретним процесом реформування ООН”. І має йтися не лише про представництво тут, у Раді Безпеки. Застосування права вето – ось що потребує реформи, і це може стати ключовою реформою. Тим, що повертає силу Статуту ООН.

Разом з цим президент України визначив кроки, які допоможуть вирішити цю проблему:

*“**Перший крок**. Якщо війну неможливо зупинити через те, що всі зусилля блокуються вето агресора чи того, хто потурає агресору, потрібно виносити це питання на розгляд Генеральної Асамблеї. За умови набрання двох третин голосів, які відображатимуть волю націй глобальної кваліфікованої більшості – вето має реально долатися, і така резолюція Генасамблеї повинна бути обов’язковою для виконання всіма державами-членами;*

***Другий крок**. Рада Безпеки ООН має бути повністю підзвітною перед націями світу. Я вітаю пропозиції різних лідерів розширити представництво націй у Раді Безпеки. Коло постійних членів Ради безпеки має відображати сучасність. Сучасність і справедливість;*

***Третій крок**. Потрібна система превенції агресій через раннє реагування на дії, спрямовані проти територіальної цілісності та суверенітету держав. Настав час це зробити. Націям світу варто погодити такий механізм реагування на агресії для захисту інших, який кожен хотів би для власної безпеки".*

Підсумовуючи сказане президентом можна сказати, що Організація об'єднаних націй перебуває в глухому куті щодо агресій і закликав реформувати Радбез ООН.

Наступною безпековою організацією є Організація з безпеки і співробітництва в Європі (ОБСЄ; OSCE) – найбільша у світі регіональна міжурядова організація з питань безпеки [3]. Має статус спостерігача в ООН. Об'єднує 57 країн-учасниць, розміщених у Північній Америці, Європі та Азії.

ОБСЄ у війні між Україною та росією виконала наступні кроки:

у 2014 році ОБСЄ спорядила моніторингову місію на Донбас на прохання України;

1 липня 2014 в Баку XXIII-а ухвалила резолюцію абсолютною більшістю голосів, що засуджує росію за анексію Криму і сприяння розвитку збройного конфлікту в Україні на щорічній Парламентській асамблеї ОБСЄ;

8 липня 2015 в Гельсінкі XXIV-а щорічна Парламентська асамблея ОБСЄ схвалила резолюцію: "Очевидні, грубі і невиправлені порушення РФ зобов'язань у межах ОБСЄ і міжнародних норм", у якій визнала дії росії актом військової агресії проти України.

Проте не зважаючи на активні кроки, правильні кроки, ми спостерігаємо прихильність та симпатію багатьох членів та представників ОБСЄ до росії.

22-га зимова сесія ПА ОБСЄ 2023 року, що відбулась 23-24 лютого у Відні пройшла без участі України. Україна відмовилась від участі на знак протесту проти допущення російської делегації до участі у засіданнях.

Відень, як місцеперебування штаб-квартири ОБСЄ, потроху перетворюється центром для інтерпретації росією її війни проти України.

На підтвердження зазначеного варто привести цитату колишнього очільника Луганської ВЦА у 2014-2015 роках Геннадія Москаля, який ОБСЄ називав це утворення паразитарним, від якого немає жодної користі [4]:

"Я бачив роботу ОБСЄ, і чесно говорю, що від них, як від мінеральної води - ні користі, ні шкоди нема. Серед них дуже багато прихильників росії. Це такий змішаний орган, який імітує, що він дуже потрібний. Їм платять гарні гроші, їх страхують на випадок смерті або нещасного випадку. Я, окрім як у ресторанах, пивбарах за чаркою горілки або віскі, майже на передовій їх не бачив."

Переходимо до третього ключового суб'єкта національної безпеки – НАТО. Україна не є членом альянсу. На мою думку за всю допомогу, яку ми отримуємо нам варто завдячувати насамперед підтримці Сполучених Штатів Америки. Проте вступ до альянсу геть інша історія. До альянсу входять ряд держав, які мають симпатію до нашого ворога та відверто йти проти держави, яка має певний економічний вплив відмовляться [5].

На мою думку Україні для забезпечення суверенітету та територіальної цілісності варто розглядати наступні варіанти військової співпраці з союзними державами, а саме:

1. Створення регіонального безпекового альянсу: Україна може розглядати можливість створення регіонального безпекового альянсу разом з іншими країнами Європи або з країнами, які мають спільний кордон. Такий альянс може забезпечити безпеку в регіонах, зокрема шляхом спільних військових вправ та оперативної співпраці.

2. Європейська оборонна співпраця: Україна може брати участь у європейській оборонній співпраці, щоб забезпечити безпеку в регіонах. Така співпраця може включати спільні військові вправи, обмін даними та співпрацю з іншими країнами Європи для покращення безпеки та оборони.

Варіант Європейської оборонної співпраці має ситуаційний характер та розбирати окремо не має жодного сенсу. Варто більше акцентувати увагу на створенні нового регіонального безпекового альянсу.

Як на мене платформою зазначеного безпекового альянсу може слугувати Литовсько-Польсько-Українська бригада імені Великого гетьмана Костянтина Острозького, бригада країн Люблінського трикутника, яка була створена в 2014 році. Проте даній організації не вистачає міцного союзника, який би мав серйозний ядерний потенціал, якою може бути Великобританія.

Альянс Британії та країн Люблінського трикутника може мати наступні важливі фактори у війні з росією:

військова підтримка: Британія та Польща є членами НАТО, тому мають сильну військову потужність. Це може допомогти Україні у забезпеченні безпеки та захисту території від можливих атак Росії;

економічна допомога: Британія, Литва та Польща можуть надати економічну підтримку Україні, яка може стати корисною у забезпеченні потреб населення та розвитку господарства;

політична підтримка: Альянси Британії, Литви, Польщі та України можуть звернутися до міжнародної спільноти з проханням підтримати Україну та засудження дій росії. Це може підвищити шанси на залучення міжнародної підтримки у боротьбі з росією;

інформаційна підтримка: Альянс може надавати інформаційну підтримку, яка допоможе протистояти російській пропаганді. Це може включати поширення

інформації про справжній стан речей в Україні, відображення позиції міжнародної спільноти, а також відповідь на дезінформацію росії.

Про започаткування нового тристороннього формату співпраці між Україною, Великою Британією та Польщею 17.02.2022 міністр закордонних справ України Дмитро Кулеба заявив на спільній з державним секретарем Великої Британії Ліз Трасс пресконференції у Києві, дана співпраця покликана реагувати на загрози європейській безпеці та посилювати економічну співпрацю між країнами.

Загалом, згаданий альянс має високий потенціал та при проведенні правильної, дієвої політики та усуненні бюрократичної складової матиме більший потенціал від існуючих міжнародних організацій.

Завдання сектору оборони, при створенні даного альянсу: щоденно показувати високий рівень професіоналізму під час організації та проведення заходів співпраці, саме тому в сьогоденні ми маємо плідно працювати для набуття спроможностей Збройних Сил України та інших складових Сил Оборони нашої держави відповідно до принципів і методології євроатлантичних держав і з урахуванням національних особливостей.

Список використаних джерел:

1. Організація Об'єднаних Націй// Вікіпедія. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0.
2. Промови та звернення. Застосування права вето потребує реформування, і це може стати ключовою реформою ООН – виступ Президента України на засіданні Ради Безпеки ООН. Офіційне інтернет-представництво [Електронний ресурс]. - Режим доступу: https://www.president.gov.ua/news/speeches.
3. Організація безпеки та співробітництва в Європі. Україна і ОБСЄ // Вікіпедія. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0.
4. Фрагмент інтерв’ю голови Закарпатської ОДА, екс-керівника Луганської обласної військово-цивільної адміністрації Геннадія Москаля телеканалу “112 Україна”[Електронний ресурс]. – Режим доступу: https://web.archive.org/web/20171112185913/https://ua.112.ua/mnenie/zakonom-pro-reintehratsiiu-ordlo-my-ne-vyzhenemo-rosiiski-viiska-z-donbasu-ta-krymu-419808.html.
5. Організа́ція Північноатланти́чного до́гово́ру, також Північноатланти́чний алья́нс або НАТО. // Вікіпедія. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/D0%9D%D0%90%D0%A2%D0%9E.

Вікторія СЕМА
НАВС
ORCID: 0009-0002-7835-0193
E-mail: vika1018@ukr.net

СТРАТЕГІЧНІ КОМУНІКАЦІЇ У СФЕРІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ

Україна – перша країна, що закріпила поняття стратегічні комунікації у державних документах – Воєнній доктрині України [1], Доктрині інформаційної безпеки України [2] та Стратегії інформаційної безпеки України [3]. Стратегічні комунікації грають ключову роль у формуванні громадської свідомості, міжнародному сприйнятті та взаємодії з різними суб'єктами національної та міжнародної арени. Такий підхід свідчить про важливість інформаційної безпеки та комунікаційних стратегій у сучасному світі.

Стратегічні комунікації в сфері забезпечення національної безпеки та оборони відіграють ключову роль у забезпеченні ефективного функціонування національних систем безпеки та захисту. Цей аспект стає все важливішим у сучасному світі, оскільки інформаційні технології роблять інформаційне простір більш доступним і вразливим на широкий спектр загроз. Ось деякі ключові аспекти стратегічних комунікацій у сфері забезпечення національної безпеки та оборони:

розробка та впровадження стратегічних комунікаційних стратегій та планів, які підтримують національну безпеку і оборону. Координація зусиль різних галузей та відомств для досягнення спільних цілей;

збір та аналіз інформації щодо поточних загроз і викликів для національної безпеки та оборони. Розуміння поглядів та намірів можливих противників або суб'єктів, які загрожують національній безпеці;

публічна інформація та освіта громадськості щодо питань національної безпеки та оборони. Пояснення стратегій, політики та рішень у цих сферах громадськості;

співпраця з медіа для забезпечення об'єктивного та точного висвітлення подій у сфері національної безпеки та оборони. Це включає в себе інтерв'ю, прес-конференції та інші форми спілкування з журналістами;

вплив на громадськість та противника через психологічні операції;

захист важливих інформаційних ресурсів та інфраструктури від кібератак. Розробка кіберстратегій та заходів для забезпечення цілісності інформації;

співпраця з іншими країнами, міжнародними організаціями та союзниками у сфері національної безпеки та оборони. Дипломатичні зусилля та обмін інформацією [5].

Україна стикається з численними проблемами у сфері стратегічних комунікацій у забезпеченні національної безпеки та оборони, які впливають на ефективність інформаційних заходів та спроможність влади взаємодіяти з громадськістю і міжнародними партнерами. Деякі з найбільш актуальних проблем включають:

Україна стала ареною гібридної війни, у якій дезінформація грає важливу роль. Російська Федерація активно використовує інформаційні канали для спотворення подій та розповсюдження пропаганди. У відповідь Україна створила центри інформаційної контрпропаганди та розвиває засоби виявлення та розкриття дезінформації;

Україна має велику кількість людей, які проживають в зоні конфлікту країни. Забезпечення їхнього доступу до об'єктивної інформації та залучення до співпраці є важливим завданням. Україна створила механізми для ведення діалогу з різними групами громадян та регіонами країни, щоб забезпечити відкритий обмін інформацією та врахувати думки та допомогу різних суб'єктів;

зростаюча кількість кібератак і спроби злому комп'ютерних систем створюють загрози для національної безпеки. Україна активно зміцнює свої кібербезпекові та інформаційні оборонні здібності для захисту важливих об'єктів та інформаційної інфраструктури від кібератак. А також Україна повинна покращити свої здібності в галузі кібербезпеки та інформаційної безпеки;

велика частина населення України може стикатися з інформаційною агресією та дезінформацією. Підвищення інформаційної грамотності і навчання громадян критично оцінювати інформацію є важливим завданням. Громадянське суспільство, журналісти та незалежні медіа грають важливу роль у розкритті правдивої інформації та відстоюванні демократичних цінностей. Україна заохочує діяльність цих суб'єктів та забезпечує їхню свободу;

Україна повинна активно співпрацювати з міжнародними партнерами в галузі інформаційної безпеки та обміну інформацією про загрози. Україна активно співпрацює з міжнародними партнерами, зокрема з НАТО та Європейським Союзом, у сфері інформаційної безпеки та обміну інформацією про загрози;

забезпечення ефективної внутрішньої координації між різними органами влади, які відповідають за національну безпеку та оборону, є важливим аспектом успішної стратегії комунікацій [4];

забезпечення свободи преси та захист прав журналістів в Україні є важливим для розширення інформаційної свободи та об'єктивної висвітлення подій.

Україна постійно розвиває свою систему стратегічних комунікацій, включаючи роботу з громадськістю, інформаційні кампанії та звітність про заходи забезпечення національної безпеки та оборони. Необхідно відзначити, що Україна продовжує працювати над подоланням викликів інформаційної війни та забезпеченням національної безпеки через ефективну систему стратегічних комунікацій та співпрацю з міжнародними партнерами.

Перспективи розвитку стратегічних комунікацій у сфері забезпечення національної безпеки та оборони в Україні включають кілька ключових напрямів:

оскільки кіберзагрози стають все більш серйозними, Україна має продовжувати розвивати свої кібербезпекові здібності та співпрацювати з міжнародними партнерами для обміну інформацією та вдосконалення заходів захисту;

важливо навчати громадян розрізняти дезінформацію від правдивої інформації та підвищувати рівень їхньої інформаційної грамотності. Це може бути здійснено через освітні та інформаційні кампанії;

Україна повинна продовжувати співпрацювати з міжнародними організаціями та партнерами, такими як НАТО та Європейський Союз, у сфері інформаційної безпеки та обміну досвідом;

незалежні медіа та журналісти грають важливу роль у розкритті правдивої інформації та контролі за діяльністю влади. Підтримка незалежних медіа та захист журналістів є ключовим завданням [6];

Україна повинна продовжувати здійснювати реформи в сфері доступу до інформації та забезпечення прозорості діяльності державних органів; інформаційне середовище постійно змінюється, тому Україна повинна бути готовою адаптуватися до нових викликів та небезпек.

Україна має потенціал для розвитку ефективної системи стратегічних комунікацій у сфері забезпечення національної безпеки та оборони, і реалізація цих перспективних напрямів допоможе зміцнити національну безпеку та стійкість країни.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року “Про нову редакцію Воєнної доктрини України” URL: https://www.president.gov.ua/documents/5552015-19443 (дата звернення 23.09.2023).
2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України” URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення 23.09.2023).
3. Про Стратегію інформаційної безпеки URL: https://zakon.rada.gov.ua/laws/show/n0080525-21#Text (дата звернення 23.09.2023).
4. Резникова О. Щодо концепції забезпечення національної стійкості в Україні. Аналіт. записка. Серія “Нац. безпека”. 2022. № 8. С. 1–8.
5. Стратегічні комунікації для безпекових і державних інституцій: практичний посібник / [Л. Компанцева, О. Заруба, С. Череватий, О. Акульшин; за заг. ред. О. Давліканової, Л. Компанцевої]. Київ: ТОВ “ВІСТКА”, 2022. 278 с.

Лариса СНІГУР
НА СБУ
ORCID: 000-0001-8412-3734
E-mail: larisa.snigur7@gmail.com

ВОЛОНТЕРСТВО ЯК СКЛАДОВА ГУМАНІТАРНОГО РЕАГУВАННЯ ТА ІНСТРУМЕНТ ПУБЛІЧНОЙ ДИПЛОМАТЇЇ

Публічна дипломатія – один з основних інструментів стратегічних комунікацій держави, що працює на створення позитивного міжнародного іміджу країни, її впізнаваність, розбудову репутації у світі зовнішньої політики держави, а використання інструментів публічної дипломатії сприяє поширенню застосування "м'якої сили" в міжнародних відносинах. Публічна дипломатія спрямована на розширення діалогу між громадянами і закордонними партнерами, передбачаючи активний міжнародний обмін, створення інформаційних програм, тобто пропагування власної культури зовні. Таким чином, публічна дипломатія в умовах повномасштабної агресії російської федерації в Україні набуває особливої актуальності як метод досягнення зовнішньополітичних цілей, привертання уваги до грубих порушень прав цивільного населення і некомбатантів в умовах війни, а також інформування громадян інших країн о подіях, які в перспективі можуть вплинути на їх життя. В умовах війни публічна дипломатія виходить за межи традиційної мети, а саме підвищення рівня та якості знань світової спільноти про певну країну, підвищення суспільної оцінки держави, зацікавлення суспільства певною країною. Цьому сприяє активне залучення гуманітарного сектора, зокрема неурядових організацій і волонтерів до інформування суспільства та привернення уваги світової спільноти до події (1, с. 40-44).

Сьогодні волонтерські організації і волонтери як потужний елемент громадянського суспільства беруть активну участь як в соціальних, так і в соціально-інформаційних проектах. Волонтерство як ефективна складова гуманітарного реагування в кризових ситуаціях, що побудована на горизонтальних зв'язках, інтегрована в суспільство і активно взаємодіє з державними установами, а також має високий рівень довіри як внутрішніх, так і зовнішніх цільових аудиторій. Відсутність бюрократії в волонтерських організаціях забезпечує швидке реагування на виклики: налагодження логістичних ланцюгів постачання та розподілу допомоги на територіях в зоні бойових дії, містах евакуації, та в окупованих громадах, організація допомоги в евакуації та інформаційної підтримки громадян тощо. Так, налагоджені певні механізми співпраці з партнерами\донорами та людьми, які потребують допомоги, надало можливість в максимально стислі строки вирішити питання із забезпечення продуктами харчування, питною водою, засобами гігієни, одягом, ліками тощо постраждалих від російської агресії. Цьому також сприяла активна участь

українського населення в волонтерському русі. За даними Charity Aid Foundation World Given Index 2022 (3), Україна з 20 місця в 2021 (2) і 2022 роках піднялася на 10 позицій і вийшла в топ-10 країн по залученності населення до волонтерської діяльності. Як свідчать дані соціологічного дослідження групи “Рейтинг” майже 50% українців займаються волонтерською діяльністю, 6% із них - на постійній основі (4).

Волонтерство в умовах війни - один з ефективних способів для цивільних громадян зробити внесок в оборону країни, відчути приналежність до національної спільноти, а для громадян інших країн - приєднатися до захисників, зрозуміти мотивацію, продемонструвати єдність цінностей, проявити емпатію.

Спроможність волонтерського руху і неурядових організації оперативно реагувати на ініціативи влади і громадянського суспільства може бути використана для просування актуальних меседжів на міжнародній арені. Висвітлення подій в неофіційних джерелах, привернення уваги до небезпеки для цивільного населення, спричиненої діями агресора, сприяє як інформуванню так і консолідації світової спільноти. Обмеженість об’єктивної інформації про події в Україні, узагальнення, імперсоніфікація в засобах масової інформації інших країн мінімизують увагу зовнішніх цільових аудиторій до війни, її наслідків, страждань населення і кількості втрат. У тої же час гнучкість та адаптивність до швидких змін, а також зворотній зв’язок з цільової аудиторією робить волонтерську ініціативу ефективним інструментом налагодження взаємодії на рівні громадянського суспільства як всередині країни, так і зовні.

Проведення волонтерами в соціальних мережах або закордоном аукціонів по збиранню коштів для потреб ЗС України та людей, які постраждалих від агресії російської федерації, супроводжується поширенням інформації про злочини країни-агресорки. Організація українських фестивалів волонтерами діаспор і волонтерами-біженцями – інструмент поширення інформації про культуру України, її традиції, цінності, історію, а також злочини країни-агресорки. Фандрайзінгові платформи також стають інструментом інформування і привертання уваги до подій, а також залучення пересічних громадян до вирішення проблеми, тобто демонстрації своєї громадянської позицій.

Залучення гуманітарними організаціями відомих людей як амбасадорів – інструмент поширення інформації про реальні події серед широкої медіа-аудиторії. Як наслідок – підвищиться рівень емпатії світової спільноти до ситуації в Україні та розуміння нашої системи цінностей.

Волонтерські ініціативи сприяють зміцненню національної гордості та єдності, розвивають в українських громадянах почуття солідарності та національної ідентичності, а також дають можливість громадянам інших країн сформувати позитивну думку щодо української спільноти і привернути увагу до подій в Україні. Бренд Україна (українська кухня, національний одяг, символіка, прикраси) набуває популярності саме через міжособисті контакти, розуміння

єдності цінностей і залученості громадян інших країн до вирішення проблем, зумовлених агресією росії.

Таким чином, гуманітарне реагування, а саме волонтерство і дії неурядових організацій, що спрямовані як на внутрішню та і зовнішню цільову аудиторію одночасно можна розглядати як “м'яку силу”, що ефективно використовується на тактичному рівні публічної дипломатії в умовах війни.

Список використаних джерел:

1. Mark Leonard, Catherine Stead, Conrad Smewing. Public Diplomacy. London: The Foreign Policy Center, 2002. 101 p.
2. Charity Aid Foundation World Given Index 2021. веб-сайт URL: https://www.cafonline.org/about-us/publications/2021-publications/caf-world-giving-index-2021 (дата звернення: 20.09.2023).
3. Charity Aid Foundation World Given Index 2022. веб-сайт URL:https://www.cafonline.org/about-us/publications/2022-publications/caf-world-giving-index-2022 (дата звернення: 20.09.2023.
4. Формула стійкості України: основні складові під час та у поствоєнний період. веб-сайт URL: https://ratinggroup.ua/research/ukraine/ukraine_s_resilience_formula_the_essential_components_during_war_and_post-war_6_11_june_2023.html (дата звернення: 20.09.2023).

Василь ЦЕГЕЛЬНИК
ORCID: 0000-0001-7361-9822
Михайло ФАЙФУРА
НАСВ ім. гетьмана Петра Сагайдачного
ORCID: 0000-0002-0013-0767
E-mail: vasyl8857@gmail.com

ЗБРОЙНІ СИЛИ УКРАЇНИ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Російська федерація 24 лютого 2022 року розпочала проти України повномасштабну збройну агресію, яка продовжується і зараз. Збройна агресія російської федерації проти України є тяжким міжнародним злочином (відповідно до сучасного міжнародного права), що тягне за собою міжнародно-правову відповідальність рф. З моменту вторгнення в Україну міжнародна спільнота застосовує проти рф міжнародно-правові санкції. В цих умовах Збройні Сили України відіграють важливу роль у відбитті збройної агресії з боку рф. Бойовий досвід російсько-української війни 2022-2023 років свідчить, що для перемоги над

ворогом потрібно забезпечити Збройні Сили України сучасним озброєнням і військовою технікою.

Артилерійські підрозділи ЗСУ відіграють важливу роль в складі Сил оборони в ході російсько-української війни. З початком відбиття повномасштабної російської агресії артилерійські підрозділи застосовувються для:

знищення місць зберігання та засобів підвозу паливо-мастильних матеріалів та боєприпасів;

знищення противника в районах зосередження;

ураження важливих об'єктів противника (ПУ);

артилерійської підтримки військ, що обороняються, та здійснюють контрнаступ тощо.

Окремим важливим завданням є боротьба з артилерією противника – контрбатарейна боротьба, успішна реалізація якої забезпечує вогневу перевагу над противником та, як результат, зниження ефективності вогневого ураження ним. Досвід показує, що ефективна контрбатарейна боротьба – важливий чинник досягнення успіху в бою, особливо в умовах, коли застосування авіації вкрай ускладнене, або не можливе.

Значно покращити наші спроможності здатні поставки західних високотехнологічних реактивних систем залпового вогню разом з сучасними системами цілевказання (автоматизації). Швидко змінити ситуацію можливо за рахунок міжнародної технічної допомоги, зокрема використовуючи механізм ленд-лізу. Тому важливим вважається постачання реактивних систем залпового вогню провідних країн світу: США, ФРН, Велика Британія, Франція. Оптимальними для вирішення поточних завдань щодо нанесення ураження противнику вбачаються такі системи,як M142 XIMARS та "Astros II".

Також значно підвищити ефективність вогню артилерії дозволяє застосування артилерійськими підрозділами БпЛА, таких як MiniShark (дрон створений для виконання розвідувальних завдань і може виявляти наземні цілі в інтересах артилерії, спеціальних підрозділів та частин сухопутних військ), Raybird-3 та інші.

Таким чином, застосування БпАК дає можливість в режимі "on-line" (наближеному до реального), приймати рішення щодо ураження об'єктів противника, підвищити точність вогню артилерії та скоротити витрату боєприпасів.

Отже, для України впровадження нових сучасних типів озброєнь не є справою довільного вибору, а питанням національної безпеки, захисту життєво важливого національного інтересу.

Список використаних джерел:

1. Воєнна доктрина України. Затверджено Указом Президента України від 24 вересня 2015 року № 555/2015. URL: https://www.president.gov.ua/documents/5552015-19443/.

2. Контрбатарейна боротьба у ЗСУ https://armyinform.com.ua/2023/08/17/kontrbatarejna-borotba-u-zsu-zaznaye-revolyuczijnyh-zmin/.
3. Focus.ua https://focus.ua>digital.
4. Американські XIMARS в ЗСУ https://mil.in.ua/uk/articles/amerykanski-himars-v-zsu-rik-bojovogo-zastosuvannya-po-rosijskyh-okupantah/.

Роман ЧАПЛІНСЬКИЙ
E-mail: Chaplinskiy_roman@ukr.net
Євген БОНДАРЧУК
ВА ім. Євгенія Березняка

ПІДХІД ДО ДОСЛІДЖЕННЯ ОСНОВНИХ ТЕНДЕНЦІЙ СПОРТИВНОЇ ДИПЛОМАТІЇ РФ В КОНТЕКСТІ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ВПЛИВАМ

Під час проведення Олімпійських ігор у Стародавній Греції припинялися всі війни. Адже один із головних принципів олімпійського руху – сприяти миру та гармонійному розвитку людства. Але знайшлася людина, яка цей принцип олімпізму демонстративно порушила – володимир путін:

серпень 2008 року, росія почала вторгнення в Грузію – якраз у день відкриття Олімпійських ігор у Пекіні (згідно дослідження Modern War Institute, російсько-грузинська війна стала "тренуванням" перед тим, що відбулося у 2014 році);

лютий 2014 року, під час проведення Олімпіади в Сочі путін віддав наказ на вторгнення в український Крим (Сергій Гайдук, віце-адмірал, командувач ВМС України в 2014-2016 роках, стверджував що Олімпіада в Сочі послугувала прикриттям росії для перекидання своїх додаткових військ до Криму й подальшого захоплення півострова);

лютий 2022 року, кремль розпочав повномасштабну війну проти України – одразу після закінчення Олімпійських ігор у Китаї.

Для всього цивілізованого світу росія стає країною-ізгоєм, рекордсменом за кількістю накладених санкцій та власним лідером який засуджений Міжнародним кримінальним судом у Гаазі. Санкції торкнулися і спорту. Але минув рік – і керівник Міжнародного олімпійського комітету Томас Бах несподівано змінює свою думку. Озвучує один з улюблених кремлем і його пропагандистами наративів: "Спорт має бути поза політикою". Він пропонує допустити спортсменів країни агресора на Олімпіаду-2024 року в Парижі під нейтральним білим прапором.

Ось тільки це нічого не змінює, бо кремль використовував та намагається використовувати спорт для пропаганди завжди. Спортсмени стали глашатаями наративів кремля, які відкрито і публічно підтримують війну.

Але приховати правду від усього світу їм не вдасться. На поверхню спливає інший незаперечний факт, що більшість російських спортсменів є військовослужбовцями збройних сил (ЦСКА рф). На зимовій Олімпіаді-2022 у Пекіні 90% російських медалей завоювали саме атлети російських силових структур, а на літніх Олімпійських іграх у Токіо 2021 року вони вибороли всі медалі збірної росії – загалом 71 нагорода.

У прагненні за всяку ціну проштовхнути російську збірну на Олімпіаду росія має завдання: обілити агресора і особисто президента путіна. Тому можна впевнено говорити про те, що Олімпійські ігри – 2024 року в Парижі залишаються для них вкрай важливою та пріоритетною цілю.

Маніпуляції зі спортивною дипломатією, керівництвом російською федерацією активно використовувалися вже на початку ХХ ст., чому існує безліч прикладів. Нічого не змінюється й сьогодні. Навпаки керівництво російської федерації продовжує насміхатися над усім цивілізованим світом. Підбираючи необхідні наративи, вміло, а головне “начебто не нав’язливо”, використовуючи переможні акції взяті з радянської історії, продовжує нести свою імперську пропаганду та поступово інтегрувати її у цивілізоване, світове спортивне життя.

Нова концепція зовнішньої політики рф від 31 березня 2023 року, є продовженням позиціонування “величі” росії, як країни цивілізації, євразійської і євро-тихоокеанської ядерної наддержави багатополярної міжнародної системи. Місце росії в світі визначається наявністю у неї значних ресурсів у всіх сферах життєдіяльності, її статусом постійного члена Ради Безпеки Організації Об’єднаних Націй (ООН) та однією із двох найбільших ядерних держав.

Знаходячись в кріслі Ради Безпеки, яке росія й досі займає не законно через закулісні маніпуляції після розпаду радянського союзу та маючи можливість постійного виправдовування агресії та геноциду який здійснює рф в Україні, питання участі російських спортсменів на Олімпійських іграх – 2024 в Парижі залишається відкритим. Чи може Україна та увесь цивілізований світ у ХХІ ст. дати можливість російським загарбникам і на далі маніпулювати спортивною дипломатією? Звичайно ні, і незалежно як буде діяти інша частина цивілізованого світу, маючи історичний досвід та знаючи про далекоглядні підходи до ведення росією гібридної війни, нам вкрай необхідно, не залишатися в стані очікування, а формувати і демонструвати всьому світу свої лідерські позиції.

Для детального вивчення можливостей публічної дипломатії рф, та своєчасного знайдення шляхів протидії, нами проведено експертне дослідження методом цільового динамічного оцінювання альтернатив за допомогою адаптованої аналітичної системи підтримки прийняття рішень “СОЛОН – 3”. Система дозволяє після декомпозиції основної цілі (Вплив заходів публічної

дипломатії рф в контексті російсько-української війни) здійснити оцінку кожного з напрямів – під цілі, що впливають на головну ціль (культурна дипломатія, експертна дипломатія, економічна дипломатія, цифрова і наукова дипломатія, спортивна дипломатія). У подальшому ці сформульовані під цілі також підлягали декомпозиції. Процес декомпозиції продовжувався поки множини під цілей, які впливають на головну ціль, що розкриваються, будуть складатися лише з варіантів рішень, що оцінюються. Тобто процес декомпозиції зупиняється, коли не залишилось не розкритих цілей (під цілей).

У дослідженні взяли участь сім експертів які проаналізували, їм визначені, напрями публічної дипломатії рф. Для формування основних тенденцій та написання найбільш вірогідних та найменш ймовірних сценаріїв, експертами використовувався метод попарного порівняння. Зазначена методика дала можливість здійснити перевод якісної інформації в цифрову, що візуалізується на діаграмі.

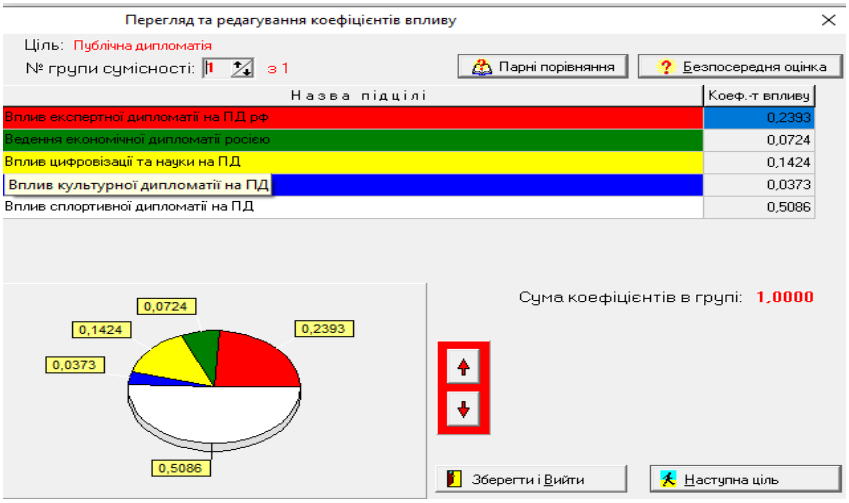


Рисунок 1. Інтерфейс проведеного дослідження.
Джерело: Система підтримки прийняття рішень “СОЛОН – 3”.
Розробник: Інститут проблем регістрації інформації.

Експертами виявлено наступні тенденції спортивної дипломатії, які в подальшому впливали на формування сценаріїв СД:

рф вміло використовує історичні наративи СД, як значний інструмент впливу на внутрішню аудиторію;

російські спортсмени залишаються бути вагомими носіями наративів кремля;

Олімпійські ігри 2024 року в Парижі для рф – пріоритетна ціль;

проглядається збільшення поступового повернення російських спортсменів до змагань великого спорту.

Нам вдалося оцінити зазначені вище напрями публічної дипломатії та побудувати пріоритетний ряд по їх застосуванню російською федерацією в контексті російсько-української війни (гібридної війни).

Разом з цим, дослідження виявило високий вплив спортивної дипломатії, як найбільш впливового напрямку публічної дипломатії рф в контексті ведення нею гібридної війни та "відкритої зовнішньої політики".

Запропонований підхід дослідження з використанням цільової динамічної оцінки альтернатив, дає можливість в подальшому сформувати активні заходи протидії та можливі шляхи запобігання проведенню рф ефективної публічної дипломатії, в першу чергу спортивної дипломатії, на передодні Олімпійських ігор – 2024 року в Парижі. Крім цього, дослідження націлює нас на постійний аналіз інформації пов'язаної зі спортивною дипломатією, прогнозування можливих сценаріїв та формуванням власних лідерських наративів.

Список використаних джерел:

1. Матяш І.Б. Публічна дипломатія: навчальний посібник. Видавництво "Горобець". Київ-Острог, 2021. – 221 с.

2. Компанцева Л., Акульшин О., Акульшина Н., Дєдушкіна Т., Заруба О., Зубченко О., Хома І., Чернігівська Н. Базові поняття стратегічних комунікацій: Стандарти на основі документів НАТО: англійсько-український та україно-англійський словник. Видавництво ТОВ "Мега-поліграф". Київ: Нац.акад.СБУ, 2019. – 336 с.

Сергій ЧЕРЕВАТИЙ,к.політ.н.
заступник Командувача ОСУВ
"Хортиця" зі стратегічних
комунікацій

Особливості розбудови стратегічних комунікацій в Східний операційній зоні ОСУВ "Хортиця"

Російська військова агресія в Україні стала яскравим прикладом гібридної війни, коли проведення інформаційно-психологічних операцій має значення рівноцінне проведенню класичних військових дій, а іноді й важливіше. Технологічні зміни у поширенні інформації зробили це поле битви гнучким, змінним та динамічним, що відповідно вимагає постійної уваги та контролю. Стало зрозумілим, що потрібні нові організаційні форми, більш самостійні, які будуть не просто налагоджувати комунікації, а часом здатні брати на себе ініціативу, генерувати цілі, проводити активні інформаційно-психологічні

операції. Для цього було створено низку структур, які займаються стратегічними комунікаціями.

За час введення посади заступника Командувача ОСУВ “Хортиця” зі стратегічних комунікацій відбулись значні зрушення у практичній площині завдяки спілкуванню та взаємодії з цільовою аудиторією. Разом з Управлінням стратегічних комунікацій Міністерства оборони України вдалось закласти підвалини для розбудови системи стратегічних комунікацій, як на східному напрямку бойових дій, так і у ЗСУ в цілому.

Створена вертикаль системи стратегічних комунікацій є потужним інструментом боротьби в інформаційному просторі та протидії пропаганді і дезінформації, що дає можливість працювати проти противника, застосовуючи весь спектр переваг психологічних інструментів сил спецоперацій.

Варто зауважити, що у безпосередньому підпорядкуванні стратегічних комунікацій ОСУВ “Хортиця” були і мобільні групи центральної теле-радіостудії Міністерства оборони України та інформаційного агентства “АрміяINFORM”. Це дозволило значно наблизитись як елементу державної інформаційної машини до системи “Onevoice”, що, у свою чергу, дало можливість, використовуючи весь цей інструментарій, доводити українські наративи до української та закордонної аудиторій, інформаційно впливати як на свої війська, так і на війська противника.

З метою досягнення вказаних вище цілей було безпосередньо задіяно роботу з національними медіа, встановлено абсолютний контакт з усіма редакціями, розпочато роботу з найбільшою аудиторією національного марафону, із залученням речника фронту.

У рамках розбудови стратегічних комунікацій спільно з іншими структурами державної влади було запропоновано з ініціативи Президента України проведення інформаційної кампанії “Фортеця Бахмут”, а одним із її найпопулярніших елементів стала уже загальновідома пісня та відеокліп “Байрактар”.

Проведено кампанію з відбору спікерів безпосередньо у підрозділах та бригадах. Їх усіх було пробрифінговано, для них було підготовлено наративи, проведено певний вишкіл, розроблено інструкцію для редакторських колективів. Внаслідок проведеної роботи вдалося створити певне суголосся, яке змогло показати ситуацію на місцях завдяки виступам офіційних речників і заздалегідь підготовлених спікерів безпосередньо у підрозділах – але контрольовано, без витоку зайвої інформації. Для прикладу, наше суспільство могло дізнатися про події у Бахмуті, де і зараз тривають важкі бої.

Особливої уваги заслуговує робота з іноземними ЗМІ, адже розуміємо, що від того, як саме Україна представлена у їхньому інформаційному просторі, залежить підтримка нашої держави в очах їхніх громадян, що у західних демократіях напряму корелює із розмірами фінансової та військової допомоги.

Укоренилась практика щотижневої співпраці з декількома потужними іноземними ЗМІ. Зокрема, було організовано низку інтерв'ю Командувача в таких відомих виданнях, як "The Economist", "TheWashingtonPost", "Ей-Бі-Сі", "ВВС" та ін.

Це, у свою чергу, дозволило донести до західних суспільств ситуацію безпосередньо з поля бою, висвітлюючи думку одного з головних людей, від якого залежить порядок дій на цьому напрямку.

Окрім зазначених вище інструментів інформаційної боротьби, використовуються і соціальні мережі, серед яких є офіційні та неофіційні сторінки наших структур. Для прикладу, на сторінці Сухопутних військ - більше 800 тис. підписників, а на каналі у Telegram - більше 50 тисяч.

До нововведень можна віднести сторінку Командувача в Telegram, адже цей месенджер є одним із найбільш трендових соціальних медіа, популярність якого росте великими темпами, а ми, у свою чергу, не могли не дати відповідь на цей виклик часу. Зауважимо, що протягом пів року перегляди сторінки зросли до 47 тис. відвідувачів, інформація, що розміщена на ній, стала першоджерелом для багатьох національних і закордонних медіа. Це інформаційне джерело застосовується не лише для інформування, але й, певною мірою, пропаганди. Наприклад, з дозволу Командувача та наших спеціальних служб ми, показували там інтерв'ю російських полонених, де ті розповідали про ставлення до них російських командирів, що стало певним деморалізуючим фактором для ворога.

Окрім соціальних медіа, використовується такий потужний ресурс, як робота з документалістикою для глорифікації, в тому числі наших воїнів, наших героїв, для створення хроніки цієї війни і розповсюдження такого роду інформації на якнайбільшу аудиторію.

Вийшли також фільми, серед яких документальна двосерійна стрічка, приурочена річниці Харківської операції – "Битва за Харків", кожна серія якої розповідає про одну з перших потужних українських перемог.

Низку документалістики було створено спільно з міжнародними партнерами. Таким чином, у наших стратегічних комунікаціях наявний і елемент "publicdiplomacy".

Створено близько семи фільмів про злочини росіян, які були скоєні на нашій землі, кінострічки про наші перемоги. Декілька кінокартин продубльовано субтитрами. Один із фільмів — про жінок, які воюють у лавах сил оборони, — презентовано в Брюсселі на Конференції з гендерних питань.

Резюмуючи, можна стверджувати, що у доволі короткі терміни було створено підґрунтя для розбудови цілісної системи стратегічних комунікації в ОСУВ "Хортиця" та в ЗСУ в цілому, перші результати роботи якої переконують у її доцільності, ефективності, великих можливостях та невичерпному потенціалі.

Олександр ЧЕЧИН, м.н.с.
ХНУПС ім. Івана Кожедуба
ORCID: 0009-0007-0974-1330
E-mail: aclapky@gmail.com

ВІЙСЬКОВА СИМВОЛІКА, ЯК ЗАСІБ ПУБЛІЧНОЇ ДИПЛОМАТІЇ. НА ПРИКЛАДІ ДОСВІДУ ХАРКІВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ПОВІТРЯНИХ СИЛ

Публічна дипломатія та заходи на її підтримку – важлива складова стратегічних комунікацій. Основна мета публічної дипломатії полягає у створенні позитивного іміджу Збройних Сил України. Шляхи вирішення цієї задачі можуть бути різними, тут використовуються і спільні військові навчання, і різноманітні науково-освітні та спортивні заходи.

Однією з важливих складових позитивного іміджу є засоби візуальної комунікації. Візуальна комунікація доволі широке поняття, яке охоплює різноманітну графіку, дизайн, рекламу і в тому числі – військову символіку. Остання повинна сформувати чіткий неповторний образ, ідентифікувати та інформувати. Окрім цього, військову символіку, особливо нарукавну, можна вважати інструментом культурного брендингу, або навіть – культурного обміну, в буквальному сенсі. Тому така символіка повинна врахувати традиції української геральдики, містити історичний підтекст, підкреслювати національну сутність, самобутність та приваблювати глядача.

З 2015 року триває ребрендинг українського війська, основні цілі якого, замінити радянсько-імперський спадок на українські військові національно-історичні традиції; впровадити такі візуальні маркери, які на багато років вперед визначають ідентичність нашого війська та закріплять всесвітньо відомий бренд – Збройні Сили України [1].

Основна увага в цій важливій роботі приділяється загальній символіці видів Збройних Сил та символіці бойових частин. Однак не менш важливою задачею є оновлення символіки вищих військових навчальних закладів.

Наприклад, Харківській національний університет Повітряних Сил є провідним освітньо-науковим видовим закладом вищої освіти Збройних Сил України. Університет має давні традиції міжнародного співробітництва, є активним учасником міжнародних освітніх та професійних асоціацій. Заклад займає високі позиції у національних та міжнародних рейтингах, а також має великий досвід в сфері публічної дипломатії.

В Харківському національному університеті Повітряних Сил створено новий геральдичний комплекс символіки університету. Робота тривала у тісній співпраці з фахівцями Українського геральдичного товариства.

В основу символіки університету було покладено оригінальний символ, який отримав назву “Хрест орла”.

Символічне зображення хижих птахів в військовій символіці має дуже давні історичні корені. В римській армії, після реформ Гая Марія (приблизно 1 століття до н.е.), орел став основним символом армії Риму. А використання хижого птаха, як символу військової авіації, почалося ще в часи Першої світової війни. В українській авіації малюнок птаха можна зустріти на літаках часів Перших визвольних змагань 1917-1922 років.

В сучасній українській авіації традиція нанесення малюнків хижих птахів на літаки зберіглася. Також орел використовується в символіці Повітряних сил Збройних Сил України, зокрема у якості знаку на пілотку.

Саме тому було прийнято рішення покласти в основу символіки університету образ хижого птаха, що повністю відповідає українським та світовим мілітарним традиціям.

“Хрест орла” є стилізованим зображенням, яке створено на основі козацького (запорозького) хреста, з видозміненими вершиною та перекладиною, рисунок 1. В своїх “кігтях” орел тримає Тризуб Повітряних Сил [3].

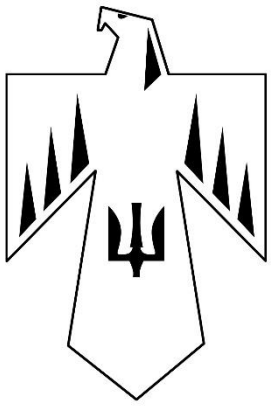


Рисунок 1. Фігура “Хрест орла”
Автор Олександр Чечин

Вершина “Хреста орла” заміщена головою хижого птаха. Верхні промені перекладини вирівняні та утворюють складені крила. Для підсилення образу птаха на крилах та шиї фігури розташоване стилізоване пір'я, у вигляді трикутників.

Подібна форма хреста часто зустрічається в українській фалеристиці. Наприклад, подібний хрест є основою відзнак “Хрест Сімона Петлюри” та її сучасного перевтілення – медалі МО України “Хрест доблесті” [2].

Основа хреста загострена, що притаманно символіці Української Повстанської армії. Такий хрест з загостреною основою іноді називають – хрест-меч. Яскравим прикладом використання фігури хрест-меч є “Хрест заслуги УПА”,

створений у 1944 році відомим українським художником Нілом Хасевичем. Дизайн Хасевича був повторений у сучасній відзнаці МО України “Хрест хоробрих” [2]. Зовнішній вигляд відзнак представлено у таблиці 1.

Таблиця 1. Українські військові відзнаки різних часів

			
Хрест Сімона Петлюри (1932 р.)	Сучасна відзнака МО України Медаль “Хрест доблесті”	“Хрест Заслуги УПА” (1944 р.)	Сучасна відзнака МО України “Хрест хоробрих”

Отже, “Хрест орла” не є простим поєднанням форм української геральдики, він уособлює нерозривний зв’язок університету зі світовою та українською мілітарною історією; враховує традиції української символіки; містить історичний підтекст та підкреслює національну сутність.

Використання такої неповторної фігури у символіці університету, безумовно викликає жвавий інтерес, а яскрава розповідь про історичні основи “Хреста орла” стає одним з заходів публічної дипломатії.

Список використаних джерел:

1. Ребрендінг армії. – Назва з екрана. – Режим доступу: https://www.mil.gov.ua/ministry/zmi-pro-nas/2018/02/02/rebrending-armii/. – Дата перегляду : 16.09.2023.

2. Заохочувальні відзнаки Міністерства оборони України. – Назва з екрана. – Режим доступу: https://www.mil.gov.ua/ministry/simvolika-ta-nagorodi/zaoxochuvalni-vidznaki-mou.html. – Дата перегляду : 16.09.2023.

3. Ярослав Тинченко. Символічний спадок Скоропадського у Збройних Силах України. – Назва з екрана. – Режим доступу: https://tyzhden.ua/symvolichnyj-spadok-skoropadskoho-u-zbrojnykh-sylakh-ukrainy/. – Дата перегляду : 16.09.2023.

Сергій ЧУБ
ORCID: 0009-0001-3703-9414
E-mail: sergijcub83@gmail.com
Кирило НІКОЛАЄВ, к.с.н., доц.
МАУП
ORCID: 0000-0003-0404-6113
E-mail: nikolaev.kirill@gmail.com

НАЦІОНАЛЬНА СТІЙКІСТЬ ЯК ОСНОВА ЄВРОПЕЙСЬКОЇ БЕЗПЕКОВОЇ СТРАТЕГІЇ ДЛЯ УКРАЇНИ

Під національною стійкістю можемо розуміти концепцію, що відображає здатність держави або нації в цілому витримувати та протистояти різноманітним внутрішнім і зовнішнім загрозам, тискам і викликам без зазначення серйозних збоїв або відступів від своїх стратегічних і національних цілей. При цьому не варто ототожнювати національну стійкість та національну безпеку. Національна безпека є дещо вужчим поняттям, яке передбачає збереження цілісності держави у військовому плані та у якості захисту від загроз розвалу цілісності держави, тоді як національна стійкість передбачає протидію загрозам на всіх фронтах: економіка, політика, військово-політична, гуманітарна, інформаційна, екологічна тощо. Та передбачає не стільки реагування на загрози, що виникли, але радше формування серед громадян та державних інституцій здатності випереджати їх появи та створення свого роду "імунітету", щодо несприйняття як мінімум гібридних загроз [1].

Відповідно до стратегії, запропонованою НІСД, національна стійкість має три орієнтири: забезпечення статусу Quo, стійкість на межі, стійкість для оновлення [2]. Реалії сучасної України поєднують два останні компоненти, адже паралельно з протидією загрозам варто готувати і оновлення, особливо для деокупованих територій.

В такому випадку, у ході розгляду інструментів європейської системи безпеки щодо побудови національної стійкості ми маємо звернути увагу на те, як саме і які засоби безпекової системи, притаманні ЄС дозволять протидіяти в межах України зовнішнім загрозам (в першу чергу з боку російського агресора) та побудові серед громадськості свідомого ставлення до спроб гібридних атак з боку ворога, адже тематика гібридності військових дій на сьогодні є одним з найактуальніших для світової сфери безпеки.

Власне на наш погляд, національна стійкість буде забезпечена найбільшою мірою за умови певних гарантій національної безпеки. Старі системи гарантій, які б підтримувалися виключно словом низки світових держав у гібридних умовах сучасності вже не діють та відбувається повернення практик початку XX ст. у плані блоковості. В такому випадку, доєднання України до певних блоків, члени-учасники яких би гарантували безпеку один одному була б більш дієвішою. Звісно, ми не можемо вказувати, що приєднання до відповідної структури є панацеєю та убезпечить

від майбутніх військових протистоянь, але учасники блоку як мінімум надають військову та фінансову підтримку один одному, що допомагає в синтезі з готовністю власне певної держави, а в нашому випадку України, до ведення війни проти ворога.

Власне, в самому ЄС визнають, що наразі у світі, що швидко змінюється, проблеми безпеки стають складнішими, багатовимірними та змінними. Жодна держава-член ЄС не може протистояти цим загрозам сама. Коли йдеться про безпеку, інтереси всіх держав-членів нерозривно пов'язані. Відповідна колективна безпека є системою допомоги та важелів утримання: військових, фінансових. В рамках європейської системи безпеки існує два варіанти подібної безпекової стратегії: НАТО та власне європейська система безпеки, як окремого військово-політичного угрупування [3]. Співпраця ЄС і НАТО є невід'ємною опорою роботи ЄС, спрямованої на зміцнення європейської безпеки та оборони, як частину реалізації Глобальної стратегії ЄС. В рамках співпраці з НАТО було підписано декілька спільних декларацій та схвалено спільні пакети пропозицій Радами ЄС і НАТО.

Співпраця між ЄС і НАТО тепер є усталеною нормою та повсякденною практикою та продовжує відбуватися на основі ключових керівних принципів: відкритості, прозорості, інклюзивності та взаємності, з повною повагою до автономії прийняття рішень і процедур обох організацій без завдає шкоди особливому характеру політики безпеки та оборони будь-якої держави-члена.

Для України наразі членство в НАТО є одним із пріоритетів, але варто врахувати позицію європейських держав та поєднати ймовірне приєднання до НАТО з власною безпековою стратегією, адже перед НАТО стоять в пріоритеті більш колективна безпека і немає гарантій повноцінної військової допомоги (під чим ми розуміємо власне надання миротворчих сил), а можливим є обмеження військовою технічною підтримкою (озброєння, стратегії тощо). В свою чергу, доєднання до європейської безпекової стратегії створює систему важелів та противаг в межах самих держав-учасників, практично убезпечуючи одна від одної та враховуючи територіальну спорідненість регіонів та більшу залежність держав між собою, відповідний інструмент сприятиме усім членам.

Список використаних джерел:

1. Національна стійкість України: стратегія забезпечення. *Український географічний журнал.* 2022. URL: https://ukrgeojournal.org.ua/sites/default/files/UGZ_2022_2_003.pdf.
2. Резнікова О. Розбудова національної стійкості: концептуальні підходи, передові світові практики. Київ : НІСД, 2019. 20 с. URL: https://niss.gov.ua/sites/default/files/2019-11/roa_presentation_niss_v01.pdf.
3. A stronger EU on security and defence. URL: https://www.eeas.europa.eu/eeas/stronger-eu-security-and-defence_en.

Kateryna AKIMOVA, graduate cadet
National University of Civil Protection of Ukraine
ORCID: 0009-0001-6406-3911
E-mail: akimovakaterine@ukr.net

DEVELOPMENT OF ADMINISTRATIVE DECISIONS DIRECTED TO INCREASE THE LEVEL OF PROTECTION OF THE POPULATION AND THE TERRITORIES OF THE KHOLODONHIRSK DISTRICT OF KHARKIV FROM DANGEROUS EVENTS

At present, the issue of martial law, which has been implemented on the territory of Ukraine, is an urgent one. Let's discuss Kharkiv region, namely the Kholodnohirsky district. Today, the adoption of targeted and rational management decisions by the local Kharkiv authorities regarding to the condition of the shelters located in the Kholodnohirsky district remains a relevant and open matter.

State-management decisions are an important element of the state management system, with the help of which the goal of actions is achieved. The beginning of the state management process is a change in the security conditions of the operation or development of the management object [1].

When considering the problems of the selected district, it is necessary to focus attention on its features, namely, the number of storage facilities and shelters located on the territory of the district and their suitability for use as intended.

A storage facility is a hermetic structure for the protection of people, where conditions are created for a certain time that exclude the influence of dangerous factors that arise as a result of an emergency situation, military (combat) actions, and terrorist attacks [2].

An anti-radiation shelter is a non-hermetic structure for the protection of people, where conditions that exclude the impact of ionizing radiation on them in the event of radioactive contamination of the area and the action of conventional means of destruction are created [2].

The simplest shelter is a fortification structure, a basement, another structure of the underground space, where people can stay temporary in order to reduce the combined damage from dangerous factors, as well as from the action of means of damage in a special period [2].

On the territory of the Kholodnohirsky district there are 31 places where storage facilities are located, among which 8 are ready for use, 1 is limited, and 22 are not ready for the use of the population of the district [3].

Also, the lack of anti-radiation shelters and the lack of information for the population about the condition and list of the simplest shelters (basements of residential buildings) that can be located nearby are no less acute problems.

In the area of 141 of the simplest shelters, there is no information about their condition, there is also an underground parking lot, but it does not meet the established requirements and cannot perform the functions of a full-fledged shelter. There are subway stations in the area such as:

subway station Kholodna Gora has a capacity of 700 people;

subway station Pivdenny Vokzal (The South Railway Station) has a capacity of 820 people;

subway station Tsentralny Rynok (The central Market) has a capacity of 800 people [3].

Therefore, based on the above, we conclude that it is expedient to implement management decisions on the territory of the district not only during the war period, but also in the post-war period in order to ensure the required level of security of the district, because the Kharkiv region borders on the enemy's borders.

The state of shelters in the Kholodnohirsky district does not meet the rules and regulations, and is inefficient and cannot fully guarantee the safety of the population.

Among the recommendations, it would be likely to emphasize the issue of arranging existing shelters and sharpening attention during new buildings that will already have shelters of the appropriate level in the project. As an example, let’s pay attention to the system of multi-apartment and private buildings in Israel.

References

1. Liashevska O.I. Teoretychni aspekty derzhavnoho upravlinnia ta pryiniattia derzhavno-upravlinskykh rishen: Visnyk NUTsZ Ukrainy. Seriia: Derzhavne upravlinnia, vypusk 2(17)2022. Posylannia na elektronnyi resurs: http://repositsc.nuczu.edu.ua/bitstream/123456789/16884/1/Liashevska.pdf.
2. Kodeks tsyvilnoho zakhystu Ukrainy vid 02.10. 2012 r. № 5403- VI. Vidomosti Verkhovnoi Rady. 2013.(№ 34-35). S.458.
3. Pasport Kholodnohirskoho raionu shchodo zakhystu naselennia pid chas vynyknennia nadzvychainykh sytuatsii ta v osoblyvyi period. Kharkiv 2022.

Дмитро БОВСУНІВСЬКИЙ
ЖВІ ім. С.П. Корольова
ORCID: 0009-0002-5868-5252
E-mail: skif928@gmail.com

РОЛЬ МЕДІА В ФОРМУВАННІ ГРОМАДСЬКОЇ ДУМКИ ТА СТЕРЕОТИПІВ

У сучасну інформаційну епоху засоби масової інформації відіграють ключову роль у формуванні громадської думки та увічненні суспільних стереотипів.

Оскільки суспільство стає все більш взаємопов'язаним через різні медіа-платформи, вкрай важливо уважно вивчити вплив цих засобів на переконання, ставлення та поведінку людей.

По-перше, засоби масової інформації служать основним джерелом інформації для широкої громадськості. Новинні агентства, платформи соціальних медіа та індустрії розваг сприяють формуванню громадської думки через контент, який вони створюють. Інформація, представлена в цих середовищах, може сильно вплинути на те, як люди сприймають і розуміють навколишній світ. Однак точність і об'єктивність цієї інформації може значно відрізнятися, що призводить до потенційних упереджень і спотворень. Крім того, засоби масової інформації мають силу зміцнювати або кидати виклик існуючим стереотипам у суспільстві. Чи то через новини, фільми чи рекламу, медіа-репрезентації можуть увічнити упереджені уявлення та узагальнення про певні групи, що призводить до створення та зміцнення стереотипів.

Ці стереотипи не лише впливають на цільові групи, але й формують суспільне ставлення та поведінку до них. Крім того, власність і контроль над засобами масової інформації відіграють життєво важливу роль у формуванні громадської думки. Концентрація влади ЗМІ серед кількох впливових організацій може обмежити різноманітність точок зору та придушити голоси незгодних. Така концентрація влади може привести до узагальнення ідей і думок, потенційно впливаючи на громадську думку в тому чи іншому напрямку. Більше того, те, як ЗМІ зображують певні проблеми, може сильно вплинути на громадську думку.

Упередженість висвітлення, формулювання та встановлення порядку денного все це методи, що Використовуються медіа-організаціями для формування того, як події та теми сприймаються громадськістю. Вибірково виділяючи певні аспекти проблеми, ігноруючи інші, засоби масової інформації можуть формувати громадську думку та створювати спотворене сприйняття реальності. Важливо усвідомити потенційні негативні наслідки ролі медіа у формуванні громадської думки та увічненні стереотипів. Неточне або упереджене повідомлення може призвести до поширення неправдивої інформації та невігластва серед громадськості, що призведе до розбіжностей у суспільстві. Ці розбіжності можуть перешкоджати прогресу, закріплювати дискримінацію та поглиблювати суспільну нерівність.

На закінчення, роль ЗМІ у формуванні громадської думки і стереотипів не можна не помітити. Медіа мають владу формувати суспільні переконання та ставлення через інформацію, яку вони представляють, стереотипи, які вони Увічнюють, та контроль, який вони здійснюють над публічним дискурсом. Як відповідальним споживачам медіа, вкрай важливо критично аналізувати та ставити під сумнів інформацію, яку ми отримуємо, щоб забезпечити більш поінформоване та інклюзивне суспільство.

Список використаних джерел:

1. Роль засобів масової інформації у формуванні громадянського суспільства України. ULR: https://core.ac.uk/download/pdf/48399666.pdf (дата доступу до статі 16.09.2023).
2. Вплив ЗМІ на формування громадської думки. Кравчук В.М., Дмитрусь О.А. URL: http://www.lsej.org.ua/6_2015/4.pdf (дата доступу до статі 19.09.2023).

Олександр ВОЙТКО, к.в.н., доц.
НУОУ
ORCID: 0000-0002-4610-4476
Ксенія ЄРГІДЗЕЙ, к.пед.н.
НУОУ
ORCID: 0000-0003-4634-133X
Дмитро СІМАНСЬКИЙ
НУОУ
ORCID: 0009-0003-4882-8309

СПРОМОЖНОСТІ СИЛ ОБОРОНИ УКРАЇНИ ЩОДО ВИРОБНИЦТВА МЕДІА-КОНТЕНТУ У ПРОЦЕСІ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ – ПРАКТИЧНИЙ АСПЕКТ

За класичною схемою планування комунікації першим пунктом плану має бути мета комунікації. З 24 лютого 2022 року мета усіх українців – одна на всіх, зрозуміла і проста – Перемога.

Така концентрація викликає зрозумілі й видимі наслідки. Зараз фактично уся комунікація (у тому числі й комунікації стратегічні, державні, Сил оборони) стала кризовою. Усе робиться в режимі “на вчора”. Цілі проєктів стають максимально короткотерміновими, тривалість кампаній ще більше зменшується, увага цільових авдиторій (українського народу) переключається навіть не щодня, а кілька разів на день. І при цьому кожен раз вона повертається до головного – війни (перемоги, виживання) [1].

Приклад ефективності української стратегічної комунікації: за результатами соцдослідження більшість закарпатських угорців вважають, що Угорщина має надати Україні зброю. За це виступає 53,6% опитаних представників угорської громади, при цьому 28,8% мають протилежну думку. Саме росію відповідальною за війну вважають 71,4% опитаних угорців, які проживають на Закарпатті. Тоді як в Угорщині, за даними останнього дослідження Globsec, проведеного у березні цього року, частка населення, яке вважає Росію відповідальною за війну, складає 54% [2].

Про визначення кілька слів. Стратегічна комунікація – це спроможність влади, це можливість будувати тривалу стратегію й інструменти впливу на мільйони для когнітивних змін (ефектів).

Якими мають процеси (дії) в комунікації Сил оборони? Відповідно, якими мають бути спроможності для оборонного планування на основі спроможностей (ОПОС)? ОПОС передбачає більш широку рамку планування, але більш чіткі та вимірювані результати, які досягаються за рахунок процесів, стандартизованих за рахунок описання ефектів, яких ми маємо досягнути.

Для бізнес чи політичної комунікації перелік таких процесів давно відомий та описаний. Відкритим є питання, чи мають комунікаційні процеси (і спроможності – відповідно) в армії суттєво відрізнятися від таких в інших державних інституціях, у бізнесі чи політиці?

Треба для початку відзначити абсолютно новий характер сучасної війни з росією. Якщо раніше комунікація була лише оздобою бойових дій (пропаганда, дезінформація), то нині – це ще один дуже важливий фронт. Фронт, на якому успіхи Сил оборони України дуже вагомі та помітні. Ключовий показник успіху в комунікації в час війни – небачена єдність українського народу в прагненні перемоги та дедалі більш вагома підтримка нашої боротьби з боку міжнародної спільноти.

Виходячи з вже наявного досвіду ведення інформаційної війни та участі в ній підрозділів Сил оборони (а також – настанов НАТО, відповідно до нашої заявленої мети вступу в Альянс) можна стверджувати, що перелік/набір процесів комунікації ЗСУ суттєво не відрізняється від такого в інших державних інституцій, а бізнес- та політичні проєкти лише переважають бюджетами та здатністю більш масштабно та гнучко залучати фахівців.

Серед основних практичних задач фахівців-комунікаційників в силах оборони:

моніторинг комунікаційний простір (це значно більше, ніж раніше, коли були лише традиційні ЗМІ);

аналіз і дослідження процесів комунікації, передбачення дії противника та інших суб’єктів;

стратегування та планування;

бюджетування та взаємодія;

виробництво контенту (у всій палітрі);

створення каналів комунікації (не лише традиційні ЗМІ);

отримання зворотнього зв'язку і коригування своїх дій відповідно;

вимірювання результативності своїх дій.

Фахівці з комунікацій Сил оборони України мають бути спроможними творити такий контент:

відео- та фотоматеріали. Як для власного використання (телестудії / відеоблогінг) так і для поширення традиційними ЗМІ та / чи у соцмережах людьми;

документальні фільми, спецрепортажі, рекламні ролики та інші готові до показу відеоматеріали;

новинні повідомлення для власних теле- та радіостанцій;

прес-релізи, повідомлення для преси;

готові інтерв'ю ключових спікерів, історії (сторі) – для ЗМІ;

аналітичні матеріали;

бюлетені, кавер-леттери, брифи;

презентації, макети реклами;

друковану пресу. Найчастіше – для військовослужбовців, інколи – для населення звільнених та прифронтових територій;

прес-заходи, прес-тури;

контент для власних сторінок у соцмережах, для сайтів;

широкий спектр контенту для ворожих авдиторій (без деталізації тут).

Важлива ремарка. В Силах оборони нині відбувається два протинаправлених процеси. З одного боку, стоїть задача по уніфікації та стандартизації усіх процесів, включно з комунікаційними – прагнучи більшої професійності та ефективності. З іншого – ми спостерігаємо постійне множення комунікаційних сутностей, усі підрозділи намагаються виробляти контент, усі займаються ІПСО, кожен взаємодіє з пресою та створює сторінки в соцмережах, збираючи пожертви. Виходячи з описаних абзацом вище спроможностей, треба визнати, що більшість суб'єктів комунікації Сил Оборони не здатні в нинішньому стані забезпечити справді ефективну комунікацію.

Прагнучи стандартизації та внормування процесів виробництва контенту важливо одночасно не загнобити творчу ініціативу окремих командирів та фахівців з комунікації. От якраз тут і потрібні процеси ефективних стратегічних комунікацій та медіа-планування. Так само – як і навчання та підвищення кваліфікації комунікаторів Сил оборони, зокрема в НУОУ [3].

Очевидно, що поширення різного контенту вимагає підвищеної уваги до комунікаційних каналів. Надто зараз, коли створити канал в Ютьюбі не коштує взагалі нічого, а охоплення успішного в Інтернеті мілітарі-блогера перевищує частку/рейтинг невеликого телеканалу. Врешті, хорошою ілюстрацією цієї тези може бути цілком асиметрична перемога української пропаганди над російською у перші місяці після повномасштабного вторгнення. Окупантам довелося терміново закривати соцмережі та залишки опозиційних незалежних ЗМІ, на боротьбу з поширенням української комунікації (зокрема, Сил оборони) виділяються величезні бюджети та чималі зусилля спецслужб.

Як практичний приклад – мобілізація/військкомати. У традиційній парадигмі клієнт ТЦК є командування Сухопутних військ. Але нині війна інша, війна

інформаційного суспільства, стейкхолдери та актори змінилися (див. абзац вище). ЗСУ стали справжнім озброєним авангардом суспільства. Стали не кріпаками, а партнерами у ході визвольної війни, відповідно – інші стосунки, інша комунікація. Не випадково, процес мобілізації в Україні став головною мішенню ворожої ІПСО [4].

Список використаних джерел:

1. Президент затвердив Стратегію деокупації та реінтеграції тимчасово окупованого Криму – Офіційне інтернет-представництво Президента України (president.gov.ua). УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №117/2021 – Офіційне інтернет-представництво Президента України (president.gov.ua).
2. Новина – Опитування: Більшість угорців, які живуть на Закарпатті, звинувачують РФ у агресії (espreso.tv).
3. Інтерньюз-Україна. "Курс стратегічних комунікацій" Лекція 4. Основні елементи стратегічної комунікації (culturepartnership.eu) Київ, 2020. – лекція 4.
4. Наказ Головнокомандувача Збройних Сил України № 70 від 18.03.2023 року "Про затвердження Порядку здійснення стратегічних комунікацій Збройних Сил України".

Лілія ДОРОШИНА, к.філол.н., доц.
НАНГУ
ORCID: 0000-0002-0199-4372
E-mail: doroshyna.lilia@gmail.com

"ІСТОРІЯ" ЯК ЗАСІБ ФОРМУВАННЯ ПОЗИТИВНОГО ІМІДЖУ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Відповідно до Доктрини стратегічних комунікацій Національної гвардії України, зв'язки з громадськістю ґрунтуються на загальних принципах публічного спілкування та є одним із головних елементів системи стратегічних комунікацій Національної гвардії України, що спрямовані на інформаційний супровід діяльності, задоволення інформаційних потреб Національної гвардії України, а також своєчасне, оперативне та об'єктивне інформування громадськості та ЗМІ щодо їх професійної діяльності в мирний час та в особливий період.

Безпосередня відповідальність за організацію зв'язків з громадськістю покладається на офіцерів підрозділів інформації та комунікації у військових частинах Національної гвардії України [1, с. 19].

До провідних засад роботи підрозділу інформації та комунікації військової частини Національної гвардії України належать оперативність, актуальність, законність, достовірність, гнучкість, наступність, конструктивність. А одним із

головних завдань, що визначаються концепцією стратегічних комунікацій Національної гвардії України, є цілеспрямована робота над формуванням позитивного іміджу Нацгвардії.

Під час підготовки матеріалів підрозділи інформації та комунікації Національної гвардії України велику увагу приділяють персоналізації, зокрема створенню й розміщенню "історій", що можуть сформувати позитивну репутацію окремого військовослужбовця, підрозділу та Національної гвардії України в цілому.

Наприклад, на офіційному сайті Національної гвардії України [3] один із його елементів, що називається "Категорії новин", містить рубрику "Історії". Ця рубрика складається з репортажів про військовослужбовців Національної гвардії України, кожен із яких показаний передусім як особистість. Відповідно, матеріал, поданий в "історіях", збагачує читачів новими позитивними враженнями, формує в них знання про діяльність Національної гвардії України.

"Історія" повинна бути чесною, гарно написаною й виходити за межі суто інформації. Проте передусім "Історія" повинна бути актуальною.

Актуальність "історії" полягає в усвідомленні читачем думки про те, що на місці цієї людини міг би бути я, що ця історія певним чином стосується мене. "Історії" повинні приваблювати й давати можливість ототожнитися з героєм. Це не означає, що читач повинен хотіти бути таким, як герой. Це означає, що читач зможе зрозуміти, чому ця людина прийняла такі рішення, і як наслідок збагатити власний світогляд [2].

Зі свого боку, щоб підготувати якісний матеріал для рубрики "Історії", офіцерові підрозділу інформації та комунікації Національної гвардії України потрібні глибоке занурення в тему, інтерес та емпатія.

Отже, підрозділи інформації та комунікації Національної гвардії України під час підготовки матеріалів повинні й надалі приділяти значну увагу персоналізації, зокрема створенню й розміщенню "історій", формуванню позитивного іміджу Нацгвардії та ефективному продукуванню відповідного інформаційного контенту про її діяльність.

Список використаних джерел:

1. Доктрина стратегічних комунікацій Національної гвардії України: затв. Наказом командувача Національної гвардії України від 22.11.2021 № 541. 2021. 30 с.

2. Паплаускайте Марічка. Кожна історія у світі стосується любові та смерті. URL: https://reporters.media/kozhna-istoriya-u-sviti/.

3. Національна Гвардія України. Категорія: Історії https://ngu.gov.ua/category/istoriyi/.

Мирослава КОСИГІНА
ЖВІ ім. С.П. Корольова
ORCID: 0009-0001-1400-776X
E-mail: Miroslava1508@gmail.com

АНАЛІЗ ІНОЗЕМНОГО НЕГАТИВНОГО ІНФОРМАЦІЙНОГО ВПЛИВУ НА УКРАЇНУ

ХХІ століття переповнює безліч альтернативних джерел інформації у вільному доступі. Ми постійно перебуваємо в інформаційному просторі у якому безперервно йде боротьба за панування та домінування. Уїнстон Черчилль казав: “Хто володіє інформацією, той володіє світом”.

Дивлячись телебачення чи слухаючи радіо ми досить рідко ставим під сумнів щойно сприйняте. Зазвичай це стається завдяки дії прийому новизни, або ж прийому довіри до авторитету. Враховуючи різні ступені обізнаності, різні рівні довіри до мас-медіа, різні рівні можливостей та доступу до інформації державі досить важко гарантувати інформаційну безпеку населення, а точніше захищеність від психологічного впливу на них.

Європа є нашим другом, який нам допомагає і підтримує, до якого ми прислуховуємося, а також який має досить вагомий вплив на нашу державу. Наразі майже не існує європейської держави в якій не існувало б політиків, що підтримують проросійські погляди. Тому ми можемо говорити про так званий негативний інформаційний вплив Європи на Україну. Певні держслужбовці систематично у виступах висловлюються на користь РФ у російсько-українській війні.

Майже ніхто з відомих західних публічних діячів, які в минулому робили проросійські заяви, не наважився підтримати Кремль безпосередньо після вторгнення Росії в Україну, бомбардуючи житлові будинки та енергетичну інфраструктуру. Ті, хто захоплювався Путіним, та підтримував анексію Криму до початку великої війни, тепер потайки переключилися на нові наративи, вигідні Москві. Тепер політики критикують постачання зброї в Україну і закликають до миру шляхом переговорів з Росією. Головна мета прокремлівських наративів – зробити Україну знесиленою і дозволити Росії зміцнити контроль над захопленими територіями.

Слід виділити різні причин такої поведінки політиків. Одні щиро вірять у свою справу та у користь, що принесуть рідній державі. Однак це хибна думка, що припинивши допомогу Україні їхня держава відновить економіку, позбудеться переселенців, працюватиме над своїм добробутом і найголовніше - досягне домовленостей з Путіним про мир. Інакший прототип проросійського політика це – людина, яка має старі зв’язки та друзів з Росії, або навіть отримує кошти за свою роботу.

Віддані часом щирі друзі Кремля за кордоном готові його підтримувати, захищати та відстоювати правоту російської політики на різних рівнях. Необхідно зрозуміти чи здатні вони переконати в цьому своїх співгромадян. Сесіль Вессьє каже: “Те, що я описую у Франції (мова йдеться про проросійських політичних діячів), відбувається і в інших європейських країнах. Днями в Німеччині вийшла книга Бориса Райтшустера. Те ж саме відбувається і в Чехії. Ондрей Кундра написав про це книгу, а ваші колеги зняли фільм “Чеські друзі Кремля”. Тобто це вже якась європейська політика, яка ведеться з Кремля.” [1].

Чимало впливових демократичних політиків бояться роз’яснити своїм громадянам, що Російська Федерація веде війну на знищення українського народу та української державності. Є особистості, які з нетерпінням чекають коли врешті-решт Україна перестане опиратися і погодиться на капітуляцію. Мовляв, під Путіним, чи ні – все одно там вирощуватимуть пшеницю, соняшник, добуватимуть руду і дешево експортуватимуть в Європу й Азію [3].

Центр “Нова Європа” у 2018 році виокремив низку інструментів, до яких Росія найчастіше вдавалася, аби зламати політичну волю країн ЄС. За останні сім місяців Москва застосовувала усі наявні важелі, вигадуючи нові, щоб налякати, схилити європейців до пом’якшення підходів. Використання ядерного шантажу стало улюбленою ідеєю російської пропаганди вже давно (впливові пропагандисти країни погрожували перетворити США на ядерний попіл ще у 2014 році). Для Путіна важливо демонструвати, що він не перебуває в повній ізоляції і до нього дослухаються провідні лідери західних країн. Особливим аспектом ділового та економічного впливу був енергетичний компонент, який використовувався для ефективного тиску на країни-члени ЄС. Головною опорою Росії у країнах ЄС залишаються політики маргінального табору – крайні праві чи крайні ліві [4].

Проросійські політики мали схожі наративи, які змінювалися відповідно до ходу дій війни. У Франції ці наративи озвучували Ле Пен, Земмур, Меланшон, Маріані та Філіппо. Варто зауважити, що лідерка французьких ультраправих протягом багатьох років підтримувала тісні зв'язки з Путіним. Ле Пен заявляла про своє захоплення Путіним, підтримку його політики та анексії Криму, незважаючи на порушення Москвою прав людини та міжнародного права. Наразі політик засудила військову агресію Росії і підтримала постачання оборонної зброї Україні, але виступила проти постачання наступальної зброї, стверджуючи, що це може спровокувати війну між Росією і НАТО. Для того щоб зрозуміти рівень підтримки народом такої позиції достатньо знати, що у квітні 2023 року Марін мала досить великий шанс виграти на президентських виборах чинного президента Франції Емануеля Макрона.

У Італії цю риторику просували Сальвіні, Фонтана та Орсіні. В свою чергу Сальвіні як лідер італійської ультраправої партії “Ліга” Маттео Сальвіні заявляв, що західні санкції проти Росії не працюють і фактично шкодять Італії, тому їх потрібно переглянути [5]. У Німеччині ці заклики підтримували Вагенкнехт, Кра і

Шварцер. Віктор Орбан в Угорщині. Цей список далеко не вичерпний. Реальність така, що західна зброя заважає Росії захоплювати більше українських земель, а російська окупація призвела до масового терору. Зіткнувшись з невдачами у війні, Росія посилила пропаганду, а псевдо пацифісти ставлять за мету не лише послабити Україну, але й підірвати Європу.

Рятуючи українське "сьогодні", євроатлантичне суспільство рятує своє власне "завтра". Більше сучасної зброї вмілому й мотивованому українському воїнові дає більше шансів на перемогу демократії над фашистською Росією [3].

Низка світових держав намагаються затягнути Україну за стіл переговорів про мир із Росією, наввипередки пропонуючи свої "мирні плани". Це не заклик до миру, це лише виправдання російської агресії.

Світові лідери – Китаю, країн Африки, Бразилії, Туреччини та навіть Папа Римський – запропонували Україні свої "мирні" плани, і жоден із них не передбачає повну перемогу держави у війні з РФ. Водночас Україна наполягає на своєму мирному плані, запропонованому ще восени 2022 року президентом Володимиром Зеленським. У його Офісі наголошують, що основна вимога до Росії задля мирних перемовин – виведення її військ із українських територій [6].

Ми не можемо на пряму стверджувати, що дії проросійських політиків вплинули на хід війни. Однак ми стовідсотково знаємо, що влада це слуга народу. Будь-який хороший президент чи депутат зобов'язаний прислуховуватися до думки народу та діяти на основі аналізу усіх вхідних. Коли політики чи активісти з проросійськими ідеями залучаються підтримкою народу вище керівництво держави не може це ігнорувати. Отже, проросійські держслужбовці свідомо намагаються вплинути на народ, залучитися його підтримкою і таким чином змінити хід війни у гіршу для України сторону.

Список використаних джерел:

1. Хто і за скільки підтримує політику Кремля у Франції? URL: https://www.radiosvoboda.org/a/27696506.html (дата звернення: 18.09.2023).
2. БАКТЕРІЇ "РУССКОГО МИРА" URL: https://texty.org.ua/projects/108282/bakteriyi-russkoho-myra-hto-pidtrymuye-rosiyu-v-yevropi/ (дата звернення: 18.09.2023).
3. Чому допомога Україні життєво необхідна самим НАТО і ЄС? URL: https://www.radiosvoboda.org/a/viyna-rosiyi-ukrayina-nato-yes/31763689.html (дата звернення: 18.09.2023).
4. 8 інструментів російського впливу: як Україні зберегти підтримку громадян ЄС URL: https://www.eurointegration.com.ua/articles/2022/10/18/7148825/ (дата звернення: 18.09.2023).
5. URL: https://www.eurointegration.com.ua/news/2022/09/5/7146155/ (дата звернення: 18.09.2023).

6. Який “мир” нав’язують Україні у війні з Росією і чому агресорка не готова до миру URL: https://tsn.ua/exclusive/yakiy-mir-nav-yazuyut-ukrayini-u-viyni-z-rosiyeyu-i-chomu-agresorka-ne-gotova-do-miru-2339827.html (дата звернення: 18.09.2023).

Ірина ЛИСИЧКІНА, к.філол.н., доц.
ORCID: 0000-0002-2050-9379
e-mail: ilysychkina@nangu.edu.ua
Ольга ЛИСИЧКІНА, к.філол.н., доц.
НАНГУ
ORCID: 0000-0002-9511-9615
e-mail: olysychkina@gmail.com

КОГНІТИВНА ВІЙНА: НОВІ СПРОМОЖНОСТІ ЧИ НОВИЙ ТЕРМІН?

В останні роки термін “когнітивна війна” все частіше зустрічається в наукових публікаціях у секторі безпеки та міцно вкорінюється в сучасній парадигмі гібридної війни, що свідчить про ситуацію військового протистояння, у якій потенційно можливе перепрограмування свідомості за допомогою сучасних технологій з метою нав'язування волі противнику без використання засобів традиційної війни або їх мінімізації. Когнітивну війну описують як використання засобів громадської думки, психологічних і юридичних методів для досягнення перемоги. При цьому дослідники зауважують, що власне когнітивна війна не може вигравати війни [1], хоча вона надає нові спроможності.

Мета цього дослідження полягає в окресленні особливостей когнітивної війни, які роблять її унікальною та розкривають її функціональний потенціал.

Згідно з розвідками НАТО [2], когнітивна війна включає в себе дії, проведені в синхронізації з іншими інструментами впливу з метою впливати на установки та поведінку, впливаючи, захищаючи або руйнуючи пізнавальні процеси на індивідуальному, груповому або популяційному рівні, щоб здобути перевагу над противником. Розроблена з метою модифікації сприйняття реальності, маніпуляція на рівні всього суспільства стала новою нормою, і це робить психічні процеси людини ключовим аспектом війни.

У Китаї когнітивну війну пов’язують із “трьома битвами” [3]: битвою за громадську думку для впливу на внутрішню та міжнародну думку громадськості, психологічною війною для шокування та деморалізації ворожих військових і цивільних осіб, і юридичною війною для отримання міжнародної підтримки через міжнародне та внутрішнє право.

Боротьба в когнітивному середовищі безпосередньо впливає на мозок, здійснюючи вплив на емоції, мотиви, судження та дії, і навіть контролюючи мозок

противника та широкої аудиторії. Мозок стає ключовим полем бою в сучасних війнах, і китайські стратеги вважають, що підсвідомий контроль над мозком ворога може викликати психічні пошкодження та змусити його відкласти зброю.

Об'єднане командування з трансформації НАТО (NATO ACT) веде роботу щодо експериментального концепту когнітивної війни, який є частиною загального Плану розвитку бойових операцій [3]. Враховуючи зростання синхронізації впливу на емоційні та підсвідомі аспекти противника, розуміння моделей, визначень, впливів і ризиків стає ключовим для прийняття належних політичних рішень, розвитку військових спроможностей та забезпечення загальної безпеки Альянсу.

Когнітивне впливове втручання часто відбувається через соціальні медіа, як-то: Facebook, Twitter, YouTube, Instagram, а також веб-сайти, інструменти, додатки/застосунки та гаджети, які надають послуги соціальних медіа. Використання пропаганди, дезінформації, обману та інформаційно-впливових заходів не є новим явищем. Новим є легкість, ефективність, низькі витрати, глобальна доступність і швидкість поширення, за допомогою яких політичні відчуття людей стосовно національної та міжнародної думки тепер можуть бути маніпульовані. Практично не можливо контролювати, хто має доступ до цієї можливості.

Когнітивна війна є ширшим поняттям порівняно з інформаційною війною, оскільки вона охоплює багато різних аспектів і відбувається в мультимодальному просторі. Це включає в себе вплив на науку та освіту з метою трансформації процесів мислення та обробки інформації.

Очевидно, що інструментарій когнітивної війни потребує систематизації та включення до нього творів літератури та кінематографу, оскільки когнітивна війна кодується в словах, образах та подіях.

Методологію когнітивної війни становить набір стратегій і методів, спрямованих на вплив на психологічну і когнітивну сферу індивідів та/або груп (часто противника) з метою досягнення певних політичних, військових або інших цілей. Ця методологія включає в себе такі основні аспекти: пропаганда, дезінформація та маніпуляція інформацією, психологічний вплив, соціальна інженерія, спостереження та аналіз, контрпропаганда та захист (зокрема через освіту, тренування та розвиток антикогнітивних стратегій), аналіз інтернаціональних аспектів та можливостей співпраці для протидії когнітивним загрозам.

Загалом, когнітивна війна стає все більш важливою складовою сучасних конфліктів та міжнародної безпеки, і розуміння її принципів та методів стає критично важливим для забезпечення національної та міжнародної стабільності.

Подальші розвідки з обраної проблематики дозволять краще зрозуміти сутність когнітивної війни, стратегії її ведення та протидії.

Список використаних джерел:

1. Takagi K. The Future of China's Cognitive Warfare: Lessons from the War in Ukraine, *The Hudson,* 22 July 2022. URL: https://www.hudson.org/research/17991-the-future-of-china-s-cognitive-warfare-lessons-from-the-war-in-ukraine (доступ 15.09.2023).
2. Cognitive Warfare: Beyond Military Information Support Operations. *ACT. Articles.* 9.05.2023. URL: https://www.act.nato.int/article/cognitive-warfare-beyond-military-information-support-operations/ (доступ 15.09.2023).
3. Kania E. The PLA's Latest Strategic Thinking on the Three Warfares. *China Brief Volume*: 16 Issue: 13. 22.08.2016. URL: https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/ (доступ 15.09.2023).

Валентина МІРОШНІЧЕНКО, д.п.н., проф.,
ORCID: 0000-0002-3931-0888
E-mail: mvi_2016@ukr.net
Вадим ЖУРАВЛЬОВ, к.псих.н., доц.,
НАДПСУ ім. Богдана Хмельницького
ORCID: 0000-0002-5209-290X
E-mail: zhuravliov067@ukr.net

ОСОБЛИВОСТІ ФОРМ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ НА ВІЙСЬКОВОСЛУЖБОВЦВ ТА ЦИВІЛЬНЕ НАСЕЛЕННЯ

Інформаційно-психологічний вплив є комплексом заздалегідь продуманих, спланованих та підготовлених дій та заходів. До об'єктів, на які він поширюється, відносять цивільну та військову інфраструктуру з інформації, морально-психологічний стан військовослужбовців та цивільного населення противника з метою досягти воєнні, політико-економічні та психологічні цілі.

Мета такого впливу містить, як завдання шкоди технічному стану збройних сил (озброєння і бойової техніки), так і поширення неправдивої інформації, деморалізацію військовослужбовців та цивільного населення противника. Адже інформація поряд із зброєю є вагомим чинником протиборства у сучасних умовах. Тому інформаційно-психологічний вплив стосується зрушень у свідомості особистості і здатний змінити морально-психологічний станвійськовослужбовців та цивільного населення.

Зовнішня сторона, організацій аспект інформаційно-психологічного впливу виявляється у різновиді його форм. Щодо шляхів та способів, завдяки яким інформаційно-психологічний вплив реалізується, то це його методи.

Такі фактори, як політична мета та масштаби війни, воєнно-політична обстановка у світі загалом та певній країні, морально-психологічний стан військовослужбовців та цивільного населення, є визначальними для вибору форм інформаційно-психологічного впливу.

До основних форм інформаційно-психологічного впливу відносять:

інформаційно-психологічні операції яксукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем і часом інформаційно-психологічних акцій та дій, які проводятьсяспланово, одночасно за визначеною послідовністю, з дотриманням єдиного задумуз метою вирішити конкретні завдання у конкретний час;

інформаційно-психологічні акції, що є обмеженимиу розумінні часу та масштабу заходами, коли інформаційно-психологічний вплив здійснюється на конкретний об'єкт (групу об'єктів);

інформаційно-психологічні дії, що єсукупністю узгоджених у розумінні мети, завдань, простору та часу заходів інформаційно-психологічного впливу.

Маємо врахувати, що заходи інформаційно-психологічного впливу проводять обидві воюючі сторони. Зокрема, у підручнику "Психологія бою" про дії з боку агресора зазначається, "щоб ужити заходів інформаційно-психологічного впливу задля підриву морально-психологічного стану наших військ, члени незаконних збройних формувань використовують широкий арсенал форм. Основними формами інформаційного впливу на підрозділи Збройних Сил є: друкована пропаганда; усна пропаганда; радіопропаганда; телевізійна пропаганда; інтернет" [1, с. 70–71]. Як переконує досвід, найефективнішими формами інформаційно-психологічного впливу на військовослужбовців та цивільне населення є різні види пропаганди; соціальні мережі.

Дослідники звертають увагу на "здійснення впливу під час діяльності у спілкуванні та на наявність визначених цілей психологічного впливу. У стихійних поведінка регулюється завдяки специфічним механізмам впливу, дія яких спостерігається і в організованих, але в стихійних вона переважає" [2, с. 158]. Вплив інформації на окремі групи людей, переважно, здійснюється у ході інформаційно-психологічних операцій, якими використовується інформація, щоб впливати на поведінку особистості через його психіку.

Отже, інформаційно-психологічний вплив є комплексом заздалегідь продуманих, спланованих та підготовлених дій та заходів. До об'єктів, на які він поширюється, відносять цивільну та військову інфраструктуру з інформації, морально-психологічний стан військовослужбовців та цивільного населення противника з метою досягти воєнні, політико-економічні та психологічні цілі. У сучасних умовах російсько-української війни та тимчасової окупації росією окремих територій сходу та півдня України існує необхідність вивчення форм, методів та принципів інформаційно-психологічного впливу з метою, з одного боку, забезпечити захист наших військовослужбовців та цивільне населення від

негативного інформаційно-психологічного впливу, з іншого боку, ефективно застосувати різні форми інформаційно-психологічного впливу проти ворога.

Список використаних джерел:

1. Психологія бою: посібник / Грицевич Т.Л., Гузенко І.М., Капінус О.С., Мацевко Т.М., Романишин А.М.; за ред. А.М. Романишина. Львів: Вид-во “Астролябія”, 2017. 352 с.

2. Корольчук М. С., Крайнюк В. М. Соціально-психологічне забезпечення діяльності в звичайних та екстремальних умовах : навч. посіб. для студ. вищих навч. закладів. Київ : Ніка-центр, 2006. 580 с.

Тетяна МУЖАНОВА, к.держ.упр., доц.
ORCID: 0000-0002-7435-0287
E-mail: muzanovat@gmail.com
Юрій ЩАВІНСЬКИЙ, к.т.н.
ORCID: 0000-0002-2319-8983
E-mail: yushchavinsky@ukr.net
Віталій ТИЩЕНКО
ДУІКТ
ORCID: 0000-0003-3849-6243
E-mail: tvs5vetal@gmail.com

ОСОБЛИВОСТІ ЗДІЙСНЕННЯ УРЯДОВИХ ЗВ’ЯЗКІВ ІЗ ГРОМАДСЬКІСТЮ В УМОВАХ МЕРЕЖЕВОГО СЕРЕДОВИЩА

Відносний стан демократії значною мірою залежить від кількості та якості інформації, яка циркулює між державою і суспільством, між урядовими установами та громадянами. У свою чергу, урядові зв’язки з громадськістю природнім чином відображають усі зміни в суспільстві та інформаційному середовищі.

Сучасне суспільство пройшло кілька інформаційних революцій, у результаті яких відбулися зміни у вартості, потоках і розподілі інформації з глибокими наслідками для балансу сил між державою і громадянами. Цим змінам сприяли також процеси еволюції інформаційно-комунікаційних технологій, внаслідок яких спостерігається створення надмірної кількості інформації, дешевої і легкодоступної, більш симетрично розподіленої між споживачами через нелінійні мережеві потоки.

У результаті виникнення глобальної мережі Інтернет переважаючий упродовж багатьох десятиліть ієрархічний порядок поширення інформації

(вертикальний із домінуванням одного із суб'єктів) поступово заміщується іншим – рівноправним і двостороннім. Тому при плануванні та здійсненні урядових зв'язків з громадськістю має враховуватися переформатування способу організації суспільства на основі мережевої логіки, яка наголошує на горизонтальних відносинах і силі потоків (які нерідко протистоять потокам влади), зростання значення мережевих структур, які володіють високим потенціалом самоорганізації й мобілізації соціальних груп.

Нарешті змінилася основа довіри між керівництвом держави і громадянами, оскільки сьогодні рівень довіри формується не, як раніше, з моральних почуттів, а за результатами прямих оцінок роботи державних органів [1].

Крім того, уряду необхідно враховувати особливості сучасної людини, якій завдяки використанню новітніх Інтернет-технології часто характерні новий тип мислення та механізми трансляції соціального досвіду, а також все зростаючий індивідуалізм, що ускладнює охоплення бажаних аудиторій повсюдно з використанням єдиного способу надання інформації й комунікації. Нинішнє кіберпокоління за короткий час стає досвідченішим, ніж люди старшого віку, може швидко оволодіти політичними знаннями, цінностями, засвоїти норми поведінки і водночас генерує нові очікування щодо політичного середовища.

Здійснення урядових зв'язків із громадськістю у мережевому просторі має враховувати істотні переваги на відміну від інших видів комунікативної взаємодії, зокрема:

можливості опосередкованої взаємодії будь-якого учасника комунікації з політичними суб'єктами і представниками органів влади через сторінки в соціальних мережах, блоги, чати, електронну пошту, скайп тощо;

розподіленість мережевої комунікації в часі і просторі, що дозволяє учасникам спілкування взаємодіяти незалежно від часу і місця їх перебування;

формування суб'єкт-суб'єктної моделі комунікації, яка передбачає толерантне ставлення до політичної позиції іншого суб'єкта, пошуку компромісів, активне взаємозбагачення всіх учасників комунікації;

відсутність соціальної і вікової диференціації учасників комунікації, завдяки чому авторитет користувача підтримується не соціальним статусом, а рівнем його інтелекту, наявністю власного погляду на політичні процеси, володінням комунікативними і комп'ютерними навичками, частою присутністю в мережі та вміннями здійснювати інтеграційні дії в політичному просторі.

Водночас, необхідно враховувати також і негативні ефекти мережевої комунікації, які суттєво впливають на процеси зв'язків уряду із громадянами.

Так, встановлено, що саме в Інтернет-просторі розгортаються гострі політичні дискусії, у результаті яких посилюється політичне протистояння, зростає рівень напруженості в суспільстві.

Швидкість мережевої комунікації, фрагментарність і мозаїчність змісту інформації мають наслідком інформаційне перевантаження людини, викликають роздратування й агресію.

З огляду на величезні обсяги інформації, нерідко суперечливої та провокаційної за змістом, яку людина не здатна опрацювати, виникає проблема оцінки й відбору інформації, розташування її в певній логічній послідовності. Надмірна кількість інформації заважає ґрунтовно аналізувати суспільно-політичні процеси, стримує політичну активність у реальному житті.

До того ж активність у віртуальному політичному просторі, яка не підкріплюється реальною діяльністю може стати причиною розвитку "симулятивної" політичної суб'єктності, яка не завжди переростає в справжню.

Також не можна забувати, що мережеві технології непомітно для людини закріплюють в її пам'яті будь-яку інформацію і в такий спосіб формують її потреби, інтереси, цінності, політичні погляди. Тому будь-який користувач завжди є потенційною жертвою маніпулятивних впливів, в тому числі з метою зміни його політичних уподобань [2].

Крім того, на думку дослідників [3], реальною є небезпека, так званої, нетократії - нової форми управління суспільством, за якої основною цінністю є інформація, а доступ до достовірної інформації і маніпуляції з нею можуть надавати владу над групою, суспільством чи державою.

Відповідно, держава має шукати і знаходити вихід із цих фундаментальних змін, використовуючи владу мережевих потоків і забезпечуючи більш ефективну комунікацію з громадянами у рамках зв'язків із громадськістю.

Уряд має ефективно використовувати мережеві платформи для спілкування з громадянами, створювати приводи для частого спілкування та взаємодії, формувати активну громадську позицію й бажання брати участь у вирішенні нагальних проблем життєдіяльності суспільства.

Як показує практика, традиційні ЗМІ програють Інтернет-ресурсам у контексті охоплення аудиторій і впливу на їхні вподобання, зменшуючи можливості громадян для ініціювання діалогу з державними органами. Крім того, відсутність індивідуального підходу обмежує силу односторонньої масової комунікації, ставлячи під сумнів ефективність кампаній у ЗМІ. Водночас, дослідження свідчать, що громадяни, які хочуть брати участь у політичній дискусії, більш схильні здійснювати комунікацію через соціальні мережі та онлайн-медіа, а не покладатися на традиційні ЗМІ й інституційні джерела [1].

Саме тому уряд має інтегрувати нові технологічні платформи у систему зв'язків із громадськістю, збільшуючи таким чином кількість доступних мережевих медіа, з яких громадяни можуть отримати доступ до інформації й надати зворотний зв'язок.

З метою підвищення ефективності зв'язків уряду з громадськістю доцільно: використовувати мережеві опитування й інші форми збору даних, щоб установити

підходи до пошуку й споживання інформації серед членів цільової аудиторії; заручитися підтримкою недержавних організацій, які користуються довірою цільової аудиторії, і залучити їх до мережевої комунікації як лідерів громадської думки; використовувати потенціал міжособистісного мережевого середовища цільової аудиторії та найбільш звичні і зручні для неї способи комунікації; застосовувати інтерактивні можливості соціальних медіа як для інформування громадян, так і надання ними відгуків і пропозицій щодо державної політики.

Отже, для узгодження методів урядових зв'язків із громадськістю та комунікаційних потреб громадян необхідним є створення структури мережевих комунікацій, яка має забезпечити врахування характеру й мотивів цільових аудиторій, загальну різноманітність джерел і каналів для їх охоплення, зрозумілий та орієнтований на споживача інформації зміст повідомлень, можливості зворотного зв'язку, а також вбудованість інформаційних потоків у соціально-політичний контекст.

Список використаних джерел:

1. Young L., Pieterson W. Strategic Communication in a Networked World: Integrating Network and Communication Theories in the Context of Government to Citizen Communication : The Routledge Handbook of Strategic Communication. Routledge Taylor & Francis Group, 2019. P.p. 93-112.

2. Краснякова О. А. Інтернет-комунікація як чинник становлення політичної суб'єктності особистості. URL: https://core.ac.uk/download/pdf/77240744.pdf.

3. Висоцька О.Є. Феномен мережевої комунікації в умовах сьогодення. URL: https://ir.nmu.org.ua.

Борис МУНТЯН, к.і.н, доц.
ВА (м.Одеса)
ORCID: 0000-0002-1284-4660
E-mail: bobmuntian2018@ukr.net

ОПЕРАЦІЯ "БАДІГАРД": ВИСНОВКИ ТА УРОКИ

В сучасних умовах з метою якісної підготовки та успішного проведення інформаційно-психологічних операцій важливе значення має вивчення історичного досвіду підготовки та проведення подібних операцій під час світових та локальних війн.

Однією із найбільш успішних дезінформаційних операцій, проведених під час Другої світової війни, вважається операція "Бадігард". Це спеціальна стратегічна дезінформаційна операція, що була проведена спецслужбами військ союзників під час

підготовки до їх вторгнення на територію Франції (операція “Оверлорд”). **Мета операції полягала у введенні в оману воєнно-політичного керівництва Німеччини щодо часу та місця десантування військ союзників.**

В межах загального плану проведення операції “Бадігард” були розроблені й реалізовані близько 35 часткових планів операцій, що розвивали, конкретизували і деталізували загальний план за певними напрямками. Так, наприклад, згідно плану операції “Фортитьюд” проводилися два комплекси дезінформаційних заходів, спрямованих на імітацію вторгнення військ союзників, перший – на узбережжя Норвегії (план “Фортитьюд-Північ”), другий – на північне узбережжя Франції в районі Па-де-Кале (план “Фортитьюд-Південь”). За планом операції “Ейрборн Сігар” здійснювалося радіоелектронне придушення засобів управління протиповітряною обороною противника під час переходу морем та десантування військ союзників і т. д.

Проведенню заходів за планом операції “Бадігард” передувала активізація роботи контррозвідувальних органів союзників. Вона була спрямована на зачистку та ліквідацію на території Великої Британії широко розгалуженої мережі німецьких шпигунів. Наявність такої мережі була обумовлена тим, що в 30-их роках минулого століття в аристократичних колах Великої Британії було багато прихильників Адольфа Гітлера та його нацистського режиму. Одним із таких прихильників був навіть британський король Едуард VIII. Німецька розвідка в повній мірі скористалася такою необачною прихильністю британської аристократії і створила на території Великої Британії потужну шпигунську мережу. Тому, під час підготовки до проведення операції “Оверлорд”, у контррозвідки союзників було достатньо роботи щодо виявлення та нейтралізації німецьких агентів. Треба відмітити, що контррозвідка союзників діяла швидко, рішуче і ефективно. За короткий час у вищому політичному та військовому середовищах були виявлені та нейтралізовані майже всі німецькі шпигуни. Більше двохсот із них були завербовані контррозвідкою союзників і саме через цих подвійних агентів німецькій розвідці поставлялася, в подальшому, хибна інформація.

Другим дієвим заходом контррозвідки союзників, проведеним у співпраці із вищим військовим керівництвом союзників, стало відпрацювання планів операцій “Оверлорд” та “Бадігард” в умовах надзвичайної таємності. З метою запобігання витокам таємної інформації було максимально обмежено коло посадових осіб, які залучалися до планування операцій. Робота з документами була організована у спеціально обладнаних приміщеннях, що виключало їх прослуховування. Виносити документи за межі цих приміщень було категорично заборонено. Контроль за дотриманням режиму таємності здійснювався високопоставленими співробітниками контррозвідки. Усі, навіть незначні, порушення режиму таємності негайно доповідалися начальнику контррозвідки і Верховному Головнокомандувачу союзними силами в Європі генералу Дуайту Ейзенхауеру.

В останній тиждень перед висадкою режим таємності був посилений і розповсюджений на всі сили вторгнення: британці затримували дипломатичну і

військову пошту, а усіх учасників десантної операції перевели в табори на базах завантаження і заборонили їх залишати. На період переходу десантних кораблів і кораблів супроводження через протоку Ла-Манш була введена сувора заборона на використання радіозв'язку. Навіть у разі пошкодження або загибелі корабля було заборонено подавати міжнародний сигнал лиха (SOS).

Німецьке командування вважало найбільш вірогідним місцем вторгнення військ союзників на територію Франції – район Па-де-Кале. Тому союзникам залишалося лише підтримувати упевненість німців в тому, що саме тут буде район десантування їх військ. На це і була спрямована операція "Бадігард".

Заходи операції "Бадігард" здійснювалися по двох основних напрямах:

поширення хибної інформації про час і місце вторгнення військ союзників;

створення на території Великої Британії штучних ознак зосередження військ і військової техніки.

Поширення хибної інформації здійснювалося шляхом:

дезінформації німецької розвідки через подвійних агентів, завербованих контррозвідкою союзників (найбільш дієвий і ефективний метод);

розповсюдження, через засоби масової інформації нейтральних країн, фальшивих відомостей щодо плану підготовки та проведення операції;

використання актора Мейріка Джеймса в якості двійника британського фельдмаршала Бернарда Монтгомері, який прибув до Гібралтара і довів до командування дислокованих там британських військ план захоплення південного побережжя Франції. Німецьке командування, отримавши цю інформацію, продовжило дислокацію своїх військ на півдні Франції. Метод доволі екзотичний, однак виявився дуже ефективним за своїм результатом.

З метою імітація районів зосередження військ і сил флоту у південно-східній частині Англії (у районі проливу Па-де-Кале) було створено 1-шу групу армій США (імітувала вторгнення на узбережжя Франції), а на півночі Англії 4-ту британську армію (імітувала вторгнення на узбережжя Норвегії). В дійсності цих угрупувань військ не існувало. Їх сили і засоби імітувалися за допомогою декількох тисяч макетів танків і літаків, штучних аеродромів, надувних десантних і бойових кораблів. Окрім цього були створені два фальшиві штаби, які безперервно обмінювалися між собою хибною інформацією.

Також здійснювались демонстративні виходи кораблів з десантом в море, їх слідування в напрямку Па-де-Коле і наступне повернення в порти базування. Це робилося з метою приспати пильність противника, щоб він не зміг відрізнити реальний вихід на початку операції від тренувального виходу.

Крім того, авіація союзників до останнього утримувалася від нанесення масованих ударів в Нормандії і бомбардувала об'єкти поблизу Па-де-Кале, посилюючи впевненість німецького командування про підготовку вторгнення саме в цьому місці.

В результаті реалізації заходів операції "Бадігард" на момент початку операції "Оверлорд" головні німецькі сили були зосереджені в районі Па-де-Кале на відстані

250 кілометрів від реального місця висадки військ союзників. Дата початку операції також стала повною несподіванкою для німецького командування. Навіть з початком вторгнення Гітлер вважав висадку союзників в Нормандії відволікаючим маневром і тільки через деякий час віддав наказ передислокувати туди додаткові сили.

ВИСНОВКИ ТА УРОКИ:

1. Операція "Бадігард" стала однією із найбільш успішних операцій по дезінформації противника, проведених під час Другої світової війни,

2. Мета операції "Бадігард" була повністю досягнута. Час початку операції "Оверлорд" та місце її проведення стали повною несподіванкою для воєнно-політичного керівництва Німеччини. Це обумовило успішне проведення операції "Оверлорд" та досягнення її цілей.

Аналіз матеріалу, викладеного у тезах дає змогу сформулювати декілька уроків, що зберігають свою актуальність і в сучасних умовах:

Урок № 1. Запорукою успішних бойових дій Збройних Сил України у війні проти російських окупантів є рішуча і ефективна робота контррозвідувальних органів спрямована на виявлення та нейтралізацію російських шпигунів на усіх ланках українського воєнно-політичного керівництва.

Урок № 2. Сучасні інформаційно-психологічні операції є ефективним засобом збереження в таємниці своїх планів та введення противника в оману.

Урок № 3. Ефективним засобом введення противника в оману щодо дислокації і зосередження угрупувань військ є дерев'яні та надувні макети бойової та спеціальної техніки, імітація роботи засобів зв'язку, використання засобів радіоелектронної боротьби.

Олександр ПЕРЕГУДА, к.т.н., с.н.с.
ORCID: 0000-0001-8802-0740
E-mail: perenshtein@gmail.com
Олена ЧЕРКЕС
ORCID: 0000-0002-2623-5364
E-mail: romantikwymen@gmail.com
Петро ПІОНТКІВСЬКИЙ, к.т.н., с.н.с.
ЖВІ ім. С. П. Корольова
ORCID: 0000-0002-9103-5393
E-mail: 005mk@ukr.net

РОЛЬ КЛАСТЕРНИХ ОСЕРЕДКІВ В ОРГАНІЗАЦІЙНО-ШТАТНІЙ СТРУКТУРІ ВИЩОГО ВІЙСЬКОВОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Суттєве збільшення кількості різноманітних зразків озброєння та військової техніки (далі – ОВТ) для Збройних Сил України зумовлює інтенсифікацію

процесів взаємодії з установами та організаціями, які беруть участь у створені оборонних технологій та сприяють розробці та постачанню нових видів озброєння.

Сьогодні в Україні розвивається кластер Brave1, який виступає єдиною координаційною платформою для підтримки впровадження сучасних технологій та розробок у сфері оборони. Замовлення від Міністерства оборони України, Генерального штабу Збройних Сил України на розробки та надання грантів – з одного боку, стартапи від бізнесу – з іншого, створюють державно-приватне партнерство у якому бізнес забезпечує інвестування, а держава деякі привілеї (наприклад, знижений рівень податкового навантаження, надання виробничих потужностей, інфраструктури). Невідповідність вимогам сучасності (воєнно-політичним, економічним, технічним) організаційно-штатної структури підрозділів вищих військових навчальних закладів (ВВНЗ), які залучені до співпраці з Brave1, проявляються в площині взаємодії з стейкхолдерами.

Рівень впливу зовнішнього середовища на організаційну складову ВВНЗ обумовлює як “можливості” так і “загрози”. До загроз слід віднести наявність значної кількості проблемних організаційно-правових питань які виникають при узгодженні спільної діяльності, наприклад, забезпечення інформаційної взаємодії шляхом обміну знаннями під час спільного вирішення проблем, врегулювання протоколів взаємодій розробників озброєння та експертних груп з проведення випробувань (досліджень) ОВТ тощо. Застосування альтернативних механізмів до способів взаємодії, зумовлює “можливості”, а саме – необхідність змінювати (впроваджувати нові) підходи до формування організаційно-штатної структури підрозділів ВВНЗ, які беруть участь у організації спільних заходів з розробниками ОВТ: освітніх консультацій, презентацій експериментальних зразків ОВТ, розробленні та реалізації спільних програм і проєктів, спрямованих на покращення рівня технологічного стану Збройних Сил України, проведенні військової експертизи тощо.

Жорстка функціонально-лінійна ієрархічна організаційна структура характерна для підрозділів ВВНЗ, не дозволяє швидко реагувати на зміни у організації спільної діяльності з розробниками ОВТ через функціональну замкненість структурних підрозділів, обмеження сфери діяльності (відповідальності) структурного підрозділу/виконавця положеннями та посадовими інструкціями, надмірний рівень централізації, гіперформалізації що вимагає виконання складних формальних процедур, узгодження вищого керівництва (як наслідок втрачається оперативність та актуальність).

Застосування принципів адаптивних (адхократичних, горизонтальних) організаційних структур дає можливість адаптуватись (пристосовуватись) до змін у зовнішньому середовищі. Тому пропонуємо для організаційно-штатної структури підрозділів ВВНЗ, які співпрацюють з розробниками ОВТ, впроваджувати кластерну організаційну структуру (як різновид матричної).

Сутність кластерних осередків в організаційно-штатній структурі ВВНЗ полягає в інтеграції груп зацікавлених фахівців (за погодженням вищого керівництва) з пріоритетних напрямків розвитку або діяльності, що зорієнтована на впровадження інноваційних нововведень.

Кластерні форми організації взаємодії використовують горизонтальну координацію співпраці. При цьому фахівці в кластері можуть мати різні ролі наприклад, лідер, адміністратор проекту, коуч, тощо. Різні ролі можуть суміщатись одною людиною, або одна роль може бути розподілена між декількома людьми. Це дає можливість коригування діяльності, перерозподілу функцій, професійного розвитку окремих фахівців. Залучення курсантів ВВНЗ до кластерів фахівці якого мають високий рівень інженерно-технічної підготовки дає можливість внести елементи креативності у вирішення проблемних питань, так як це підвищує спроможності щодо генерування нових ідей та свіжих підходів.

Приклади можливих кластерів: групи фахівців за тематичними напрямами (розвиток систем та засобів радіоелектронної розвідки, радіоелектронної боротьби, кібербезпеки, удосконалення технічної реалізації розробок (HARD, (SOFT), тощо); групи фахівців за функціональними напрямами (керівники груп/штабний кластер, логістичне, фінансово-економічне та юридичне забезпечення, підвищення кваліфікації, підтримка та розвиток редакційно-видавничої діяльності, інше).

В рамках кластера визначається: основні заходи (семінари, курси); плани розвитку; розглядаються пропозиції від розробників ОВТ, щодо організації спільних заходів; здійснюється пошук інноваційних рішень та підходів, що допоможуть посилити технологічні можливості ОВТ.

В цілому кластерний підхід є затребуваний для підтримки та розвитку інновацій, так як спонукає фахівців експериментувати, тестувати нові підходи, обирати нетривіальні шляхи для розв’язання задач у короткий термін.

Список використаних джерел:

1. Офіційна сторінка Brave1. Brave1 – кластер підтримки Defense Tech розробок в Україні. URL: https://brave1.gov.ua/ (дата звернення 11.09.2023).
2. Національна програма кластерного розвитку до 2027 . Концепція. Орієнтири розвитку. Рекомендації. INDUSTRY4 UKRAINE. 2020. URL: https://www. industry4ukraine.net/publications/proyektnaczionalnoyi-programy-klasternogorozvytku-do-2027/. (дата звернення 11.09.2023).
3. Про затвердження Положення про порядок створення і функціонування технопарків та інноваційних структур інших типів: Постанова Кабінету Міністрів України від 22.05.1996 р. № 549 (поточна редакція від 25.08.2004). URL: https://zakon.rada.gov.ua/laws/show/ 549-96-п#Text. (дата звернення 11.09.2023).

Дмитро ПОЛІЩУК
НАДПСУ ім. Богдана Хмельницького
ORCID: 0000-0003-0425-1651
E-mail: polischykdm@gmail.com

МЕТОДИКА ОРГАНІЗАЦІЇ ВЗАЄМОДІЇ СУБ'ЄКТІВ ІНТЕГРОВАНОГО УПРАВЛІННЯ КОРДОНАМИ ЩОДО ПРОТИДІЇ ТЕРОРИЗМУ В МІЖНАРОДНИХ ПУНКТАХ ПРОПУСКУ

Реалізація державної політики з питань протидії тероризму в Україні здійснюється силами та засобами єдиної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків. Складовими такої системи є територіальна та функціональна підсистеми. Взаємозв'язок між зазначеними підсистеми організовується і здійснюється шляхом: обміну інформацією про загрозу вчинення терористичних актів; проведення спільних оперативно-розшукових та інших заходів; проведення моніторингу стану і тенденцій поширення тероризму в Україні та за її межами; організації і проведення командно-штабних та тактико-спеціальних навчань і тренувань з використанням сил і засобів суб'єктів боротьби з тероризмом.

В результаті аналізу досвіду діяльності правоохоронних органів України щодо боротьби з тероризмом встановлено, що терористична діяльність, може виникати як на території держави так і за її межами, й поширюватись між державами. Тому заходи з протидії тероризму лише в межах території України не надають можливість у повному обсязі протидіяти терористичній діяльності зокрема на транскордонних каналах її прояву. Тут ефективним інструментом є механізм інтегрованого управління кордонами (ІУК), зокрема в межах системи контролю за в'їздом та перебуванням в Україні іноземців та осіб без громадянства: у державах їх походження, у суміжних з Україною державах, у пунктах пропуску і поза ними та на території України.

Суб'єкти ІУК одночасно є й суб'єктами системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків.

Організація взаємодії суб'єктів ІУК полягає у проведенні комплексу заходів з підготовки до виконання покладених завдань з протидії тероризму та дій у разі зміни обстановки зумовлених впливом терористичної діяльності. Вона спрямована на об'єднання зусиль суб'єктів ІУК для протидії тероризму.

Взаємодія суб'єктів ІУК з протидії тероризму в пунктах пропуску організовується за завданнями, імовірними варіантами впливу терористичної діяльності і варіантами дій посадових осіб, що надають випереджувальну інформації про ознаки терористичної діяльності та здійснюють контроль за перетинанням державного кордону осіб, транспортних засобів і вантажів.

Слід зазначити, що Державна прикордонна служба уповноважена законодавством України організовувати взаємодію контрольних органів і служб, що здійснюють різні види контролю в пунктах пропуску.

Отже, начальник прикордонного загону або окремого контрольно-пропускного пункту Державної прикордонної служби України під час організації взаємодії із уповноваженими посадовими особами суб'єктів ІУК з питань протидії тероризму у пунктах пропуску узгоджує питання, зокрема, щодо порядку:

обміну даними про ознаки терористичної діяльності;

проведення перевірки за базами даних Державної прикордонної служби України та Інтерполу;

проведення відповідних процедур та використання механізму взаємного доступу до інформаційних систем;

використання можливостей міжнародного співробітництва з правоохоронними органами та організаціями Інтерпол, Європол, Євроюст;

використання можливостей програмно-аналітичних модулів обробки інформації PNR (за зразком Automated Targeting System - GLOBAL);

використання продуктів кримінального аналізу;

дій персоналу, що обслуговує пункт пропуску у випадку отримання інформації або виявлення ознак терористичної діяльності;

дій, в рамках співпраці з ОБСЄ, з реалізації спільних проектів щодо підвищення спроможностей у протидії тероризму, виявленню зброї, боєприпасів, небезпечних хімічних речовин та розвитку аналізу ризиків.

Таким чином, методика організації взаємодії суб'єктів ІУК щодо протидії тероризму полягає у сукупності взаємозв'язаних способів та прийомів доцільного проведення зазначених заходів.

Анна ТОПОРЕНКО
НУЦЗУ
ORCID: 0009-0002-8329-0770
E-mail: toporenko87@gmail.com

ВПЛИВ КОНТЕНТУ ЗМІ НА ПСИХІЧНЕ ТА ЕМОЦІЙНЕ БЛАГОПОЛУЧЧЯ ЛЮДЕЙ ПІД ЧАС ВІЙНИ

Засоби масової інформації, такі як телебачення, радіо, газети, інтернет-новини та соціальні мережі, відіграють важливу роль у сприйнятті та розумінні військових конфліктів. Сучасні медіа розширюють потік інформації про воєнні події, які наразі відбуваються на території нашої держави та можуть призводити до психологічної та емоційної травми не тільки серед осіб, які безпосередньо перебувають у зоні конфлікту, але й серед тих, хто далеко від реальних зон бойових дій.

Основною метою масмедійного відображення воєнних подій на тлі інформаційного простору є інформування громадськості та донесення фактів.

Вбудовані для монетизації алгоритми, яким поклоняються багато платформ соціальних медіа, можуть гарантувати, що люди не лише отримають новини, але й отримають їх у розрахований спосіб, який може ще більше сприяти їхньому постійному споживанню медіа [1]. Однак, це може супроводжуватися надмірним емоційним стресом для глядачів та читачів, які стикаються з жорстокими та шокуючими зображеннями і відеороликами. Під впливом інформаційних подій простежуються різні емоційні реакції на масмедійний контент, включаючи страх, гнів, безпомічність та тривогу. Ці емоційні реакції можуть значно впливати на психічне та емоційне благополуччя людей, особливо на тих, хто вже раніше зазнав травм, пов'язаних з війною, або має близьких, які безпосередньо брали участь у бойових діях. Тому важливо, щоб медіа-індустрія приймала відповідальність за вплив своєї звітності на психічне та емоційне здоров'я і добробут суспільства, забезпечуючи баланс та етичну публікацію інформації.

Отже, зрозуміння впливу мас-медіа на психічне та емоційне благополуччя людей під час воєнних дій має важливе значення для розвитку програм психологічної підтримки і психотерапії для тих, хто стикається з цим впливом. Дослідження цього питання може допомогти удосконалити психічну реабілітацію і підтримку ветеранів та інших постраждалих від військових конфліктів. Важливо продовжувати дослідження в цій області та розробляти ефективні підходи до психологічної допомоги, щоб гарантувати збереження гармонійного психічного та емоційного благополуччя ветеранів і цивільних осіб, задіяних у військових конфліктах. Роблячи це, можливо прагнути до створення суспільства, здатного впоратися з психологічними проблемами, що виникають внаслідок впливу ЗМІ під час війни.

Список використаних джерел:

1. Леві Р. (2021). Соціальні медіа, споживання новин і поляризація: докази польового експерименту. American Economic Review , 111(3), 831–870. https://doi.org/10.1257/aer.20191777.

Anastasia MATSAKOVA, graduate cadet
National University of Civil Protection of Ukraine
ORCID: 0009-0001-1369-8984
Email: matsakova200@gmail.com

IMPORTANCE AND FEATURES OF PSYCHOLOGICAL SUPPORT IN MILITARY STRUCTURES

Psychological support in military structures plays one of the main and strategically important roles for the effective functioning and achievement of the goals of military organizations.

Key aspects of this role include:

Maintaining Combat Readiness: Psychologists in the military help service members maintain a high level of combat readiness. They work on the development of psychological stability and stress resistance, which are important during combat operations.

Stress management: Military personnel are exposed to significant psychological stress during service. Psychologists help manage stress, conduct individual and group consultations to reduce the impact of stress factors.

Support for veterans: Psychological support also includes support for veterans who may be experiencing psychological difficulties such as post-traumatic stress disorder (PTSD). Providing adequate psychological assistance to veterans is an important aspect of the social responsibility of military structures.

Decision support: Psychologists can participate in the development of strategies and tactics based on psychological analyzes that help improve decisions at the military command level.

Psychological preparation for international missions: If a military organization participates in international missions, psychologists prepare personnel to work in a different cultural and social environment, help eliminate cultural differences and support psychological adaptation.

Professional and personal development: Psychological support contributes to the development of servicemen as professionals and as individuals, which contributes to increasing their professional competence and a sense of satisfaction from service.

Ethical aspects of military activity: Psychologists also contribute to the formation of military ethics and help military personnel make ethically sound decisions, especially in situations involving moral dilemmas.

One of the most important issues for discussion is the peculiarities of the psychological support of military personnel during peacetime and combat periods.

After all, a full-scale war is currently going on in our country, and the help of a psychologist is an integral part of our struggle.

Psychological support during peacetime:

Professional training: In peacetime, psychologists work on the professional training of military personnel, helping them develop the skills and competencies necessary to perform their duties.

Psychological preparation for mobilization: Psychologists prepare servicemen for possible mobilization in the event of a threat to national security. This includes working with stress resistance and psychological readiness to act in crisis situations.

Supporting Personal Development: Psychologists support the personal development of service members by helping them solve personal problems, improve interpersonal relationships, and develop skills for successful service and life in civilian society.

Psychological support during the combat period:

Stressful situations: During the combat period, military personnel face stressful situations, including military operations, threats to life and health. Psychologists provide psychological support to reduce the impact of stress and traumatic events on mental health.

Post-traumatic stress disorder (PTSD): Military personnel who have been through combat can suffer from PTSD. Psychologists diagnose and treat this disorder, providing vital assistance to military personnel to facilitate their recovery after combat.

Support for combat readiness: Psychologists help maintain a high level of combat readiness by working on the moral support and motivation of military personnel during combat operations.

Team Collaboration: In combat, streamlined communication and collaboration between service members is vital. Psychologists help resolve conflicts and improve team cooperation.

Psychological analysis and decision-making: Psychologists can provide analytical support to the command, helping to analyze the psychological aspects of military operations and to make strategic decisions.

All these aspects of psychological support of servicemen are important both in peacetime and in combat, and are aimed at ensuring their physical and psychological health, as well as increasing their combat effectiveness.

Therefore, summing up, we can say that psychological support is a necessary and strategically important component of military activity, as it contributes to the preservation of combat effectiveness and psychological health of military personnel, and also affects the adoption of important strategic decisions and interaction with the public.

References:

1. Moralno-psykholohichne zabezpechennia u Zbroinykh Sylakh Ukrainy: Pidruchnyk: u 2 ch. Ch.1. Za zah. red. V.V. Stasiuka. K.: NUOU, 2012. 682 s.

2. Ostapenko I.S., Herasymchuk O.A., Kramar I.Ye., Shaptala O.I., Yakovliev S.O., Zhinchyna S.M. Moralno-psykholohichne zabezpechennia pidrozdiliv Derzhspetstranssluzhby. Ukr. derzh. un-t nauky i tekhnolohii. Dnipro, 2022. 188 s.

3. Visnyk Lvivskoho universytetu. Seriia psykholohichni nauky. 2022. Vypusk 13. S. 64–70 Visnyk of the Lviv University. Series Psychological sciences. Issue 13. S. 64–70.

Павло БІРЮКОВ, к. пед. н.
ORCID: 0000-0003-1703-1359
E-mail: birukov_paul@ukr.net
Володимир СЕЛЮК
ВІТІ ім. Героїв Крут
ORCID: 0000-0002-8003-5734
E-mail: sven444@i.ua

СУТНІСТЬ, ФОРМИ ТА СПОСОБИ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ

Постановка проблеми. Довготривале протистояння українського народу та його Сил оборони (568-ий день) широкомасштабній збройній агресії рф загострило проблему протидії інформаційно-психологічного впливу і інформаційних технологій з боку противника. Створення дієвої системи, яка б ефективно захищала та убезпечувала наших військових, українське суспільство від деструктивних впливів російської інформаційно-пропагандистської машини є досить актуальним завданням сьогодення.

Аналіз останніх досліджень та публікацій. Чимало науковців присвятили свої роботи аналізу інформаційно-психологічного протиборства, зокрема: Толубко В.Б., Курбан О.В. та інші, проте цей напрямок потребує постійного дослідження та узагальнення, оскільки російсько-українська війна триває. На сьогодні у вітчизняній науці остаточно ще не визначені єдині концептуальні погляди на проблеми інформаційної боротьби, а також на інформаційно-психологічне протиборство в цілому.

Мета доповіді Дослідити сутність, форми і способи ведення інформаційної війни, відпрацювати дієві механізми протидії деструктивному інформаційно-психологічного впливу та інформаційних технологій рф проти України.

Викладення основного матеріалу За досвідом локальних війн і збройних конфліктів, у т.ч. російсько-української війни, складовими інформаційної війни (далі – ІВ), яка поступово приходить на заміну психологічних операцій, є: радіоелектронна боротьба; психологічні операції; оперативне маскування; фізичне знищення елементів інформаційної інфраструктури; програмний

вплив на комп'ютерні мережі (комп'ютерні атаки); спеціальні інформаційні операції.

ІВ – це дії, які вживаються є метою досягнення інформаційної переваги для підтримання національної воєнної стратегії шляхом впливу на інформацію і інформаційні системи противника, захисту своєї інформації та власних інформаційних систем. Ефективність застосування сил і засобів ІВ визначається її формами і способами. Під способом ведення ІВ розуміється порядок та прийом застосування сил і засобів для захоплення й утримання інформаційної переваги над противником під час підготовки та в ході бойових дій.

Способи ведення ІВ включають в собі:

об'єкти впливу;

вид і послідовність інформаційного впливу на противника;

склад сил та засобів, що призначені для інформаційного впливу та їх оперативну побудову.

За метою та характером дій способи ІВ поділяються на наступальні і оборонні.

Наступальні способи націлені на дезорганізацію чи знищення інформаційної інфраструктури, дезорганізацію управління силами і засобами противника, зниження морально-психологічної стійкості його військ. До них належать: блокування інформації, тиск, інсценування, залякування, провокування, навіювання, виснажування, відвернення уваги, сковування сил противника, перевантаження, умиротворення, дезінтеграції.

До групи *оборонних* способів, які націлені на захист власної інформаційної інфраструктури, процесу управління та морально-психологічного стану своїх військ від впливу противника належить: деблокування інформації, демпфування, ототожнення. Поділ способів носить умовний характер, бо кожна з зазначених груп може використовуватися в наступальних і оборонних операціях.

Сутність способу блокування інформації полягає в тому, що на етапі підготовки і в ході бойових дій шляхом проведення заходів з інформаційної протидії повністю або частково перешкоджається здобування (збір) інформації про обстановку і обмін інформацією в системах управління військами і зброєю противника. Даний спосіб широко застосовувався під час операції багатонаціональних сил "Буря в пустелі" в 1991 році.

Спосіб відвернення уваги полягає в тому, що на етапі підготовки бойових дій шляхом проведення заходів з інформаційної протидії прагнуть створити реальну або фіктивну загрозу для одного з уразливих місць противника і завдяки цьому переконати його в своєму намірі діяти на одному з можливих напрямків з метою відволікання головних сил противника на вирішення другорядних завдань. Так, наприклад, російське командування у липні –

вересні 2023 року розпочало оперативне розгортання військ (сил) на Лимансько-Куп'янському напрямку з метою відволікти Сили оборони України від наступу на півдні.

Спосіб сковування сил противника є різновидом способу відвернення.

Спосіб виснажування полягає в проведенні заходів з інформаційної протидії з метою примусити противника вжити невигідні або даремні дії і, як наслідок, вступити в бій з витраченими ресурсами і зниженою боєздатністю.

Сутність способу інсценування полягає в тому, що противнику нав'язується уявлення про наявність хибної загрози для одного з його уразливих місць.

Реалізація способу дезінтеграції (розколу) полягає в нав'язати противнику уявлення про необхідність діяти всупереч коаліційним інтересам.

Спосіб умиротворення застосовується для нав'язування противнику представлення про нейтральну або союзницьку позицію протидійної сторони. Точно так, як російський диктатор В. Путін заспокоював світову спільноту в січні – лютому 2022 року, що російське збройне угруповання у складі 190 тис. військових, зосереджених на кордонах України, проводить військові навчання та за першою нагодою повернеться у місця постійної дислокації.

Спосіб залякування противника реалізується шляхом доведення до нього інформації, яка має створити уявлення про перевагу протидійної сторони. Як, приклад, постійне залякування світу з боку вищого військово-політичного керівництва рф про застосування тактичної ядерної зброї проти України та початок ІІІ світової війни. Також, Путін під час виступу у російському Владивостоці на Східному економічному форумі 12 вересня 2023 року пригрозив ударами по українським атомних об'єктах у відповідь на дії якихось диверсантів, які нібито готували підрив опори ЛЕП поруч з однією з російських АЕС.

Спосіб провокування противника має метою спровокувати його на здійснення будь-яких дій, вигідних протилежній стороні.

Спосіб перевантаження полягає в тому, щоб довести до противника такої кількості суперечливої інформації, що перевантажує його систему управління.

Спосіб навіювання заснований на формуванні і наступному використанні інформаційного стереотипу поведінки протидійної сторони.

Спосіб тиску заснований на доведенні до суспільної думки противника відомостей, які порочать його і примушують вживати помилкові дії.

Спосіб деблокування інформації передбачає проведення заходів, спрямованих на "витік" закритої інформації з метою її доведення до противника.

Спосіб демпфування полягає у зміщенні акценту наступальних інформаційних дій противника на другорядні цілі та напрямки.

Спосіб ототожнення заснований на зборі і зіставлення інформації про один і той же факт від різних джерел, що дозволяє виявити і блокувати дезінформацію.

Висновки:

На наш погляд, з метою ефективної протидії деструктивному впливу інформаційно-пропагандистської машини противника доцільно запровадити наступні заходи:

1. У зв'язку з реальною перспективою затягування російсько-української війни необхідно створити дієві механізми захисту свідомості військовослужбовця Сил оборони, пересічного громадянина України, соціальних груп від загроз ворожої деструктивної пропаганди, зокрема, створити єдиний орган управління, який відповідатиме за координацію та акумуляцію всіх зусиль протидії інформаційному впливу рф.

2. Україна має вжити жорсткі правові, організаційні, технічні заходи, заходи публічної дипломатії задля організації та забезпечення надійного захисту інформаційних джерел від спотворення рф та її поплічників.

3. Брифінги з приводу подій на фронті мають проводити тільки речники Генерального штабу, командувань військ. Коментарі мають надаватися виключно військовими, які безпосередньо беруть участь у бойових діях.

4. Запровадити у навчальних закладах навчальні спецкурси протидії інформаційної складової російської збройної агресії.

5. Розповсюдити та поширити в засобах масової інформації досвід використання підрозділами Збройних Сил України інформаційних дій (акцій) під час бойових дій, як наприклад, застосування командуванням 2-го батальйону 3-ьої штурмової бригади Збройних Сил України дрону з гучномовцем, через який оточеній групі військовослужбовців рф пропонувалось здатися в полон. Зазначений факт мав місце під час звільнення населеного пункту Андріївка в Донецькій області у вересні 2023 року.

Список використаних джерел:

1. Інформаційна безпека сучасного суспільства : навч. пос. / за заг. ред. А. І. Міночкіна. – К.: ВІТІ НТУУ "КПІ". 2006. – 188 с.

2. Інформаційна боротьба: теоретичні та воєнно-прикладні аспекти: навч. пос. (за ред. Толубка В.Б.). – К.: НАОУ, 2003 – 218 с.

3. Сучасні інформаційні війни в мережевому он-лайн просторі: навч. пос. / О.В. Курбан. – Київ: ВІКНУ, 2016. - 286 с.

4. Сьогодні інформаційна війна – це стрижнева конструкція будь-якої війни - Ганна Маляр – Режим доступу: https://armyinform.com.ua/2023/02/27/sogodni-informaczijna-vijna-cze-stryzhneva-konstrukcziya-bud-yakoyi-vijny-ganna-malyar-2/.

Аміна ВЕСЕЛЬСЬКА
ЖВІ ім. С. П. Корольова
ORCID: 0009-0003-7704-1804
E-mail: aminessa007007@gmail.com

БЕЗПЕКОВІ ПРІОРІТЕТИ ЗОВНІШНЬОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Сучасна військово-політична ситуація навколо України вказує на те, що у воєнній сфері основні виклики та загрози національній безпеці нашої держави з боку Росії є як ніколи актуальними. Частина російських викликів щодо України носять асиметричний характер і поряд із глобальними загрозами тероризму та кіберзлочинності значно переважають над "традиційними" військовими загрозами. Росія намагається переконати світову спільноту в своїй правоті, а тому використовує для цього всі наявні можливості. Як влучно зауважив український дослідник І. Тодоров, сила пропаганди, грошей та інших видів впливу призвела до того, що позиція Росії відстоюється не лише окремими прошарками населення, а й певними політичними силами і політиками. В умовах військової загрози питання обороноздатності України та стану її армії стало потужним чинником у формуванні безпекової стратегії не лише України, але і Європейського континенту.

Відтак, основними напрямами державної політики з питань національної безпеки України в інформаційній сфері є: забезпечення інформаційного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації (далі – ЗМІ) до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України; забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, захист персональних даних, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність ЗМІ та журналістів, заборони цензури, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції, за виконання професійних обов'язків, за критику; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України [1].

Аналіз антиукраїнських дій в інформаційному просторі вказує на те, що слід зробити акцент на збереженні національної ідентичності та популяризації

національної культури як базису не лише інформаційної безпеки України, але й загалом національної. Захист інформаційного суверенітету України виділяється як один із пріоритетних напрямів забезпечення національної безпеки. Проте законодавство не містить адекватного тлумачення зазначеного поняття, як і конкретних механізмів його забезпечення. Так, на сьогодні взагалі відсутній механізм ефективного та швидкого блокування (обмеження доступу) ресурсів з протиправним контентом, зокрема розміщених на технічних майданчиках за кордоном, як і власне визначення шкідливого контенту. Окрім цього, відсутній механізм запобігання та протидії поширенню інформаційної продукції антиукраїнського змісту, шляхом визначення загальних критеріїв її віднесення до заборонених для розповсюдження; 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.

Поряд із поняттям "інформаційний суверенітет" широко вживається "цифровий суверенітет", яке тісно пов'язане з поняттям "кібервійна", що є продовженням війни за допомогою інформаційних і комунікаційних систем, проте із двома фундаментальними відмінностями: вона не призводить до фронтального протистояння ворогуючих сторін та прямих жертв . Зважаючи на низку важливих проблем, що заважають створити ефективно діючу національну систему протидії загрозам в кіберпросторі, а саме: термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних та технічних продуктів іноземного виробництва, складнощі із кадровим наповненням відповідних структурних підрозділів актуальним є питання побудови системи кібернетичної безпеки [2].

Для успішного входження нашої держави в міжнародні інформаційні обміни вона має зосередитись насамперед на таких напрямах у сфері правової діяльності: розробляти систему правових актів, спрямованих на якісне збереження національних інформаційних ресурсів, їх розвиток і ефективне використання в національних інтересах; здійснювати необхідну адаптацію національного інформаційного законодавства до загальновизнаної міжнародної правової бази з метою активізації своєї участі у інформаційних обмінах; брати активну участь у міжнародній правотворчості, що має оперативно регламентувати нові явища в сфері інформатизації; сформувати правову базу для регламентації участі у міжнародній діяльності по забезпеченню дотримання міжнародного інформаційного законодавства, боротьби з кібертероризмом та ін. видами інформаційної злочинності.

Питання національної безпеки у реалізації Україною своєї зовнішньої політики у сучасник умовах російської агресії є надзвичайно вагомим й актуальним. Воно стосується таких сфер державної політики, як захист суверенітету та забезпечення міжнародної підтримки у протистоянні з агресором.

Зовнішня політика України повинна враховувати особливості державної стратегії у сфері безпеки, як у внутрішньому (національно-державний), так і зовнішньому (регіональний і глобальний) вимірах. Подальше врахування безпекових аспектів під час формування і реалізації зовнішньої політики України дозволить розширити кількість потенційних союзників у побудові нової архітектури регіональної та глобальної безпеки, що в перспективі сприятиме підсиленню обороноздатності України.

Список використаних джерел:

1. Про основи національної безпеки України : Закон України від 19.06.03 р. // Відомості Верховної Ради України (ВВР). – 2003. – № 39. – Ст. 351.

2. Горовий В.М. Правові перспективи національного розвитку. – Режим доступу :http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/nablizhajuchi-derzhavu-do-suspilstva/#st hash.AgJjKJa4.dpuf.

3. Тодоров І.Я. 2017. НАТО і війна на сході України (2014-2017 рр.) Збірник наукових праць Стратегії зовнішньої та безпекової політики провідних міжнародних акторів. Київ: Державна уста-нова “Інститут всесвітньої історії НАН України”, с. 102-109.

Валерія ГОРБАТЮК
ЖВІ ім. С. П. Корольова
ORCID: 0009-0002-2279-6452
E-mail: Valeria.illiterate@gmail.com

АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВІД ФЕЙКІВ, ЩО РОЗПОВСЮДЖЕНІ ЧЕРЕЗ МЕРЕЖЕВІ МЕДІА В УМОВАХ ВІЙНИ

Інформація є дієвою зброєю в сучасних конфліктах та війнах. Розповсюдження пропаганди, дезінформації, фейків, маніпуляції в інформаційному просторі – такі методи стали невід’ємною частиною війни. Найбільш яскравим прикладом її еволюції стала Україна. 8 років росія активно веде інформаційну війну проти нашої держави, але слід зауважити, що інформаційні операції проводились ще задовго до початку фази активних бойових дій. Велика мережа російських медіа по всьому світу є доказом й того факту, що наш ворог намагається вести інформаційну війну не лише проти нас, але й проти усього світу.

На сьогоднішній день особливо дієвим є розповсюдження негативного психологічного впливу через соціальні мережі, адже ними користується більшість населення. Соціальні мережі стали місцем для розповсюдження фейків, з метою моделювання певної поведінки цільової аудиторії. В умовах війни протидія

психологічному впливу, зокрема фейкам російської пропаганди є актуальною проблемою. Багато інформаційних каналів в соціальних мережах “ВКонтакте”, “Одноклассники”, “Telegram” тощо, які створені росією активно використовуються спеціальними підрозділами для розповсюдження інформації, що містить негативний психологічний вплив, що в умовах війни спрямований на дестабілізацію ситуації в Україні, підрив довіри до наших Збройних Сил, вищого політичного керівництва, навіювання паніки, страху, знецінення нашої культури, знищення національної ідентичності.

Метою доповіді, є аналіз проблеми розповсюдження фейків в мережевих медіа, загроз, що вони несуть та можливості їх виявлення та захисту від неправдивої інформації що розповсюджена в мережевих медіа. Вже існують дослідження щодо можливості захисту від інформаційного впливу в соціальних мережах, в даній статті розглянуто методи захисту від психологічного впливу розповсюдженого в мережевих медіа, а саме від медіаманіпуляцій. За роки війни частково люди навчилися перевіряти інформацію на достовірність та розпізнавати інформацію, що має деструктивний характер.

Слід розглянути деякі базові ознаки фейків у соціальних мережах. Інформаційні повідомлення, що переповнені емоціями викликають бажання поділитися ними. Такий прийом використовують для вірусного поширення фейкової інформації, тобто наповнюють емоціями, частіше негативними, щоб люди ділились такими повідомленнями і “втягували” широке коло осіб під дію негативного впливу, що міститься в даному меседжі. Ще одна ознака – відсутність або мінімальна кількість даних, за якими можна об’єктивно оцінювати розповсюджувану інформацію, а саме відповіді на питання: Хто? Що? Коли? Як? Чому? Де сталася подія? Такі основні журналістські питання дають можливість перевірити, уточнити, дізнатися, чи насправді ця подія відбувалася. Мають бути вказані конкретне прізвище чи дата, цифри, посилання на джерела, звідки ця інформація взята. Обов’язково треба звертати увагу, на ресурс, першоджерело. Ще одну ознаку складніше перевірити, це – достовірність це перевірка та підтвердження фактів з офіційних джерел. Слід враховувати, що соціальні мережі найчастіше використовуються для розповсюдження чуток та фейків. Факт – це те, що можна перевірити, те, що не змінюється з часом, він об’єктивний і зафіксований. Можливості перевірки фейку немає, скоріше за все він буде лиш існувати в соціальних мережах. Саме тому користувачі соціальних мереж легко попадають під дію негативного психологічного впливу, фейків.

Соціальні мережі створені для розважальних цілей та спілкування а під час війни їх активно використовують для інформаційно-психологічного впливу на певну цільову аудиторію.

Таким чином інформацію потрібно аналізувати і обмежити її розповсюдження в соціальних мережах. В умовах війни та перенасиченості інформаційного простору вміння аналізувати інформацію в мережевих медіа набуває особливої актуальності.

Тому, у подальших дослідженях необхідно звернути особливу увагу на шляхи підвищення медіаграмотності населення.

Список використаних джерел:

1. URL: https://artefact.live/інформаційний-захист-держави-в-умова/ (дата звернення: 18.06.2022).
2. URL: https://www.radiosvoboda.org/a/п-ять-порад-як-захистити-себе-та-близьких-від-фейків-і-медіаманіпуляцій-/30908928.html (дата звернення: 18.06.2022).
3. URL: https://tribun.com.ua/63693 (дата звернення: 18.06.2022).

Вікторія ІВАНОВА
ДНДІ ВС ОВТ
ORCID: 0009-0003-3776-969X
E-mail: viktoria180177@gmail.com

ТРАНСФОРМАЦІЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ З ПОЧАТКОМ ПОВНОМАСШТАБНОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ

У теперішній час сучасні збройні конфлікти поєднують як збройні, так і інформаційні методи ведення війни. Головна мета інформаційної війни – вплив на свідомість і поведінку людей за допомогою маніпулювання інформацією, щоб змусити їх мислити і діяти в інтересах агресора.

Засобом ведення інформаційної війни є інформаційна операція, що представляє комплекс узгоджених та взаємопов'язаних заходів маніпулювання інформацією, що здійснюються за загальним планом з метою досягнення та утримання переваги через вплив на інформаційні процеси в системах противника.

В умовах повномасштабної війни проти України суб’єкти інформаційного протиборства російської федерації активно нарощують свої можливості та створюють нові підходи до інформаційної агресії, поєднуючи спроможності розвідки, дій у кіберпросторі, радіоелектронної боротьби, а також більш традиційних заходів інформаційного впливу (інформаційних і психологічних операцій, дій із введення в оману) для домінування в інформаційному протиборстві на стратегічному, оперативному і тактичному рівнях.

У російській окупаційній армії підрозділи для ведення інформаційної-психологічної війни називаються частинами психологічних операцій (ПсО). Для порівняння, в Збройних силах України використовується абревіатура ІПсО –

інформаційно-психологічні операції, які належать до сфери відповідальності Сил спеціальних операцій.

Історія створення російських частин ПсО починається з часів створення робітничо-селянської червоної армії. Перші спеціалізовані підрозділи ПсО були створені під час Радянсько-Японської війни у 1939 році. Не зважаючи на короткий термін бойових дій – близько п'яти місяців, керівництво угруповання червоної армії, спромоглось залучити до ведення психологічної війни висококваліфікованих спеціалістів: журналістів, поліграфістів, сходознавців, перекладачів. А також вперше було створено окремий відділ для ведення психологічної війни.

Після розпаду СРСР органи спецпропаганди були підпорядковані ГРУ ГШ ЗС рф. Приблизно в 2010-2012 роках, частини ПсО були виведені з воєнної розвідки та переведені до складу Головного оперативного управління ГШ ЗС рф.

Сили психологічних операцій рф складаються з декількох компонентів: сили та засоби ПсО військових формувань; сили та засоби ПсО спецслужб; цивільні державні структури, які залучені до проведення інформаційних операцій; цивільні недержавні структури (підконтрольні уряду); релігійні організації, які залучені до проведення інформаційних операцій.

Після розпаду Радянського Союзу з метою формування сепаратистських настроїв для забезпечення виконання імперських планів нового керівництва, російська федерація не припиняла використовувати інформаційно-психологічний вплив на людей, які проживали в прикордонних регіонах України. У переважно російськомовних областях розповсюджувалась тематична друкована продукція, книги, плакати, засоби пропаганди із закликами до створення квазіреспублік на території України. За допомогою інформаційно-психологічних впливів здійснювався селективний відбір найбільш вразливої аудиторії для формування категорії людей, з якими в подальшому планувалось проводити більш активні дії щодо створення потрібного психотипу.

У 2008 році під час другої Російсько-Грузинської війни, незважаючи на серйозні проблеми російської армії, частини ПсО проявили себе досить результативно, врахувавши цей досвід, рф застосувала його під час операції по анексії Криму, а потім Донбасу. До прикладу події в цих регіонах журналісти висвітлювали, подаючи точку зору нібито місцевих жителів, насправді ж це були спеціально привезені росіяни – як частина інформаційної операції.

З 2014 року в інтересах загонів психологічних операцій рф починається використання комплексів радіоелектронної боротьби для розсилки смс військовим та цивільним, посилюється використання тролів та ботів у соціальних мережах, що було спрямовано, насамперед, на деморалізацію та

дезорганізацію фронту та тилу, формування атмосфери безнадійності та приреченості.

З початком повномасштабної російсько-української війни інформаційно-психологічна діяльність рф була націлена на дискредитацію військового та політичного керівництва держави, зміщення інформаційного фокусу на поразки та невдачі, розповсюдження наративів про зраду з боку союзників та інше. Це було покликано створити у громадян та в лавах ЗС України відчуття безперспективності спротиву, зниження бойового духу та заохочення до капітуляції. В той час багатьом українцям через стрес та величезний потік інформації було важко розрізнити фейк від правди.

У першій половині 2023 року на російських телеграм-каналах і в соцмережах активізувались інформаційно-психологічні операції з питань потенційного контрнаступу українських військ, для цього росіяни використовували старі відео та фото, які демонстрували підбиту техніку, загиблих та полонених, поширюючи недостовірну інформацію про бойові дії.

Таким чином, історично прослідковується трансформація інформаційної політики рф по відношенню до України. До 2010 року спостерігається нав'язування певних наративів про братні народи зі спільною історією та культурою, де Україна не може бути частиною Європи, бо вона є частиною "руського миру". З 2014 року, аргументуючи анексію Криму, путін пояснював, що Крим – це російські землі подаровані Україні Леніним. З 2014 року з'являються фейки про розп'ятого хлопчика в Слов'янську та обґрунтування початку воєнних дій на Донбасі захистом російськомовного населення. У 2022-2023 році з'являються наративи про нацистів, що будуть брати в рабство російськомовних громадян та інше.

Але з часом росія стає менш модернізованою у поширенні своєї дезінформації, в соціальних мережах налагоджено механізм протидії російським ботам і тролям, українські телеканали створюють контенти у вигляді коротких, змістовних відео, де докладно розкриваються фейки російських інформаційно-психологічних операцій.

Воєнною розвідкою України публікуються факти та окремі розвідувальні дані, які розкривають наміри агресора, оприлюднюють докази вчинення росією воєнних злочинів.

Українці споживають інформацію більш виважено, критично ставлячись до маніпулятивної та викривленої інформації, будуючи навколо себе той інформаційний простір, який допоможе нам перемогти.

Всі перелічені заходи доводять свою ефективність, оскільки російська пропаганда не може досягти своїх головних цілей, через що росія програє в інформаційній війні.

Юрій КОВНИЙ, к.е.н., доц.
ЛНУ ім. Івана Франка
E-mail: Kovnyte34@ukr.net
ORCID: 0000-0002-1230-5050

СПЕЦІАЛЬНИЙ УПОВНОВАЖЕНИЙ ЩОДО ЕТНОНАЦІОНАЛЬНОЇ ПОЛІТИКИ: БЕЗПЕКОВІ ПИТАННЯ

Спеціальний уповноважений – це посадова особа або представник, якому надані особливі повноваження або відповідальність для вирішення певних завдань або питань у межах своїх компетенцій. “Омбудсмен – це інституція, створена для боротьби зі зловживанням владою державними службовцями та для допомоги чиновникам у здійсненні уряду ефективно та чесно, а також для заохочення посадових осіб виконувати свої обов’язки та надавати якісні послуги” [1, с.124]. Спеціальний уповноважений з прав людини має за мету захист та сприяння правам і свободам людини в певній сфері.

Вчені української правової доктрини акцентують увагу на необхідності розробки цілісної етнонаціональної правової політики на різних комунікативних платформах, оскільки проблема належної комунікації суб’єктів етнонаціональних відносин пріоритетно має безпекове значення. Відсутність дієвої правової політики вказує на наявність значних труднощів у визначених пріоритетних напрямках правової політики держави. Комплексний акт щодо етнонаціонального правового регулювання повинен включати в себе мету, методи, засоби та принципи майбутнього розвитку держави та правової системи. Хоча певні аспекти правової політики можна закріпити в окремих законодавчих актах, це, безумовно, недостатньо для відповіді на виклики сучасної соціально-правової реальності.

Окрім визначення прав суб’єктів такої правової політики вагомо забезпечити комплекс гарантій. Судові гарантії, безумовно є одними з найбільш ефективних, проте позасудові організаційно-медіаційні процедури забезпечують швидше і компромісне вирішення ситуації.

Створення посади спеціального уповноваженого у сфері етнонаціональної політики є досить вагомим аспектом удосконалення правового гарантування у визначеній сфері. Тому визначимо роль спеціального уповноваженого у сфері етнонаціональної політики, і перманентно захначимо що загалом вона полягає у захисті та підтримці прав і інтересів корінних народів, національних меншин, інших суб’єктів у різних сферах суспільно-політичної та правової діяльності. Основні аспекти функціонування цієї інституції, на нашу думку мають передбачати:

захист прав представників суб’єктів етнонаціональної політики, тому спеціальний завдання виявлення та реагування на можливість порушення прав

народу/народностей, етнічних груп, корінних народів, національних меншин тощо. Це може бути пов'язано з правами на землю, водними ресурсами, культурною спадщиною, освітою, здоров'ям та іншими аспектами життя;

захист культурної спадщини суб’єктів етнонаціональних відносин, зокрема до повноважень досліджуваної інституції слід включити можливість прийняття рішень у збереженні та відновленні культурних та традиційних цінностей етнонаціональних груп суспільства, що загалом включає підтримку у збереженні мов, релігій, ремесел та інших аспектів культури;

інститут спеціального уповноваженого покликаний сприяти консультаціям та партнерству, оскільки він може може об'єднувати представників національних меншин, корінних народів, громадські еліти, владу та інші стейкхолдерів для вирішення питань, що стосуються прав окремих етнонаціональних груп та їх взаємодії загалом, особливо це вагомо для вирішення безпекового питання, оскільки вказане може забезпечити проблеми консенсусу та вирішення конфліктів;

роль спеціального уповноваженого полягає також в тому, що він в межах своїх повноважень вирішує проблеми досягнення цілей сталого розвитку, особливо щодо просвітництва та освіти, тому що ця інституція може виступати як освітній ресурс, надаючи інформацію про культуру, історію та потреби етносів та народів. Це сприяє усвідомленню суспільством важливості захисту їх прав.

Правова політики не є сталим поняттям, вона потребує поступального розвитку та удосконалення, саме спеціальний уповноважений, що має можливість моніторингу та аналізу становище етнонаціональних груп й розроблення політики удосконалення захисту та гарантування їх прав, свобод та законних інтересів.

Отож, уповноважений у справах етнонаціональної політики виступає як посередник між урядом та представниками національних меншин, корінними народами та іншими суб’єктами етнонаціональних відносин, сприяючи діалогу та вирішенню проблеми. Досліджуваний інститут також відіграє важливу роль у попередніх конфліктах та сприянні побудові взаєморозуміння та толерантності між більшими групами суспільства.

Список використаних джерел:

1. Kafrawi R. M., Umam K., Fallahiyan A. Implementation of the Authority of the Indonesian Ombudsman Representative of the Province of Nusa West Southeast in Oversight of Public Services in the Village *Jatiswara*. *2023.* №.38 (2). P.124-133.

Сергій МАРЧЕНКОВ, к.пед.н.
ORCID: 0000-0003-4597-3618
E-mail: marchenkov1978@ukr.net
Сергій ШИШКІН
ЖВІ ім. С.П. Корольова
ORCID: 0009-0001-0354-9504
E-mail: ihruk44@gmail.com

ПРОБЛЕМИ ПРОВЕДЕННЯ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ ТА ПІДВИЩЕННЯ ЇХ ЕФЕКТИВНОСТІ

З початком повномасштабного вторгнення російської федерації проблематика досягнення ефективності при здійсненні психологічного впливу підрозділами психологічних операцій ЗС України стала особливо актуальною [1]. Причиною часткових труднощів у цьому є цензура та закритість інформаційного простору рф, узурпація довіри населення пропагандистськими ресурсами, підконтрольними державній владі та бізнес-еліті.

Агресія країни-терориста проти України триває з 2014 року але введення наративів проти всього українського в російських ЗМІ триває починаючи з 1991 року, адже інформаційно-психологічні операції проти України були зафіксовані ще в ті часи [2]. Вони були присутні у більшості ЗМІ, та навіть у розважальному контенті. Такий тривалий та активний психологічний вплив на населення сформував у цільової аудиторії хибне сприйняття реальності та неправильні цінності щодо оцінки ситуації, яка відбувається у наш час. Крім того, політика масової цензури через системний моніторинг спецслужбами інформаційних джерел, блокування ресурсів та видалення будь-якої провокуючої інформації закликає до мітингів, дискредитує провладні структури рф, розповідає історичну правду, викриває страшенну бідність звичайного населення та корупцію верхівки, тощо.

Отже, зважаючи на складну ситуацію, в інформаційній сфері можливість ґрунтовно здійснювати психологічний вплив на російські маси залежить від виконання запропонованих етапів, а саме:

правильний аналіз та підбір ЦА для проведення заходів психологічного впливу;

комплексний підхід до планування та проведення ПсО зі здійсненням довготривалого психологічного впливу з використанням методу “40 на 60” [3];

ґрунтовний аналіз вразливостей ЦА для досягнень поставлених цілей ПсО;

застосування усіх доступних цільовій аудиторії інформаційних платформ для проведення заходів психологічного впливу.

Слід зазначити, що важливо активізувати створення та розвиток власних каналів доставки матеріалів психологічного впливу до цільової аудиторії, з окремим перманентним фінансуванням, які будуть повністю відповідати в інформаційному плані запитам середньостатистичних представників цільової аудиторії та ні чим не

будуть відрізнятися від “рупорів” пропаганди рф на початку їх існування. Основними наративами таких ресурсів повинні бути актуальні теми, що відповідають порядку денному цільової аудиторії без використання провокаційних закликів та висловлювань.

Такі дії дозволять через певний час досягти необхідної аудиторії, що дасть можливість втілювати метод “40 на 60”, який буде непомітним для звичайних мас, які вважають ці ресурси авторитетними та перевіреними.

Отже, на даний момент в інформаційному просторі стоїть задача, досягнення якої прискорить перемогу Сил оборони України на полі бою, а саме: отримання переваги у ворожому інформаційному просторі, що збільшить ефективність психологічних операцій, а виконання цього завдання вимагає від підрозділів ПсО розумної ініціативи, злагодженої роботи та відточення механізмів доставки матеріалів ПсВ.

Список використаних джерел:

1. Твердохліб Ю. М. Інформаційно-психологічні операції у російсько-українській гібридній війні : дисертація. Чернівці, 2019. 168 с.

2. Сьогодні Україна не програє інформаційну війну Росії, а успішно протистоїть усім інформзагрозам : АрміяInform. 2021. URL: https://armyinform.com.ua/2021/11/02/sogodni-ukrayina-ne-prograye-informaczijnu-vijnu-rosiyi-a-uspishno-protystoyit-usim-informzagrozam/ (дата звернення 24.09.2023).

3. Метод “гнилой селедки” : детектор медіа. 2015. URL: https://detector.media/withoutsection/article/110011/2015-08-11-metod-gnyloy-seledky/ (дата звернення 24.09.2023).

Олег МЕДВЕДЄВ
НУОУ
ORCID: 0009-0007-2513-2092
Email: oleh.medvedev@gmail.com
Ігор СІВОХА
НУОУ
ORCID: 0000-0001-5377-2520

ЗРИВ МОБІЛІЗАЦІЇ З МЕТОЮ ПІДРИВУ ОБОРОНОЗДАТНОСТІ ЧЕРЕЗ РОСІЙСЬКІ ТА ПСЕВДОУКРАЇНСЬКІ ТЕЛЕГРАМ КАНАЛИ

“Тенденція використання соціальних мереж для здійснення інформаційного (психологічного) впливу на визначені цільові аудиторії на сьогодні стала реальністю, а застосування соціальних мереж стало повсякденним процесом дестабілізації

суспільно-політичної обстановки в країні-мішені" [1].
У 2022-2023 роках істотно прискорився процес змін в ієрархії каналів комунікації: відбулися подальше зниження частки телебачення як джерела новин, зростання ролі інтернету, соціальних мереж, особливо месенджерів, насамперед Telegram. Київський міжнародний інститут соціології (КМІС) констатує, що телебачення остаточно поступилося інтернету першістю як джерело отримання інформації: "Замість кількох потужних телевізійних каналів "виросли" сотні онлайн-джерел, кожне з яких не може похвалитися великою часткою "ринку" [2].

Якщо аналізувати сумарний час споживання новин у соціальних мережах, за даними КМІС, то 41% припадає на Telegram, 37% – на YouTube, у той час як Facebook – 12%. На сьогодні Telegram став ключовою платформою для поширення російської пропаганди каналами, які формально позиціонують себе як українські, орієнтуються на українську аудиторію і подають українські новини в російській інтерпретації. У липні 2022 року СБУ, Міністерство оборони та інші українські відомства опублікували зведений список таких Telegram-каналів, підконтрольних Кремлю. "В умовах, – зазначають спецслужби, – коли Україна успішно протистоїть російському нападу, вкрай актуальним є питання інформаційної безпеки. Адже не маючи можливості перемогти на полі бою, ворог намагається посіяти "зраду" та розхитати українське суспільство".

При контент-аналізі ворожих каналів чітко проглядаються ключові наративи, месиджі і теми, розраховані на підрив обороноздатності України, дискредитацію Збройних Сил України, зниження бойового духу. Особливості інформаційно-психологічного впливу на масову свідомість військовослужбовців добре відомі і досліджені. Серед них – "ініціювання сумнівів серед особового складу в доцільності ведення бойових дій; дезінформація військовослужбовців щодо реального стану справ на полі бою; створення паніки, масових психозів, настроїв поразки серед військовослужбовців; нагнітання страху бути вбитим або отримати тяжкі каліцтва" [3].

Однією з центральних тем російських телеграм-каналів стала мобілізація в Україні. Кампанія, очевидно, орієнтована як на цивільну аудиторію, так і на середовище військових. Ворог прагне генерувати недовіру українців до влади та знизити мотивацію долучення до армії. На загал – створити реальні проблеми для поповнення ЗСУ і таким чином - знизити обороноздатність країни.

Російські пропагандисти відверто декларують у своїх каналах мету кампанії із дискредитації мобілізації: контрнаступ ЗСУ залежить від того, наскільки швидко йде поповнення. Зокрема, @legitimniy та @rezident_ua писали про те, що "Украине необходимо собрать десятки тысяч новых солдат и сформировать резервы в более чем 200 тысяч солдат".

Російські канали нагнітають загальну паніку про нібито насильницьку мобілізацію до лав ЗСУ. Наприклад, @Ze_Kartel опублікував цілу добірку епізодів, як військкомати вручають повістки у громадських місцях: від кафе до церков і

бомбосховищ; “на похороні у Львові та недільній службі у церкві”; на гірськолижних курортах Карпат. Ці повідомлення - коктейль фейків, маніпуляцій і достовірної інформації, яка на задум розповсюджувачів має викликати довіру до усієї цієї пропагандистської суміші.

Ворог також наголошує на недотриманні принципу соціальної справедливості при мобілізації. Так, підозрюваний у державній зраді Шарій протиставляв простим чоловікам дітей та родичів можновладців, які виїхали за кордон. Канал @legitimniy звинувачував працівників військкоматів у корупції та ухилянні від фронту: “Большинство этих ребят, которые раздают вам повестки, купили эти безопасные места, чтобы самим не ехать в бахмутовскую мясорубку или другие “проклятые места”. Інші канали так само розігрували карту соціальної нерівності, поширюючи фейкове відео на кшталт “военкомы на шикарной машине угрожают охраннику жилого комплекса отправкой в армию за то, что он не открыл им шлагбаум”.

Особливу увагу противник приділяє розпалюванню міжетнічної, міжрегіональної та мовної ворожнечі, протиставляли схід і захід України: мовляв, повістки роздають “особенно активно в восточной части страны, население русскоязычных (“пророссийских”) регионов давно считают второсортным”. Жителів сходу і півдня України у трактуванні російської пропаганди відправляють у найгарячіші точки, аби позбутися “проросійських російськомовних українців”. Розігрувалася й угорська карта. Канал @ZeRada1 розповідав про нібито масове вручення повісток у містах Берегове, Виноградів та селі Сюрте, де живе значна угорська діаспора і цитував угорську журналістку: “Если так будет продолжаться, на Закарпатье не останется ни одного венгра”.

Залякували тим, що мобілізованих направляють на фронт без підготовки “На Украине разразился скандал … свежемобилизованный гражданин из 57-й опбр уже через 2 дня после “добровольной мобилизации” оказался на фронте”. @opersvodki публікував фото чоловіка без рук з погано перекладеним з російської підписом (“тварі вручили повестки”): “…на фронт попытались призвать украинца без рук. На очереди слепые и безногие”.

Росіяни не обмежуються лише розповсюдженням дезінформації. Вони закликають українців до непокори та акцій протесту, рекламують українські онлайн сервіси, які інформують про місця видачі повісток чи юридичні послуги з уникнення мобілізації. Весною 2023 року кіберфахівці Служби безпеки України заблокували 26 Телеграм-каналів, які перешкоджали мобілізації українських громадян призовного віку. Насамперед вони, повідомляє УНІАН, надавали дані про актуальні місця вручення військовозобов’язаним повісток та закликали ховатися від представників військкоматів.

Такі захисні дії цілком виправдані, але протидія кампанії потребує зусиль із медіа-освіти українців, поширення правил елементарної медіа-гігієни. Одним із інструментів протидії є фахове використання прийомів і методів стратегічної комунікації: публічної дипломатії, зв’язків з громадськістю, військових зв’язків,

інформаційних та психологічних операцій. Потрібні і новітні технологічні рішення. Так, фахівці Інституту стратегічних комунікацій Національного університету оборони України запропонували метод прогнозування поширення інформаційних загроз у соціальних мережах, що містить у собі математичні моделі та методику їх застосування та розроблення програмних комплексів щодо обмеження доступності деструктивної інформації" [4].

Список використаних джерел:

1. Сідченко С., Залкін С., Хударковський К., Ревін О. Особливості підготовки і проведення інформаційної (психологічної) операції у соціальних мережах. Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи : тези доп. ІІІ Міжн. наук.-практ. конф. (м. Київ, 31 жовтня 2022р.). Київ : ННЦСК СЗНБО НУОУ, 2022. С. 48-51.
2. Київський міжнародний інститут соціології. Демократія, права і свободи громадян в умовах війни // 17.08.22 – Режим доступу ttps://www.kiis.com.ua/materials/pr/20220817.
3. Саунін Р. "Особливості інформаційно-психологічного впливу на масову свідомість військовослужбовців". Стратегічні пріоритети інформаційної безпеки держави у сфері оборони в умовах воєнного стану: тези доп. ІІ міжв. наук.-практ. конф. (м. Київ, 29 листопада 2022р.) Київ. КЗІТтаІБ НУОУ, 2022, с. 121-124.
4. Войтко В., Солонніков В., Рахімов В. "Прогнозування розповсюдження деструктивного інформаційного впливу в соціальних мережах". Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи : тези доп. ІІІ Міжн. наук.-практ. конф. (м. Київ, 31 жовтня 2022р.). Київ : ННЦСК СЗНБО НУОУ, 2022. – 205 с.

Надія МІРОШНИК
Слухач навчальної групи 8204
Інститут стратегічних комунікацій
НУОУ
ORCID: 0009-0001-1238-7359
E-mail: nadij@i.ua

ОСОБЛИВОСТІ РОЗВИТКУ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ ОПЕРАЦІЇ ЗБРОЙНИХ СИЛ УКРАЇНИ

Щоб вирішити проблему організації використання інформаційного простору в інтересах Збройних Сил на початку 2000 років було розроблено теорію інформаційно-психологічної операції (протиборства) [1].

У 2007 році теоретичні основи такої діяльності були включені до Засад підготовки і застосування Збройних Сил України. На цьому процес інтеграції інформаційно-психологічної операції (далі – ІПсО) у практику застосування Збройних Сил практично зупинився через організаційно-адміністративні ускладнення, адже ця діяльність належала до сфери повноважень Головного управління розвідки Міністерства оборони України. Надалі не було видано жодного керівного документа з питань ІПсО, а військові частини ІПсО використовували для збирання інформації з відкритих джерел в інтересах розвідувально-інформаційної діяльності.

У ході опрацювання питань підготовки та застосування Збройних Сил України Головне оперативне управління Генерального штабу дійшло до висновку, що теорія ІПсО не відповідає вимогам сьогодення через обмеженість її мети і виконуваних завдань. Це змусило керівництво Збройних Сил України деталізувати мету інформаційно-психологічної операції, зокрема нею стало змушення противника до прийняття та реалізації неефективних (недоцільних) рішень, ускладнення функціонування (виведення з ладу) елементів системи управління військами.

Після початку 2014 року ІПсО була розділена на інформаційну та психологічну операції Збройних Сил України, мета останньої є створення необхідних змін у діяльності (поведінці) цільової аудиторії противника та умовах інформаційного простору, які сприятимуть досягненню цілей застосування ЗС або операцій угруповань військ (сил).

Завданнями інформаційної та психологічної операції є [2]:

інформаційний вплив – вплив на комп'ютерні мережі противника шляхом введення у них спеціальних програм; радіоелектронне подавлення засобів РЕБ противника та здійснення радіоелектронного захисту; захист інформації в комп'ютерних мережах;

психологічний вплив – підтримка діяльності місцевих органів виконавчої влади, створення позитивного враження населення про дії своїх військ; запобігання наслідкам психологічного впливу противника та його нейтралізація, поширення серед особового складу противника негативної та суперечливої інформації; пропаганда високої боєздатності ЗС України.

Завдання інформаційної операції визначаються на підставі [3]:

мети і завдань застосування ЗС України (операцій угруповань військ (сил);

форм і способів ведення операцій (бойових дій);

складу військ (сил).

Стало зрозуміло, що необхідно виконувати ширший перелік заходів і залучати різнорідні сили і засоби для комплексного впливу на свідомість противника, його інформаційно-технічні системи, інформаційні процеси та саму інформацію [4].

У зв'язку з цим було ініційовано створення нового напряму в теорії та практиці застосування Збройних Сил України – інформаційної операції, а для керування такою діяльністю у вересні 2013 року в Головному оперативному управлінні

створено відділ інформаційної боротьби. У грудні 2014 року відділ розробив Концепцію інформаційної операції Збройних Сил України. Надалі було видано тимчасові настанови з психологічної (грудень 2016 року) та інформаційної операцій (березень 2017 року) Збройних Сил України. Інформаційну операцію було включено в Систему застосування Збройних Сил, що визначалося Основами ведення операцій військ (сил) Збройних Сил України.

Таким чином, із середини 90-х років XX ст окреслилася нова сфера збройної боротьби – інформаційний простір і виникла потреба ведення дій у цьому просторі. Значення таких дій – інформаційних операцій та їх частка у загальному масштабі збройної боротьби в сучасних умовах постійно збільшується. Інформаційні операції передують застосуванню бойових частин, супроводжують військові операції і тривають ще довго після завершення активного збройного протистояння.

Список використаних джерел

1. AJP-3.10 Allied Joint Doctrine for Information Operations, Edition A, Version 1, доктрина НАТО. December 2015.

2. Commander's Handbook for Strategic Communication and Communication Strategy, Version 3.0, US Joint Forces Command Joint Warfighting Center, посібник ЗС США зі стратегічних комунікацій. 24 June 2010.

3. Joint Information Operations Planning Handbook, посібник ЗС США з планування інформаційних операцій. July 2019, Joint Command, Control and Information Warfare School, Joint Forces Staff College.

4. Allied Command Operations' (ACO) Comprehensive Operations Planning Directive (COPD), Interim 2.0, директива Командування НАТО з операцій щодо порядку оперативного планування. 04 October 2020.

Юрій МІХЄЄВ, к.т.н., ст.дос.
ЖВІ імені С. П. Корольова
ORCID: 0000-0002-6239-2324
E-mail: yuramiheev@ukr.net

СПОСІБ ДОСЛІДЖЕННЯ ВЗАЄМОЗВ'ЯЗКІВ МІЖ ОБ'ЄКТАМИ ПІД ЧАС ПЛАНУВАННЯ ПСИХОЛОГІЧНОЇ ОПЕРАЦІЇ

Вилучення сенсу із зібраних даних під час інформаційно-аналітичної роботи потребує належної організації отриманої інформації. Одним із способів організації інформації є її візуалізація [1–3]. Такий підхід дозволяє досліджувати взаємозв'язки між об'єктами під час планування психологічної операції (акції) (особами з числа цільової аудиторії). Аналіз взаємозв'язків передбачає пошук

найстійкіших взаємозв'язків між об'єктами, тимчасових, випадкових, закономірних їхніх проявів.

Для дослідження взаємозв'язків може використовуватися релятивна (асоціативна) діаграма [3]. Така діаграма взаємозв'язків дозволяє визначати організаційну структуру групи осіб з числа цільової аудиторії, рівень належності її до організацій, оточення окремої особи, її контактів. Завдяки діаграмам взаємозв'язків може встановлюватися дійсне і формальне лідерство особи. У подальшому такі відомості використовуються для формування механізмів впливу на задану ЦА. Побудова діаграми взаємозв'язків між об'єктами передбачає такі етапи:

I етап. Відбір об'єктів, що підлягають аналізу та внесення їх у матрицю взаємозв'язків;

II етап. Розроблення матриці (матриць) взаємозв'язків між об'єктами;

III етап. Підрахунок кількості взаємозв'язків для кожного об'єкта;

IV етап. Побудова діаграми взаємозв'язків та карти інформаційного поля.

Для запису назв усіх типів об'єктів використовуються діагональні матриці з використанням системи символів для позначення взаємозв'язків між об'єктами. Після того, коли матрицю розроблено, здійснюється підрахунок кількості взаємозв'язків за типом для кожного об'єкта.

На наступному етапі розробляється початкова діаграма взаємозв'язків між об'єктами. Особи, які мають найбільшу кількість взаємозв'язків, становлять певний центр впливу. Наявні взаємозв'язки виокремлюються за типами та подаються у вигляді діаграм. Також на діаграмі можуть позначатися типи взаємозв'язків між об'єктами. Далі на основі побудованої діаграми може бути розроблено карту інформаційного поля, яка передбачає відображення взаємозв'язків між особами з числа цільової аудиторії, що досліджується (рис. 1).

На основі візуального подання типу стосунків між об'єктами може встановлюватися напрям впливу між окремими об'єктами або різними групами об'єктів.

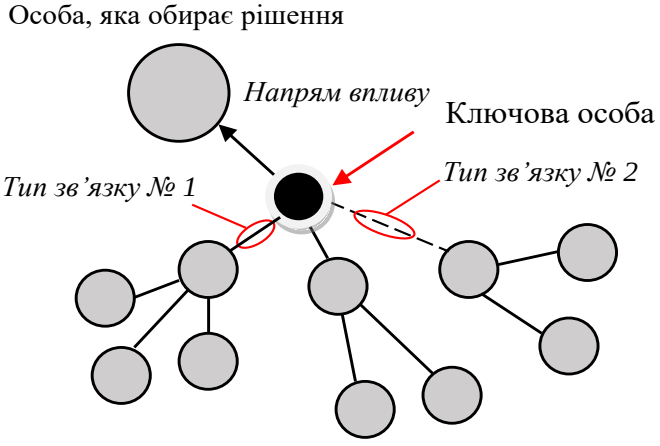


Рисунок 1 – Спосіб подання карти інформаційного поля

Такий підхід до відображення інформації про об’єкти під час планування психологічної операції (акції) на етапі аналізу району операційного середовища та цільової аудиторії дозволить у зручний спосіб здійснити пошуку точок уразливостей у системі стосунків агентів впливу, ключових лідерів (лідерів думки).

Список використаних джерел:

1. The Open Graph Viz Platform [Електронний ресурс]. – Режим доступу: https://gephi.org/ (дата звернення: 01.08.2023).
2. Powerful and intuitive graph visualization software built for teams [Електронний ресурс]. – Режим доступу: https://linkurious.com/linkurious-enterprise-explorer/ (дата звернення: 01.08.2023).
3. Федчак І. А. Основи кримінального аналізу: навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

Вікторія НАМЕСТНІК, к.н.держ.упр.
НУОУ
ORCID: 0000-0002-9385-7905
E-mail: namestnikviktoria@gmail.com

СОЦІАЛЬНІ МЕРЕЖІ ЯК СЕРЕДОВИЩЕ ПРОВЕДЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ ПРОТИВНИКА

У Стратегії інформаційної безпеки [3], прийнятій у 2021 році, соціальні мережі згадуються в контексті глобальних загроз та викликів як суб’єкти впливу в інформаційному просторі. В умовах відбиття широкомасштабної збройної агресії Росії проти України соціальні мережі та месенджери стали одним із найпоширеніших джерел інформації в Україні. За даними опитувань, 85% українців щоденно використовують інтернет, 74% опитаних вказали соціальні мережі як основне джерело отримання новин, а 60% – довіряють новинам у соціальних мережах. За результатами цього ж опитування, у 2022 році значно зросла популярність використання Telegram. Він став основною соціальною мережею як для комунікації, так і для споживання новин [2]. Також чільне місце посідає Facebook (Meta) - на початку 2022 року кількість користувачів цієї соцмережі перевищувала 2,91 мільярда [0]. Разом з тим, недостатній рівень медіаграмотності (медіакультури) українців визначений однією з глобальних загроз в інформаційному просторі [3]. Саме тому масове залучення авдиторії та

висока швидкість поширення інформації роблять соцмережі та месенджери ефективним середовищем проведення інформаційних та психологічних операцій.

Варто зауважити, що така тенденція притаманна не лише вітчизняному, а й зарубіжному інформаційному простору. Найбільш агресивний інформаційно-психологічний вплив Росія намагається чинити щодо західних держав-партнерів України. Особливістю інформаційно-психологічних операцій в українському інфопросторі є те, що вони спрямовані на підсилення паніки й страху в українському соціумі, підрив довіри до влади та Сил оборони України, розділення українців на основі політичних чи релігійних уподобань, мовного питання тощо. Натомість, ключовою метою інформаційно-психологічних операцій у зарубіжному інфопросторі є зниження рівня підтримки України та виправдання воєнних злочинів російської армії. Така інформаційна спрямованість сприяє досягненню геополітичних цілей противника.

Наприкінці 2022 року дослідники українського сегмента Telegram виокремили понад 300 каналів, що просували російську повістку в український інфопростір [0], проте ця цифра не є остаточною через динамічність роботи месенджера (телеграм-канали можуть вільно змінювати власника чи риторику контенту). Більшість цих телеграм-каналів є анонімними, проте частина з них чітко асоціюються з проросійськими особистостями (політиками, журналістами, блогерами, тощо). Часто канали намагаються мімікрувати під проукраїнські й приховано поширюють меседжі, співзвучні з наративами російської пропаганди.

В умовах воєнного стану українці почали частіше звертатись до офіційних джерел інформації, зокрема до верифікованих сторінок представників влади чи відомств у соціальних мережах. Тому противник створює фейкові акаунти, що за стилем оформлення схожі на офіційні. Такі акаунти також стають джерелом дезінформації, або ж метою їх діяльності є підрив довіри до влади – через множину псевдоофіційних акаунтів користувачі втрачають довіру до офіційних повідомлень.

Також інформаційно-психологічні операції противника спрямовані на дискредитацію вищого керівництва Міністерства оборони України, Збройних Сил України, розвідувальних органів тощо. Поширюючи фейкові повідомлення про загибель чи поранення керівників, противник намагається чинити когнітивний вплив одночасно на кілька цільових аудиторій – родини вищого керівництва, військовослужбовців ЗС України та українське суспільство загалом. Метою таких повідомлень є поширення страху, паніки, зневіри тощо.

Ще одним напрямом інформаційно-психологічних операцій, які противник проводить у соціальних мережах чи месенджерах – збір розвідданих з відкритих джерел (OSINT-технології – Open Source Intelligence). У чатах чи на сторінках спільнот за допомогою різноманітних технік маніпулювання українців спонукають до поширення інформації про переміщення техніки ЗС України, даних про військовослужбовців (зокрема за допомогою сторінок, присвячених пошуку

зниклих безвісти чи полонених), інформацію про розміщення української системи протиповітряної оборони та ін.

З 2014 року волонтерська підтримка Сил оборони України є доволі суттєвою, тож частина інформаційно-психологічних операцій противника спрямована саме на дискредитацію волонтерського руху, нова хвиля активізації якого відбулася після повномасштабного вторгнення Росії на територію України у 2022 році. Через велику кількість різноманітних волонтерських зборів стало можливим шахрайство з метою привласнення коштів чи викрадення персональних даних довірливих користувачів соціальних мереж. Використовуючи реальні факти шахрайства противник проводить інформаційно-психологічні операції, метою яких є зниження довіри до волонтерських організацій та зменшення підтримки ЗС України.

Одним із ключових способів протидії деструктивному інформаційно-психологічному впливу соціальних мереж може слугувати підвищення рівня цифрової та медіаграмотності населення. У Стратегії інформаційної безпеки [3] для вирішення цієї проблеми передбачено проведення просвітницьких кампаній з медіаграмотності, що сприятимуть розвитку критичного мислення, фактчекінгу (перевірки фактів) тощо. Разом з тим, має бути налагоджена чітка, динамічна і ефективна система комунікації з громадськістю для спростування дезінформаційних вкидів або ж запобіганню інформаційно-психологічних операцій противника.

Список використаних джерел

“Кремлівська гідра”: 300 телеграм-каналів, які отруюють український інфопростір URL: https://detector.media/monitorynh-internetu/article/205954/2022-12-14-kremlivska-gidra-300-telegrm-kanaliv-yaki-otruyuyut-ukrainskyy-infoprostir/ (дата звернення: 25.09.2023)

Найпопулярніші соціальні платформи за кількістю активних користувачів за місяць URL: https://uaspectr.com/2021/12/12/najpopulyarnishi-sotsialni-merezhi-u-sviti-2022/ (дата звернення: 25.09.2023)

Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року ”Про Стратегію інформаційної безпеки”. Указ президента України № 685/2021 від 28 грудня 2021 року URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 25.09.2023)

Рівень цифрової грамотності українців: про що свідчить дослідження Мінцифри URL: http://nrcu.gov.ua/news.html?newsID=97355 (дата звернення: 25.09.2023)

Юрій ОПАНЮК
ЖВІ ім. С.П. Корольова
ORCID: 0009-0007-0379-4669
E-mail: opan.fr@gmail.com

ТЕХНІЧНЕ ОБҐРУНТУВАННЯ ВИМОГ ДО МОБІЛЬНОЇ ЗВУКОМОВНОЇ СТАНЦІЇ ПІДРОЗДІЛІВ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ ЗС УКРАЇНИ

В умовах відбиття Силами оборони України збройної агресії російської федерації збільшилася роль психологічних операцій у цій війні, а саме технічних засобів, що застосовуються як і підрозділами психологічних операцій Збройних Сил України так і ворогом. Так, з моменту початку широкомасштабного вторгнення, як і Сили оборони України, так і збройних сил рф на території України застосовують різні засоби звукомовлення [1]. Це пов’язано з такими їх перевагами порівняно з іншими засобами поширення матеріалів психологічного впливу (ПсВ) (телерадіомовлення, друковані засоби та інші), як оперативність доставки матеріалів, охоплення чітко визначеної за територіальною ознакою цільової аудиторії (ЦА), відсутність необхідності застосовувати будь-які технічні засоби для сприйняття інформації [2]. Тому, ЗС є важливим засобом інформаційного протиборства саме на тактичному рівні. Отже з метою подальшого ефективного виконання завдань підрозділами ПсО ЗС України необхідне удосконалення експлуатаційних, ергономічних та тактичних характеристик зразків озброєння та військової техніки (ОВТ) цих підрозділів.

Важливу роль при плануванні серій впливу належить питанням вивчення доступності ЦА, а саме побудові моделі поширення акустичних сигналів в складних перешкодових середовищах. Такий підхід дає можливість чітко визначити охоплення ЦА саме при застосуванні ЗС, що у подальшому може бути використано при оцінюванні ефективності спланованої серії впливу.

До теперішнього часу зазначене вище завдання вирішувалося в основному експертним шляхом, особливо у частині, що стосується аналізу доступності ЦА [3]. Як правило, при цьому оцінювання ефективності ПсВ мало неформалізований характер з високим ступенем суб’єктивізму. На сучасному етапі першочергово потребує вирішення завдання щодо, підвищення ефективності застосування ЗС та побудові ефективної моделі поширення акустичних сигналів в складних перешкодових середовищах з урахуванням сучасних засобів протидії як у кібернетичному так і фізичному просторі [4].

Крім того одним із ключових напрямків, що визначає перспективи розвитку науково-технічної та технологічної бази удосконалення існуючих та розробки перспективних зразків ОВТ є розробка науково-методичного апарату обґрунтування вимог до характеристик таких зразків ОВТ. В умовах активної фази бойових дій та з метою ефективного відбиття військової агресії рф встановлено,

що оснащення підрозділів ПсО має проводитися тільки озброєннями та військовою технікою, яка за своїм технічним рівнем не поступається або перевершує іноземні зразки ОВТ. Отже, розробка науково обґрунтованих методів обґрунтування вимог до характеристик зразків ОВТ є актуальною. Тому одним основних завдань, яке потребує вирішення на сучасному етапі, для підвищення ефективності ПсВ полягає в розробленні методу технічного обґрунтування вимог до мобільних ЗС підрозділів психологічних операцій Збройних Сил України.

Список використаних джерел:

1. Орищук І. О. Марченков С. М. Бойове застосування підрозділів і частин ІПсО. ч. 1. Структура та озброєння сил психологічних операцій збройних сил російської федерації та країн НАТО: консп. лек. Житомир: ЖВІ, 2021. 193 с.
2. Грищук Р. В., Орищук І. О., Савчук В. С. Аналіз ролі й місця сил та технічних засобів психологічних операцій в локальних війнах та збройних конфліктах сучасності. Інформаційні технології у сфері безпеки та оборони. Київ : НУОУ, 2017. С. 27-30.
3. Грищук Р. В. Основи кібернетичної безпеки: монографія / відп. ред. Ю. Г. Даник, Житомир : ЖНАЕУ, 2016. 636 с.
4. Грищук Р. В., Канкін І. О., Охрімчук В. В. Технологічні аспекти інформаційного протиборства на сучасному етапі. Захист інформації. Київ, 2015. Т. 17. – № 1, С. 80–86.

Роман ПАСІЧНИЙ, к.політ.н., доц.
НУ “Львівська політехніка”
ORCID: 0000-0002-4687-3523
E-mail: roman.y.pasichnyi@lpnu.ua

МЕДІАГРАМОТНІСТЬ ЯК ЧИННИК ПРОТИСТОЯННЯ ВОРОЖИМ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ОПЕРАЦІЯМ

Проблематика протидії ворожим інформаційним впливам, набула особливої актуальності в контексті російсько-української війни оскільки інформаційно-психологічні операції (ІПСО) чинять загрозу суспільному спокою та національній безпеці. Науково-технічний прогрес сприяє різноманіттю засобів ведення інформаційних атак, а залучення недержавних акторів та інформаційних технологій (зокрема соціальних мереж) дають можливість здійснювати прихований тиск на супротивника який камуфлюється під “громадську думку” або “настрої населення”. На сьогоднішній день існує значна кількість визначень ІПСО, від затверджених у статутах збройних сил [1] до наукових дефініцій. Разом з тим,

усі вони зводяться до розуміння інформаційно-психологічних операцій, як заходів з метою впливу на поведінку громадян в інтересах авторів ІПСО.

Особливостями російських ІПСО з 2022р.є їх застосування в вузькому значенні, а саме як інструмент, що супроводжує бойові дії або передує їм і застосовуються переважно для деморалізації і дезорієнтації ЗСУ та цивільного населення.

Зазвичай, дослідники виділяють три рівні операцій, в залежності від масштабу впливу: стратегічні, оперативні та тактичні [2, с. 7]. Відповідно до масштабів впливу ІПСО, необхідно на нашу думку, розрізняти і засоби протидії. Протидіяти на стратегічному рівні, який спрямований на просування проросійських наративів в світовому масштабі, безперечно мають працювати державні інститути. Макаренко Л., вважає, що таким інструментом протидії можуть стати стратегічні комунікації [3]. На оперативному та тактичному рівні з цією задачею протидії ІПСО, на нашу думку, краще справляться місцева влада та громадський сектор, зокрема відповідальні локальні ЗМІ, оскільки операції такого рівня часто орієнтовані на аудиторію по географічному принципу і діють вибірково на населення певного регіону. Органам влади на місцях або ЗМІ простіше і швидше перевірити/спростувати дезінформацію та прокомунікувати з місцевим населенням.

Окрема роль у процесі протидії інформаційним впливам на локальних рівнях, відводиться освіті, зокрема формуванню навичок критичного мислення та медіаграмотності. Розвиток цих навичок є своєрідною “вакцинацією” суспільства щодо дезінформації та ІПСО. Вагому роль у формування медіаграмотності громадян відіграють такі ініціативи як: заходи з медіа грамотності Академії Української преси, О.Мороз “Як не стати овочем”, А.Романюк “Нота Єнота”, “StopFake”, “По той бік новин”, матеріали “VoxCheck”, “Texty.org” та інші. Незважаючи на таку значну кількість освітніх ініціатив, з 2020р до 2022р., відсоток осіб які відвідали курси зросло з 2% до 5%. ГО “Детектор медіа” здійснило дослідження “Індекс медіаграмотності українців: 2020-2022” згідно якого івень загального індексу медіаграмотності українців значущо змінився за два роки: з 2020 по 2022 рік. Частка аудиторії з вищим за середній рівнем показника зросла з 55% до 81%. Показник зріс завдяки тому що, українці частіше шукають посилання на джерело в матеріалі (39% vs 28%), орієнтуються на справжність на відео/фотопідтвердження (32% vs 26%), перевіряють інформацію на достовірність з 24% до 47%.Також більша кількість українців ідентифікують маніпуляції в ЗМІ, ознайомлені з ознаками достовірності новин, знайомі з принципами журналістської етики [4].

Незважаючи на зростання показників медіа грамотності, динаміка зростання показника відвідуваності освітніх ініціатив залишається низькою. Формування необхідних фахових компетенцій необхідно ввести в освітні стандарти не тільки для спеціальностей вищої, але й середньої школи та позашкілля. Окрему увагу

варто приділяти дорослому населенню, зокрема проводити освітню й роз'яснювальну особам старшого покоління. Питання форм та методів роботи з цими категоріями населення, залишається відкритим.

Список використаних джерел:

1. Field Manual 33-1. Psychological Operations. https://web.archive.org/web/20100902004138/http://www.enlisted.info/field-manuals/fm-33-1-psychological-operations.shtml
2. Мегель А., Яремчук М. Ворожі ІПСО. Як визначити та протистояти. Київ, 2022. – 98 с.
3. Макаренко Л.П. Стратегічні комунікації як засіб запобігання та протидії інформаційним війнам. Регіональні студії, ДВНЗ "Ужгородський національний університет", №30, ст.75-82.
4. Індекс медіаграмотності українців: 2020-2022ю ГО "Детектор медіа", квітень 2023. https://detector.media/doc/images/news/58855/ua_report_medialiterasy_index-dm_20-22_short-2.pdf?fbclid=IwAR0rFXFyJRZAYeQhAonPuYiNuSpzVNq-3KKAE5VV3yS37CPLW_2RNClXp64.

Вадим ПАХОЛЬЧУК, д.ф.
ВІ КНУ ім. Тараса Шевченка
ORCID: 0000-0002-9657-6148
E-mail: vadym_pakholchuk@knu.ua

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ОПЕРАЦІЇ ІЗ ВИКОРИСТАННЯМ ЕКОНОМІЧНИХ ТА ФІНАНСОВИХ НАРАТИВІВ

Інформаційно-психологічні операції (далі – ІПСО), відіграють важливу роль у формуванні економічного та фінансового середовища. Даний вид заходів включає у себе стратегічне поширення інформації та маніпулювання психологічними факторами з метою впливу на процеси прийняття рішень у галузі економіки та фінансів. У даних тезах викладено багатогранний характер ІПСО та їх вплив на економічні та фінансові системи.

ІПСО охоплюють широкий спектр технік, включаючи пропаганду, дезінформацію та управління сприйняттям. Ці заходи можуть використовувати людські когнітивні упередження та емоції для досягнення конкретних економічних та фінансових цілей. Основною метою часто є здобуття конкурентної переваги, маніпулювання настроями ринку чи просування певної економічної програми.

ІПСО можуть впливати на настрої ринку шляхом стратегічного поширення позитивної або негативної інформації. Наприклад, неправдиві чутки про фінансовий стан компанії можуть призвести до панічного продажу чи купівлі акцій, спричиняючи значні коливання ціни на ринку.

Найбільш типовим у сфері бізнесу є використання трейдерами та інвесторами ІПСО для маніпуляції цінами акцій. Схеми "накачування і продаж" передбачає, що вартість акцій штучно завищують за допомогою оманливої інформації. Організатори даних заходів з часом зможуть ліквідувати позиції за завищеними цінами, вводячи в оману нічого не підозрюючих інвесторів та наносячи їм значні збитки.

Наприклад, на валютному ринку ІПСО можуть впливати на вартість валют. Уряди та інституції можуть поширювати викривлену економічну інформацію чи чутки, щоб девальвувати чи ревальвувати вартість своєї валюти для отримання конкурентної переваги в міжнародній торгівлі.

Емоції, такі як страх та жадібність, можуть бути використані для маніпуляції фінансовими рішеннями. Оманлива інформація, що викликає страх, може призвести до панічного продажу, в той час як обіцянка швидких прибутків може призвести до ірраціональних покупок [1].

На сьогодні ІПСО є невід'ємною складовою воєнних дій. Наприклад використання завищених інфляційних очікувань населення з метою створення дефіциту товарів першого вжитку шляхом підштовхування їх до створення додаткових резервів та ірраціональних покупок.

Проте характер подібних заходів може мати ознаки як мікро, так і макро рівня. Наприклад, психологічні операції Іраку у свій час мали на меті тиснути на ті країни, що підтримували коаліцію та ті ООН-резолюції, які були накладені на Ірак. Ще один напрям роботи Іраку полягав у залученні підтримки з метою накладення економічних санкцій на державу замість альтернативи проведення військових дій. А вже згодом проводилися операції для протидії економічним санкціям та їх зняттю [2].

ІПСО застосовувалися для підтримання економічних заходів, беручи участь в операціях у Іраку та Перській затоці. ІПСО також були важливою частиною декількох операцій по морським блокадам постачання, включаючи Операцію "Свобода Іраку".

Засоби національної сили постійно використовуються Урядом США для просування політики США по всьому світу. ІПСО підтримує багато дипломатичних, інформаційних, військових та економічних заходів для досягнення цілей Уряду США.

Пропагування наративів сильної світової економіки з метою підвищення національної безпеки, сприяючи процвітанню і свободі в інших частинах світу посилює економічний вплив провідних країн світу. Економічне зростання, розвиток вільної торгівлі та вільних ринків сприяє створенню глобальної

економічної системи, яка в свою чергу об'єднує розрізнені ринки та держави. Однак у глобальній та взаємопов'язаній системі уряди можуть використовувати свою економічну потужність як інструмент національної сили. Прикладом економічного заходу є встановлення зон виключення. Метою може бути переконання націй чи певних цільовх груп змінити свою лінію поведінки на вимоги санкціонуючого органу або боротися із подальшими санкціями чи загрозою застосування сили.

Економічні засоби тиску та психологічні операції (ІПСО) впливають на національну безпеку та зовнішню політику всіх держав. Просування ідей економічного зростання через вільну торгівлю та ринки сприяє загальному процвітанню і може використовуватися для досягнення стратегічних цілей. Також важливо розуміти роль психологічних операцій у впливі на громадську думку та підтримку різних заходів, включаючи введення санкції, проведення блокад та створення зон виключення. В той же часз міна національної стратегії або політики може вплинути на характер та масштаб використання ІПСО для досягнення національних цілей та підтримання безпеки.

Список використаних джерел:

1. Deakin R. L. Economic information warfare: Master Thesis. 2003. 221 p.
2. Goldstein F. L. Psychological operations: principles & case studies. Diane Pub Co, 1996.

Людмила ПЕЛЕПЕЙЧЕНКО, д.філол.н., проф.
ORCID: 0000-0002-9812-986X
E-mail: pelepln2014@gmail.com
Світлана РЕВУЦЬКА, к.пед.н., доц.
НАНГУ
ORCID: 0000-0002-6568-236X
E-mail: svetrev2014@gmail.com

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ОПЕРАЦІЇ В ПРОЦЕСІ ЗДІЙСНЕННЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ: ДОСВІД І ПЕРСПЕКТИВИ

Інформаційно-психологічні операції (ІПО) являють собою потужний механізм комунікативного впливу на масову свідомість. Названі операції здавна широко застосовуються і у виконанні воєнних завдань [6]. Попри великий потенціал, важливий для воєнної сфери, ІПО недостатньо досліджені в науці. Можливо, це пояснюється тим, що сам феномен ІПО перебуває на перетині декількох наук: воєнного мистецтва, психології, політології, теорії комунікації і деяких інших. Мало

вивчене питання і про те, яке місце посідають ІПО в процесі здійснення стратегічних комунікацій.

З огляду на значущість заявленої проблеми і її недостатню вивченість у нашому дослідженні була поставлена мета окреслити підходи до здійснення ІПО в процесі стратегічних комунікацій військових формувань України.

Передусім важливо уточнити сам термін "інформаційно-психологічні операції", який у поданому формулюванні сприймають не всі науковці. Деякі вчені розмежовують поняття інформаційних операцій і психологічних операцій [4; 5]. Інші дослідники розглядають інформаційний вплив як один із заходів психологічної війни, що передбачає вплив інформацією (словом) на свідомість, і тоді логічно прийняти термін інформаційно-психологічні операції [3]. Приєднуючись до останнього підходу, ми беремо до уваги ще й такі аргументи:

1. Будь-яка інформація, що подається адресату, тією чи іншою мірою впливає на його картину світу, оцінки, а отже, може здійснювати і психологічний вплив, коригуючи поведінку адресата.

2. Психологічний вплив не може здійснюватися без певної інформації, обсяг і зміст якої залежить від умов дискурсу.

Перш ніж окреслювати підходи до здійснення ІПО в процесі стратегічних комунікацій розглянемо питання про те, як представлено названий вид діяльності в Доктрині стратегічних комунікацій ЗСУ [1] та Доктрині стратегічних комунікацій НГУ [2]. Зауважимо, що в жодній із Доктрин термін ІПО не використовується.

У Доктрині ЗСУ дається визначення термінів, що стосуються суто інформаційної діяльності (інформаційна сфера, простір, середовище, дії, ефект, спроможності, інформаційно-аналітичне забезпечення [1, с. 6-7]), а також термінів, пов'язаних із психологією (психологічна акція, ефект [там само, с. 7]). Зауважимо, що у визначенні психологічної акції фіксується увага на зв'язку з інформацією: "Психологічна акція – організоване застосування визначених сил і засобів Сил спеціальних операцій для виконання завдань з інформування та (або) здійснення психологічного впливу на емоційний стан, мотивацію, раціональне мислення обмеженої за масштабом та районом цільової аудиторії та зміни моделі її поведінки у спосіб, що сприятиме досягненню військових та політичних цілей" [1, с. 8].

У Доктрині НГУ згадуються вже не тільки загальні терміни, пов'язані з інформаційною діяльністю, а й термін "інформаційна операція" [2, с. 6]. Наводиться визначення термінів "психологічна акція" та "психологічна операція", які в концепції документа співвідносяться як загальне і часткове: "Психологічна операція – **сукупність** узгоджених і взаємопов'язаних за метою, завданням, місцем і часом **психологічних акцій** та інших дій, застосування визначених сил і засобів, які **проводяться за єдиним замислом і планом**, для здійснення впливу на когнітивну, емоційну і мотиваційну сфери визначених цільових аудиторій та зміни моделей їх поведінки на сприятливі для досягнення військово-політичних, військових і невійськових цілей під час виконання завдань у складі операції Об'єднаних сил" [там

само, с. 8].

Викладені спостереження свідчать, що попри відмінності у термінології в обох Доктринах визнається важливість психологічних та інформаційних операцій і не заперечується взаємозв'язок між ними.

Про практичне втілення заявлених підходів можна довідатися, ознайомившись із сайтами названих формувань в мережі Інтернету та відеороликами, представленими в YouTube. В названих видах кіберпростору подано багато цікавої і корисної інформації, яка, безсумнівно, здатна здійснити і когнітивний, і суто емоційний вплив на адресатів, проте подані матеріали є епізодичними, не пов'язаними з певними темами, тому вони не являють собою ІПО, які мають бути підготовлені цілеспрямовано, "за єдиним замислом і планом" [там само]. Отже, можна стверджувати, що потенціал ІПО у здійсненні стратегічних комунікацій повною мірою ще не використано. Окреслимо перспективи цієї діяльності. Зауважимо, що в нашій праці йдеться про відкриті ІПО для дружньої і нейтральної цільових аудиторій. Такий ракурс пояснюємо тим, що ІПО для ворожої аудиторії мають бути таємними, і їх мають розробляти військові, поставивши за мету максимально сприяти виконанню службово-бойових завдань у протиборстві з ворогом. Стосовно відкритих ІПО, обраних в нашому дослідженні, вважаємо за доцільне висвітлити такі питання стратегічної діяльності: цільові орієнтири та тематика ІПО у період повномасштабної війни російських агресорів проти України; основні принципи роботи із цільовими аудиторіями; форми і методи стратегічного впливу; очікуваний результат.

Обов'язково умовою розроблення ІПО вважаємо урахування соціального контексту – в нашому випадку повномасштабної війни. У цей період, на нашу думку, цільовою аудиторією ІПО доцільно зробити молоде покоління і пересічних громадян зрілого віку. Основною метою ІПО має бути формування масової свідомості молоді і громадян зрілого віку, в якій ключовими поняттями будуть такі, як патріотизм; ненависть до ворога; бажання всіляко підтримувати українських військових. Виховання патріотизму базується на багатовекторній тематиці: обізнаності з реальною історією України, а не вигаданою пропагандою радянського періоду; ознайомленні з видатними постатями українців, які зробили значний внесок у різні сфери розвитку України; адекватне пояснення сучасних подій і т. ін. Із комплексу принципів роботи назвемо основні. На нашу думку, до них належать такі: інтерактивний зв'язок із цільовою аудиторією і принцип діяльнісного підходу до роботи. Інтерактивний зв'язок потребує таких форм і методів стратегічного впливу, які б не обмежувались наративами, а поєднували розповіді і пояснення з переконаннями в правильності певних тверджень та спростуванні хибних думок, а особливо фейків і маніпулятивних повідомлень агресорів. Діяльнісний підхід передбачає, що і в переконанні, і в спростуванні думок на сайтах військових формувань будуть брати участь представники обраних цільових аудиторій. Очікуваний результат ІПО для дружніх і нейтральних цільових аудиторій можна

стисло описати так: у масовій свідомості українців створяться своєрідні когнітивні опори, які допоможуть їм давати адекватні оцінки подіям і не реагувати на деструктивні наративи інформаційних агресорів.

Узагальнимо викладене і сформулюємо основні думки. У здійсненні стратегічних комунікацій до початку повномасштабної війни не повною мірою використано позитивний потенціал ІПО, що необхідно взяти до уваги в майбутній стратегічній діяльності. Тематика, цільові установки, принципи, форми і методи стратегічного впливу мають забезпечити створення когнітивних опор у масовій свідомості українців, які забезпечать правильну інтерпретацію подій та імунітет до деструктивного впливу ворожих ІПО.

Список використаних джерел:

1. Доктрина зі стратегічних комунікацій. Вересень 2020. URL: https://cutt.ly/HbJhqXT
2. Доктрина стратегічних комунікацій Національної гвардії України. URL: https://cutt.ly/aOGWQSR.
3. Компанцева Л. Ф. Соціальні комунікації для фахівців сектору безпеки та оборони: підручник: у 2-х т. К.: Нац. акад. СБУ, 2016. Т.1. 267 с.
4. Почепцов Г. Від “покемонів” до гібридних війн: нові комунікативні технології XXI століття: монографія. К: Видавничий дім “Києво-Могилянська академія”, 2017. 260 с.
5. Присяжнюк М. М., Пампуха І. В., Петрик В. М. Основні поняття та особливості проведення спеціальних інформаційних операцій [Електронний ресурс] *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2014. Вип. 46. С. 112–120. URL: http://nbuv.gov.ua/UJRN/Znpviknu_2014_46_19
6. Сунь-дзи. Мистецтво війни / пер. Лесняк Сергій. Київ: Либідь, 2015. 112с. URL: https://cutt.ly/BnekCyw.

Сергій ПЕРЕГУДА
НУОУ
ORCID: 0009-0004-8020-7841
E-mail: s.peregyda@i.ua

МЕТОДИЧНИЙ ПІДХІД ЩОДО ОЦІНЮВАННЯ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ ЗА СТАНДАРТАМИ НАТО

Оцінювання психологічних операції за стандартами НАТО проводяться у динамічній обстановці, домени якої (політична, економічна, соціальна, військова,

інфраструктурна, інформаційна (PMESII) постійно змінюються. Командири потребують зворотного зв'язку щодо оцінки операцій щоб бути поінформованими про прогрес зі створення потрібних ефектів, встановлення вирішальних умов і досягнення цілей, що у свою чергу дозволяє вносити зміни до оперативних планів і надавати пропозиції щодо прийняття рішень вищим військовим і політичним керівництвом. Оцінювання психологічних операцій також забезпечує важливий внесок до процесу збирання та обробки інформації, який нарощує та підтримує цілісне розуміння ситуації та оперативної обстановки.

Аналіз джерел показав [1-3], що оцінювання психологічних операції дозволяє виміряти прогрес та результати операцій у військовому контексті та послідуючу розробку висновків і рекомендацій для прийняття рішень.

У [2] зазначено, що показник оцінювання ефективності є міра, що використовується для визначення поточного стану системи.

В [3] навпаки визначено, що показник оцінювання є міра, що використовується для визначення завершеності (повноти і якості) проведених дій військ (сил). Також в цьому джерелі наведено, що оцінювання ризику– постійно триваюче відслідковування (моніторинг) стратегічних і оперативних ризиків на відповідному рівні військового командування.

Метою тез є наведення методичного підходу щодо оцінювання психологічних операції за стандартами НАТО.

Метою оцінювання психологічної операцій є підтримка процесу прийняття рішень у трьох сферах:

оцінюється прогрес у виконання плану операції (дії, завдання);

оцінюється ефективність проведених дій шляхом вимірювання досягнення результатів (створення необхідних ефектів, встановлення вирішальних умов, досягнення цілей та кінцевого стану);

робляться висновки щодо минулої обстановки, у деяких випадках проводиться прогнозування майбутніх трендів і розробляються рекомендації, наприклад, щодо переходу операції у наступну фазу (етап) або внесення змін до плану операції на базі цих висновків.

Оцінювання ПсО може бути застосоване до конкретних операцій, подій або тем, як в контексті плану операції, так і поза ним. Оцінювання може розглядати цілий ряд часових відрізків від короткотермінових змін до довготермінових довжиною у роки. Існує багато шляхів, за якими відповідальність за рівень і часовий період оцінювання операції можуть бути розділені, в залежності від особливостей контексту, рівня командування та потреб командира [4].

В цілому на будь-якому рівні та періоді часу існує два типи оцінювання операцій, які можуть проводитись під час їх ведення: "історичний" та "прогностичний". "Історичне" оцінювання у ході операції забезпечує командира оцінкою виконання дій та прогресом в напрямку створення потрібних ефектів, створення вирішальних умов, досягнення цілей та кінцевого стану. Цей тип

оцінювання використовує історичні дані для визначення трендів змін, включаючи поточний стан. “Прогностичне” оцінювання будується на історичному оцінюванні та допомагає екстраполювати поточні тренди в майбутнє, таким чином визначаючи потенціальні можливості та ризики для командира.

Оцінювання ПсО підтримує та постійно взаємодіє з процесами збирання та обробки інформації, планування та ведення операцій.

Процес збирання та обробки інформації є важливим під час планування операції, але також тісно пов’язане із веденням операції та її оцінюванням. Системне розуміння є важливим для початкової розробки процесу оцінювання операції, а через цикл оцінювання процес повинен надавати нові дані, а також використовувати результати оцінювання. Продукти, що розробляються у ході процесу оцінювання операції, допомагають зрозуміти оперативну обстановку і ця оновлена інформація повертається назад до бази знань. Процес оцінювання операції є взаємозалежними через цінність їх спільних взаємозв’язків з базою знань.

Планування. Оцінювання операції має важливий зв’язок з плануванням: персонал, який залучений до планування та оцінювання операції, повинен працювати у тісній співпраці для забезпечення того, щоб всі завдання, дії, ефекти та цілі, які визначені у плані, були вимірюваними, а складові документи плану розглядали б ресурси та заходи, які необхідні для проведення оцінювання операції. Головним призначенням оцінювання операції є підтримка прийняття рішення шляхом надання необхідних рекомендацій для корегування плану на основі результатів його виконання.

Виконання (ведення операції). Виконання відноситься до всіх процесів і технік управління операцією. Це включає підготовку розпорядчих документів, управління бойовими діями, координацію і взаємодію з іншими акторами, включаючи невійськові. Хоча характер управління операціями може сильно варіюватись в залежності від обстановки, масштабу операції та персоналу, спільним компонентом є необхідність постійного зворотного зв’язку щодо прогресу завдань і дій, створення потрібних ефектів і досягнення цілей. Плани операцій не розглядаються такими, що є повністю вірними, тому протягом їх виконання вони потребують постійного уточнення на основі оцінювання ходу операції. Тому постійне оцінювання є необхідним елементом виконання плану операції.

Таким чином, процес оцінювання психологічної операції включає чотири основні кроки:

1 крок – вироблення порядку оцінювання операції та підтримки планування;

2 крок – розробка плану збору даних інформації;

3 крок – збір даних та їх зберігання;

4 крок – аналіз, інтерпретація та рекомендації.

Кожен із наведених кроків буде наповнено відповідно до змісту керівних документів Збройних Сил України за напрямком організації психологічної операції.

Список використаних джерел

1. NATO Operations Assessment Handbook", Version 3.0, посібник НАТО. 01 July 2015.

2. AJP-5 Allied Joint Doctrine for the Planning of Operations, Edition A Version 2, 24 May 2019, доктрина НАТО з оперативного планування.

3. ATP 3-13.1 The Conduct of Information Operations, публікація СВ США щодо ведення інформаційних операцій. October 2018;

4. Psychological Operations Process Tactics, Technics and Procedures (FM 3-05.301), 30 August 2007. Настанова з психологічних операцій СВ США.

Ярослав ПОРАДА
ЖВІ ім. С. П. Корольова
ORCID: 0009-0000-8241-348X
E-mail: yarosla.advice@gmail.com

ВИКОРИСТАННЯ ЗАСОБІВ ПРОПАГАНДИ ЗС РФ В ХОДІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

У ситуації повномасштабної агресії Російської Федерації (РФ) проти України важливо звертати особливу увагу на питання інформаційної безпеки громадян, оскільки вплив інформації на населення та на Збройні Сили України стає однією з основних складових сучасної гібридної війни. Російська пропаганда включає в себе широкий спектр заходів, спрямованих на створення дезорієнтації та деморалізації українського суспільства.

Збройні Сили РФ мають значний досвід використання різноманітних засобів впливу на своє власне населення та на сусідні країни, включаючи Україну. В цьому контексті досліджуються методи і техніки впровадження пропаганди, які включають розповсюдження фейкових новин через російські ЗМІ та спеціальні військові підрозділи. Фейки, як інструмент, що спотворює факти або надає неправдиву інформацію, використовуються для маніпуляції свідомістю цільової аудиторії. Це може включати спотворення контексту, підштовхування до певних дій чи думок, які служать інтересам тих, хто поширює фейки.

Для захисту від такої фейкової інформації важливо розвивати медійну грамотність та критичне мислення в суспільстві. Особливу увагу потрібно приділяти перевірці джерел інформації та фільтрації сумнівних джерел. Крім

цього, російська пропаганда використовується для формування враження про гуманітарну допомогу на тимчасово окупованих територіях України. Російські війська можуть видавати допомогу мирним жителям, проте це робиться з метою створення позитивного іміджу у російських ЗМІ та захоплення влади над інформаційним простором.

Також слід зазначити, що російська пропаганда активно використовує місцеве населення на тимчасово окупованих територіях України для поширення своїх інформаційних повідомлень. Збройні сили РФ можуть використовувати цивільних жителів як "лідерів думок", щоб впливати як на власне населення, так і на населення України.

Розвиток медійної грамотності та критичного мислення в суспільстві є важливою задачею, яка допоможе людям краще розуміти та аналізувати інформацію, яка до них надходить. Ось кілька кроків, які можуть сприяти цьому процесу:

навчання в школах і навчальних закладах: Медійна грамотність і навички критичного мислення можуть бути впроваджені в навчальні програми. Уроки з медійної грамотності можуть включати розуміння різних типів медій (текст, відео, соціальні мережі), вміння розпізнавати маніпулятивні прийоми та фейки, а також аналіз структури новин та джерел інформації;

сприяння самоосвіті: Людям потрібно надавати можливість навчатися самостійно. Доступ до онлайн-ресурсів, які надають практичні поради щодо перевірки інформації та розвитку критичних навичок, може бути корисним;

критичне сприймання інформації: Навчити людей питати про джерело інформації, його надійність та можливі мотиви публікації. Важливо навчити впізнавати заголовки, які мають схильність до сенсаційності та зайвого емоційного навантаження;

застосування критичного мислення: Навчити аналізувати та порівнювати інформацію з різних джерел перед тим, як приймати важливі рішення. Демонструвати, як розпізнавати брехливу інформацію і як шукати додаткові джерела підтвердження;

критичний погляд на соціальні мережі: Навчити людей бути обережними в соціальних мережах, де фейки і маніпуляція інформацією поширюються особливо швидко. Фокусувати увагу для перевірки джерел та фактів перед репостом або поділом інформації;

сприяння обговоренню: Важливо створювати платформи для вільного обговорення інформації та поглядів, але з розумінням, що кожен має право на свою думку. Дискусії допомагають розвивати аргументаційні навички та критичне мислення.

Важливо розуміти, що розвиток медійної грамотності та критичного мислення – це постійний процес, і він важливий для формування раціонального та інформованого суспільства, особливо в умовах поширення фейкової інформації та

пропаганди. Загалом, роль інформаційної війни та пропаганди стає дуже важливою в умовах конфлікту в Україні, і аналіз методів протидії пропаганді відіграє ключову роль у підтримці національної безпеки та збереженні довіри громадян до інформаційного простору.

Список використаних джерел:

1. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №685/2021 URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення 18.09.2023).

2. Дезорієнтація, демотивація, дезорганізація і деморалізація: якими методами Росія веде інформаційну війну проти України URL: https://vgolos.ua/news/dezoriientaciya-demotivaciya-dezorganizaciya-i-demoralizaciya.-yak-rosiya-vede-informaciynu-viynu-proti-ukrayini_1414097.html (дата звернення 18.09.2023).

3. Інформаційна війна: як розпізнати фейки та маніпуляції URL: https://naurok.com.ua/prezentaciya-informaciyna-viyna-yak-rozpiznati-feyki-ta-manipulyaci-344784.html (дата звернення 18.09.2023).

Інна ПРОНОЗА, к.політ.н., доцент
ORCID: 0000-0002-2683-0630
E-mail: inna140379@ukr.net
Марія СУРОВА
ДЗ “Південноукраїнський національний педагогічний університет імені К.Д. Ушинського”
ORCID: 0009-0007-3762-1555

ІНФОРМАЦІЙНІ (ПСИХОЛОГІЧНІ) ОПЕРАЦІЇ ЯК ІНСТРУМЕНТ ІНФОРМАЦІНОЇ ВІЙНИ

Докорінні зміни, що наразі відбуваються в сучасному геополітичному та безпековому середовищах навколо нашої держави, обумовлюють необхідність аналізу, вивчення та подальшого практичного застосування нових підходів до планування, організації та проведення інформаційних (психологічних) операцій, задля уникнення та зменшення негативних наслідків їхнього впливу. Оскільки інформаційні (психологічні) операції є однією з сучасних форм геополітичного протиборства, в основі яких лежить досягнення і утримання інформаційної переваги на усіх теренах інформаційно-політичного сучасного суспільства.

Безперечно що нові тенденції у сфері способів і засобів ведення війни, які спричинені розвитком інформаційних технологій, свідчать про революційні зміни, які відбуваються у військовій справі та безпековій політиці держави.

В гібридній війні проти України “росія” поєднує військові методи боротьби з політичним тиском і економічним шантажем, інформаційними (психологічними) операціями (ІПсО) у засобах масової комунікації, зокрема, в соціальних мережах з використанням проплачених інтернет-тролів, ботів та ботоферм, навмисним введенням українського суспільства в оману задля маніпулятивного впливу на свідомість громадян шляхом поширення дезінформації з подальшою упередженою інтерпретацією певних подій, що спрямовано на формування громадської думки, що вигідна країні-агресору [0]. Таким чином інформаційна складова будь-яких як національних, так і міжнародних суспільних процесів відіграє ключову роль.

Функціонально інформаційна складова реалізується завдяки таким явищам як “інформаційна війна” та “спеціальні інформаційні операції” (далі – СІО). Для змістовного вивчення визначення цих понять та явищ можемо звернутись до досліджень провідних фахівців ЦРУ та МО США: “Інформаційна війна – це попередньо сплановані психологічні дії в мирний чи військовий час, спрямовані на ворожу, дружню чи нейтральну аудиторії, які впливають на установки і поведінку людей з метою отримання політичної чи військової переваги” [0].

В умовах сьогодення відбувається інтенсивне використання засобів та інструментів інформаційної війни з метою забезпечення власних інтересів світовими лідерами та країнами, проводяться дослідження і розробки нової інформаційної зброї, що дозволяє здійснювати безпосередній контроль над інформаційними ресурсами потенційного противника, а в необхідних випадках прямо впливати на них. З огляду на це, поняття “спеціальні інформаційні операції” (спецінформоперації, психологічні операції) необхідно розглядати через призму інформаційних війн.

Звернемо увагу, що Польовий статут FM 33-1 МО США надає чітке визначення спецінформоперації: “Інформаційні операції – це попередньо сплановані психологічні дії в мирний і військовий час, спрямовані проти ворожої, дружньої або нейтральної аудиторії шляхом впливу на настанови та поведінку з метою досягнення політичних або військових переваг. Вони включають в себе психологічні дії з стратегічними цілями, психологічні консолідуючі дії та психологічні дії з безпосередньої підтримки бойових дій” [0]. Тобто інформаційно-психологічні операції “є основним компонентом інформаційно-психологічної війни” [0] і за характером впливу їх класифікують на:

“пропагандиські”, коли інформаційні акції мають переважно пропагандистський характер, наприклад, в ході політичної боротьби чи в рамках просування ідеології;

“дезінформаційні”, коли метою є введення конкурента в оману, такі операції використовуються як в політичній і економічній боротьбі, так і у військових конфліктах;

“маніпулятивні”, коли основним завданням є контроль поведінки противника;

оборонні операції (“контроперації”), в яких ставиться за мету нейтралізувати інформаційно-психологічний вплив противника, захистити від цього впливу своїх прибічників, і здійснити інформаційно-психологічний вплив у відповідь.

Зазначаємо, що СІО як інструмент інформаційної війни та ресурс в системі протидії загрозам національній безпеці України посідають особливе місце – як самостійний механізм реалізації заходів інформаційно-психологічного спрямування і як допоміжний напрям діяльності в реалізації політичних, економічних, військових та інших заходів, які без належної інформаційної підтримки приречені на неуспіх. СІО можуть реалізовуватись не лише при забезпечені інформаційної, але й інших складових національної безпеки, яка є складним та багатоаспектним феноменом.

Список використаних джерел:

1. Деркаченко Я. Інформаційно-психологічні операції як сучасний інструмент геополітики. Глобальна організаціясоюзницького лідерства. 2016. URL : http://goal-int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/
2. Пєвцов Г. В., Залкін С .В., Сідченко С. О., Хударковський К. І. Інформаційно-психологічні операції: планування, протидія, технології: монографія. Харків. ДІСА ПЛЮС, 2020. 252 с.
3. Стратегічна концепція оборони та безпеки членів Організації Північноатлантичного договору від 19.11.2010 р. URL: https://www.nato.int/cps/uk/natohq/official_texts_68580.htm.
4. How We Serve National Security. URL:https://www.janes.com/FM%2033-1.

Володимир РАХІМОВ
НУОУ
ORCID: 0000-0001-9868-986X
E-mail: paradokc1@gmail.com
Олексій ЧЕРНОБАЙ, д.ф.
НУОУ
ORCID: 0000-0001-9970-5534
E-mail: oieksii.chernobai@gmail.com

ДИФУЗІЯ ІННОВАЦІЙ – ГОЛОВНИЙ ІНСТРУМЕНТ ВПРОВАДЖЕННЯ НАРАТИВУ В СОЦІАЛЬНИХ МЕРЕЖАХ В ІНТЕРЕСАХ ЗВ'ЯЗКІВ З ГРОМАДСЬКІСТЮ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

У сучасному світі інформація має вирішальне значення для прийняття рішень, як на театрі війни так і у свідомості кожного військовослужбовця, причому те, як відбувається інформування та психологічний вплив на визначені цільові аудиторію, залежить від того, яка інформація циркулює в

інформаційному середовищі. Основними засобами дій в інформаційному середовищі є психологічні операції, військові зв'язки з громадськістю, електромагнітний вплив, операції в кіберпросторі й бойові дії, які мають бути скоординовані і інтегровані протягом усього процесу планування та підтримувати усі види діяльності і відповідати наративу [1].

Зв'язки з громадськістю як головний елемент стратегічних комунікацій відповідає за підтримку та поширення інформації щодо військових цілей і завдань Сил оборони шляхом своєчасного донесення до аудиторії точної інформації.

Сфера зв'язків з громадськістю зазнала значного розвитку, особливо у військових організаціях, таких як Збройні сили України (далі – ЗСУ). Оскільки поширення інформації стає все більш складним і важливим, прийняття інноваційних стратегій є необхідним елементом діяльності для налагодження комунікацій на всіх рівнях управління та з усіма верствами населення. Розглядаючи підходи маркетингу щодо продажів товарів в соціальних мережав, а саме дифузію інновацій дає змогу проаналізувати та використати дану модель для аналізу процесів поширення інформації в соціальних мережах.

Розглядаючи загальні підходи теорії дифузії інновацій, яка була розроблена Евереттом Роджерсом, який запропонував розуміння того, як нові ідеї, технології чи практики поширюються в суспільстві чи організації [2]. Він визначив п'ять категорій аудиторій: новатори, ранні послідовники, рання більшість, пізня більшість і відстаючі. Процес сприйняття щодо придбання товару, послуги або інформації включає в себе канали комунікації, час і соціальні системи, які є важливими компонентами для успішного впровадження інновацій. Ця теорія забезпечує надійну основу для розуміння того, як інновації, включно з наративними стратегіями, можуть бути ефективно представлені громадськості.

Зв'язки з громадськістю у Збройних Силах України (військові зв'язки з громадськістю) потребують в впровадженні ефективних наративних стратегій в соціальних мережах для взаємодії з громадськістю, зміцнення довіри та формування сприйняття. Добре сформований наратив, який поширюється в соціальній мережі може допомогти донести до суспільства місію, цінності та внесок ЗСУ у врегулюванні або вирішенні будь якої ситуації в умовах миру чи війни, а також усунути проблеми з комунікацію та слугувати, як інструмент протидії дезінформації.

У контексті впровадження наративу військові зв'язки з громадськістю мають визначити новаторів та першопрохідців у визначених силах та серед цільової аудиторії. Залучення ключових осіб може створити вірусний ефект, який безпосередньо вплине на інших користувачів мережі, щоб вони прийняли наратив.

Теорія дифузії підкреслює важливість каналів комунікації для поширення інформації в соціальних мережах. Військові зв'язки з громадськістю маю визначити найбільш впливові та ефективні платформ для поширення свого наративу. Використовуючи соціальні мережі для проведення прес-релізів, інтерв'ю та ініціативи із залучення громадськості дає можливість ефективно доносити свої меседжі до більш ширшої цільової аудиторії.

Часові рамки відіграють важливу роль в процесі поширення інформації в соціальній мережі, на різних проміжках час буде спостерігатись різна динаміка сприйняття та поширення, яка буде відображати параметри залученості та охоплення цільових аудиторій, що дасть можливість визначити коли зовнішній вплив такий як реклама, актуальність, доступність перейде у внутрішній вплив де будуть задіяні соціальні аспекти мережі. Послідовне донесення інформації та її підживлення є дуже важливими процесі поширення наративу.

В процесах інформування та поширення інформації в соціальних мережа військові зв'язки з громадськістю повинні продемонструвати свою відданість прозорості, чесності та етичній поведінці. Цього можна досягти, демонструючи досягнення організації, визнаючи виклики та надаючи точну інформацію.

Отже, в епоху цифрових комунікацій теорія дифузії інновацій є потужним інструментом для Збройних Сил України для ефективного впровадження наративів на платформах соціальних мереж в інтересах зв'язків з громадськістю. Визначаючи ключових користувачів соціальної мережі, обираючи відповідні канали комунікації, враховуючи час на сприйняття інформації, адаптуючись до зворотного зв'язку, для охоплення більшої цільової аудиторії, розбудовуючи довіру та впливаючи різні сегменти громадськості в мережі зв'язки з громадськістю у Збройних Силах України можуть формувати наративи, які будуть резонувати з визначеними цільовими аудиторіями та сприяти створенню позитивного іміджу Збройним Силам України як в серединні нашої держави так і за її межами. Оскільки інформаційна сфера продовжує розвиватися, застосування інноваційних стратегій, таких як дифузія інновацій, є важливим для впровадження їх в сфері військових зв'язків з громадськістю, щоб ефективно комунікувати з громадськістю.

Список використаних джерел:

1. Allied Joint Publication-10.1 (AJP-10.1), Edition A, Version 1,dated January 2023.

2. Rogers E. M. Diffusion of innovations (3rd ed.). New York: Free Press of Glencoe, 1983. 453 p.

Сергій СІДЧЕНКО, к.т.н., с.н.с.
ORCID: 0000-0002-1319-6263
E-mail: sidserg@email.ua
Сергій ЗАЛКІН, к.в.н., с.н.с.
ORCID: 0000-0002-0518-4414
E-mail: sergejzalkin1952@gmail.com
Костянтин ХУДАРКОВСЬКИЙ, к.т.н., доц., с.н.с.
ORCID: 0000-0002-9508-9014
E-mail: konsthud@meta.ua
Олександр РЕВІН
ХНУПС ім. Івана Кожедуба
ORCID: 0000-0001-8758-6419
E-mail: revin_al@meta.ua

ВАРІАНТ РЕАЛІЗАЦІЇ СЦЕНАРНОГО ПІДХОДУ ПРИ ПЛАНУВАННІ ІНФОРМАЦІЙНОЇ (ПСИХОЛОГІЧНОЇ) ОПЕРАЦІЇ

Інформаційні (психологічні) операції (ІПсО) і впливи (ІПВ) на сьогоднішній день є невід'ємною складовою збройної боротьби, а в умовах повномасштабної збройної агресії РФ проти України не варто недооцінювати значимість інформаційних засобів ведення війни. У воєнних доктринах більшості провідних країн світу інформаційні (психологічні) операції розглядаються, з одного боку, як важливий компонент підготовки і проведення військових операцій, а з іншого боку, як самостійний вид бойових дій.

Потенціал ІПсО (ІПВ), що здійснюється Україною стосовно РФ, ще не використаний повністю. Зокрема, певні зусилля можуть бути спрямовані на підрив економічної стабільності у визначеному регіоні, наприклад, у тимчасово окупованому Криму. Тож, спланована і проведена ІПсО з метою створення економічного безладу та поширення панічних настроїв серед місцевого населення може бути цілком виправданою. Для цього може бути застосований сценарний підхід при плануванні ІПсО (ІПВ). Розглянемо один із варіантів його можливої реалізації.

Значні обмеження транспортного сполучення тимчасово окупованого Криму з територією РФ, перспективи звільнення окупованих територій Силами оборони України та логістичні обмеження поставок різноманітних товарів на фоні значної інфляції російського рубля створюють необхідні інформаційні передумови для проведення ІПсО. Варіанти сценаріїв подібної операції можуть бути різні.

Інформаційним приводом може слугувати розповсюджений меседж про те, що Центробанк РФ, розуміючи безальтернативність звільнення Криму і виходу РФ

з його території, здійснює виведення з обороту в Криму російського рубля, замінюючи його на підробку.

Цільовою аудиторією для такої операції можуть бути дрібні підприємці та власне більша частина пересічного населення тимчасово окупованого Криму.

Інформаційний (психологічний) вплив на визначену цільову аудиторію передбачає виконання декількох етапів.

В ході підготовчого етапу проводиться аналіз інформаційної обстановки в даному регіоні, створюється узагальнений психологічний портрет цільової аудиторії та розробляється сценарій проведення ІПсО.

На наступному етапі створюється інформаційний привід, в ході якого відбувається виведення цільової аудиторії зі стану психологічної рівноваги. Для варіанту сценарію, що розглядається, таким приводом може бути вилучення з обігу підробок російського рубля із широким висвітленням даного факту у ЗМІ. Для цього можуть застосовуватися інформаційні канали в соціальних мережах (Telegram-каналах), інформаційні сайти Інтернет, передачі радіо- та відеомовлення, друкарська продукція тощо.

В ході основного етапу поширюється інформація (чутки) про виведення з обороту в Криму російського рубля.

На етапі закріплення результатів впливу поширюються песимістичні прогнози щодо подальшого розвитку подій, обговорюються винні, тощо.

Схема сценарію проведення ІПсО представлена у таблиці 1. Сценарій проведення ІПсО відображається у скоординованому плані його проведення та комплексі необхідних бойових і довідкових документів. При розробці сценарію проведення ІПсО визначаються основні та додаткові заходи, форми, методи та прийоми їх виконання.

Таблиця 1. Схема сценарію проведення ІПсО на зазначену цільову аудиторію тимчасово окупованого Криму

№ з/п	Складові сценарію	Заходи, що передбачаються	
		основні	додаткові
1	2	3	4
1.	Об’єкт впливу	Дрібні підприємці та більша частина пересічного населення Криму	
2.	Мета впливу	**Створення економічного безладу і поширення панічних настроїв серед місцевого населення**	
3.	Завдання впливу	Підрив економічної стабільності в регіоні	Висвітлення фактів незадоволення населення, поширення панічних настроїв, банкротство підприємців; обмеження доступу до товарів першої необхідності; створення передумов для масових акцій непокори та

№	Складові	Заходи, що передбачаються	
			підтримка Сил оборони України
4.	Інформаційний привід	Меседж про те, що Центробанк РФ скорочує фінансування будь-яких програм у тимчасово окупованому Криму і здійснює виведення з обороту російського рубля, замінюючи його на підробку	Несвоєчасна виплата заробітної плати, пенсій, соціальних виплат; підвищення цін; висвітлення у ЗМІ фактів знаходження (вилучення з обігу) підроблених російських рублів; пригнічення прав і свободи громадян
5.	Методи впливу	Безпосереднього впливу: залякування – донесення до цільової аудиторії спеціальної інформації або штучне створення таких обставин, що викликають у неї відчуття занепокоєності, сумнівів, невпевненості, страху, паніки	Опосередкованого впливу: дискредитація місцевої влади, економічних дій (неспроможність налагодити своєчасну виплату заробітної плати, пенсій, допомоги, поставку товарів першої необхідності, ліків)
6.	Канали впливу	соціальні мережі; чутки	
7.	Місця здійснення впливу	Інтернет; громадський транспорт; ринки; заклади громадського харчування	Інші місця скупчення людей
8.	Найбільш сприятливий час	Передвиборча кампанія; суспільно-політичні акції, акції громадянської непокори	
9.	Сили та засоби впливу	Підрозділи ІПсО (Інтернет); агенти впливу; FM-радіо	
10.	Бажаний стан об’єкту впливу	Панічні настрої серед населення; виїзд з території Криму російських громадян, колаборантів; втрата впевненості в поведінці	
11.	Ознаки прояву впливу	Офіційні заяви представників місцевої влади із спростуванням у засобах масової інформації	Коментарі, обговорення у соціальних мережах; виступи окремих осіб; проведення неорганізованих мітингів
12.	Заходи протидії впливу	Жорстка цензура у засобах масової інформації; обмеження Інтернету; використання сил поліції, інших підрозділів проти мирного населення; арешти	
13.	Методи підсилення ІПВ	Ефект первинності; використання медіаторів	Групові акції; суспільні збори

Результат проведення ІПсО залежить від багатьох чинників і, в першу чергу, від якості її планування, точності оцінки характеристик цільової аудиторії, своєчасного моніторингу і корегування ходу здійснення ІПВ та спроможностей сил, що залучаються. Запропонований підхід до формування сценарію ІПсО на визначену цільову аудиторію тимчасово окупованого Криму дозволяє забезпечити високу якість здійснення ІПВ і створити умови для звільнення території від російських загарбників.

Список використаних джерел:

1. Інформаційно-психологічні операції: планування, протидія, технології : монографія / Пєвцов Г.В. , Залкін С.В., Сідченко С. О., Хударковський К. І. Харків. : ДІСА ПЛЮС. 2020. 252 с.
2. Пєвцов Г. В., Залкін С. В., Сідченко С. О., Хударковський К. І. Методичний підхід до формування сценарію проведення інформаційно-психологічного впливу на осіб, що приймають рішення. Системи обробки інформації. 2019. Вип. 1(156). С. 74–81. https://doi.org/10.30748/soi.2019.156.10.
3. Пєвцов Г. В., Залкін С. В., Сідченко С. О., Хударковський К. І. Особливості формування сценарію проведення інформаційно-психологічного впливу в ході реалізації стратегічних комунікацій. Наука і техніка Повітряних Сил. 2019. Вип. 3(36). С. 40–46. https://doi.org/10.30748/nitps.2019.36.05.

Олександр ТОМАШЕВСЬКИЙ
НУОУ
ORCID: 0000-0001-8145-3092
E-mail: tomashevskiyalexandr@gmail.com

АНІЛІЗ ОПЕРАЦІЙНОГО СЕРЕДОВИЩА В ІНТЕРЕСАХ ІНФОРМАЦІЙНОЇ ОПЕРАЦІЇ ЗБРОЙНИХ СИЛ УКРАЇНИ

Основною метою комплексний аналіз операційного середовища в інтересах інформаційної операції Збройних Сил України є аналіз зв’язків – виявлення та візуалізація зв’язків між особами, організаціями та іншими акторами для кращого розуміння ситуації. Аналіз зв’язків вимагає ретельного збору даних, виділення значних ресурсів (часових і людських) для його проведення і має три основні цілі [1, 2]:

знайти відповідність інтересів між акторами;

знайти аномалії, виявивши порушені зв’язки;

знайти нові (приховані) моделі інтересів (наприклад, у соціальних мережах).

Аналіз зв’язків проводиться за етапами, описаними нижче.

1 етап – створення списку акторів (окремих осіб, суспільних груп, організацій тощо) та внесення їх до матриці зв’язків.

2 етап – внесення до таблиці підтверджених фактів зв’язків між акторами.

3 етап – підрахунок зв’язків між акторами.

4 етап – побудова початкової діаграми впливу. На цьому етапі потрібно починати з тих акторів, які мають найбільше зв’язків. Спочатку слід виявити міжособистісні зв’язки, потім окреслити (виокремити в квадрати) територіальні

зв’язки (наприклад, у межах громади), а потім – організаційні (наприклад, професійні зв’язки).

5 етап – розробка символів для позначення різних видів зв’язків акторів.

6 етап – визначення (створення) схеми ієрархії зв’язків.

7 етап – створення карти інформаційного поля. На цьому етапі виявляються ключові актори, які є основними зв’язковими між тими, хто приймає рішення, та виконавцями. Часом їх легко встановити (якщо аналізувати діяльність певної організації або об’єднання), а іноді це потребує комплексних зусиль різних структурних підрозділів штабу, обробки даних від різних джерел [3].

8 етап – ідентифікація взаємовідносин та інтересів. На цьому етапі важливо визначити акторів, рівновіддалених від решти (акторів, організацій, груп, спільнот), які можуть бути визначені як незаангажовані.

9 етап – визначення “потенційного знання”. Здійснення аналізу зв’язків дозволяє знайти можливі прогалини в системі взаємовідносин ключових лідерів та інших акторів, відповідно – спланувати заходи щодо перевірки цього прогнозу [4].

Сучасні кризи характеризуються складною взаємозалежністю та поєднанням історичних, політичних, військових, соціальних, культурних та економічних проблем. Тому рішення, необхідні для вирішення криз, також мають складний і комплексний характер. На цей час для аналізу комплексної стратегічної та оперативної обстановки НАТО використовує конструкцію PMESII, що має шість основних доменів [1].

P – Політичний. Будь-яке об’єднання цивільних акторів, організацій та установ, як офіційних, так і неформальних, що мають владу / керують в певних географічних межах або організацій і застосовують різні форми, інструменти політичної влади та впливу. Сюди включаються політична система, партії та основні актори, а також культурні, історичні, демографічні, релігійні фактори, що формують ідентичність суспільства.

M – Військовий. Збройні сили та допоміжна інфраструктура, що створені, підготовлені, розвиваються і підтримуються для досягнення та захисту національних або організаційних цілей безпеки. Сюди включаються також аспекти внутрішньої безпеки країни.

E – Економічний. Складається із загального обсягу виробництва, розподілу та споживання всіх товарів та послуг для країни чи організації. Сюди включається не тільки економічний розвиток країни, але і розподіл багатства.

S – Соціальний. Взаємозалежна мережа соціальних інститутів, які підтримують, надають різні можливості, культурно об’єднує окремих осіб та забезпечують участь в досягненні особистих та життєвих цілей в межах спадкових та неспадкових груп як у стабільному, так і в нестабільному середовищі. Домен охоплює такі соціальні аспекти, як релігія, структура суспільства, правова та судова система, поліція, гуманітарна діяльність.

І – Інфраструктура. Основні об’єкти, послуги та обладнання, необхідні для функціонування громади, організації чи суспільства. Включає логістичну, комунікаційну та транспортну інфраструктуру, школи, лікарні, розподіл води та електроенергії, каналізацію, зрошення, географічне положення тощо.

І – Інформація. Вся інфраструктура, організація, персонал та компоненти, які збирають, обробляють, зберігають, передають, відображають, поширюють та використовують інформацію. Охоплює інформацію та комунікаційні медіа.

Таким чином, комплексний аналіз операційного середовища є основою для планування інформаційної операції та відповідно до умов обстановки повинен постійною переоцінюватись і уточнюватись, оскільки виявлення критичних вразливостей у противника може змінюватися протягом усієї інформаційної операції через інтерактивний характер війни та зміну цілей будь-якого учасника бойових дій.

Список використаних джерел

1. AJP-5 Allied Joint Doctrine for the Planning of Operations, Edition A Version 2, 24 May 2019, Доктрина НАТО з оперативного планування.

2. ATP 3-13.1 The Conduct of Information Operations, публікація СВ США щодо ведення інформаційних операцій. October 2018.

3. Psychological Operations Process Tactics, Technics and Procedures (FM 3-05.301), 30 August 2017. Настанова з психологічних операцій СВ США.

4. Leigh Armistead “Information Operations. Warfare and the Hard Reality of Soft Power”, Potomac Books, INC, Washington D.C.

Сергій МАРЧЕНКОВ, к.пед.н.
ORCID: 0000-0003-4597-3618
E-mail: marchenkov1978@ukr.net
Сергій ШИШКІН
ЖВІ ім. С. П. Корольова
ORCID: 0009-0001-0354-9504
E-mail: ihruk44@gmail.com

ПРОБЛЕМИ ПРОВЕДЕННЯ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ ТА ПІДВИЩЕННЯ ЇХ ЕФЕКТИВНОСТІ

З початком повномасштабного вторгнення російської федерації проблематика досягнення ефективності при здійсненні психологічних операцій стала особливо актуальною [1]. Причиною часткових труднощів цьому є цензура та закритість

інформаційного простору рф, узурпація довіри населення пропагандистськими ресурсами, підконтрольними державній владі та бізнес-еліті.

Хоч і де-факто агресія країни-терориста проти України триває з 2014 року, введення наративів проти всього українського в російських ЗМІ триває починаючи з 1991 року, адже проведення психологічних операцій були зафіксовані ще в ті часи [2]. Вони були присутні у більшості ЗМІ, та навіть у розважальному контенті. Такий тривалий та активний психологічний вплив на населення сформував у цільової аудиторії хибне сприйняття реальності та неправильні цінності щодо оцінки ситуації, яка відбувається у наш час.

Крім того, проводиться політика масової цензури, методом якої є вже не перший рік здійснення моніторингу спецслужбами інформаційних джерел, блокування ресурсів та видалення будь-якої невигідної інформації, яка закликає до мітингів, дискредитує провладні структури рф, розповідає історичну правду, викриває страшенну бідність звичайного населення та корупцію верхівки тощо (на підставі Федерального закону № 97- ФЗ від 05.05.2014 “Про внесення змін до Федерального закону “Про інформацію, інформаційні технології і про захист інформації” [6] та на підставі Федерального закону №139-ФЗ від 28.07.2012 “Про внесення змін до Федерального закону “Про захист дітей від інформації, що завдає шкоди їх здоров'ю та розвитку” і окремих законодавчих актів Російської Федерації” [7], Федерального закону №398-ФЗ від 28.12.2013 “Про внесення змін до Федерального закону “Про інформацію, інформаційні технології і про захист інформації” [8] та на підставі “законів пакету Ярової” [5; 9; 10], Федеральний закон від 4 березня 2022 року № 32-ФЗ “Про внесення змін до Кримінального кодексу Російської Федерації та статті 31 та 151 Кримінально-процесуального кодексу Російської Федерації” (у ЗМІ відомий як “ Закон про фейки” або “Закон про військову цензуру”)).

Також слід зазначити, що будь-які спроби виразити свою думку в інформаційному просторі карається переслідуванням правоохоронними органами та масовими залякуваннями. Дані фактори негативно впливають на якісне проведення психологічних заходів, та досягнення бажаних результатів підрозділами ЗСУ.

Зважаючи на таку ситуацію, успіх українських інформаційних військ у боротьбі за можливість ґрунтовно здійснювати психологічний вплив на російські маси залежить від виконання даних кроків:

правильний аналіз та підбір ЦА для проведення заходів ПсО;

здійснення довготривалого психологічного впливу з використанням методу “40 на 60” [3];

використання вразливостей ЦА для досягнень своїх цілей;

застосування усіх наявних інформаційних платформ для проведення психологічних заходів.

Слід зазначити, що важливо активізувати створення та розвиток власних каналів доставки матеріалів психологічного впливу на російські маси, які будуть повністю відповідати в інформаційному плані запитам середньостатистичних громадян Російської Федерації та ні чим не відрізнятися від рупорів влади рф на початку їх існування. Також варто вести інформаційні ресурси доволі обережно: уникати використання провокаційних закликів, висловлювань, які не відповідають порядку денному звичайних росіян, аби не привертати уваги до контенту та уникнути блокування російськими органами. Такі дії дозволять через певний час досягти необхідної аудиторії, що дасть можливість втілювати метод "40 на 60", який буде непомітним для звичайних мас, які вважають ці ресурси авторитетними та перевіреними.

Отже, на даний момент перед Україною в інформаційному просторі стоїть задача, досягнення якої прискорить перемогу наших Збройних сил на полі бою, а саме – збільшення ефективності у здійсненні психологічних операцій. Виконання цього завдання вимагає від підрозділів ПсО розумної ініціативи, злагодженої роботи та відточення механізмів доставки матеріалів ПсВ.

Список використаних джерел:

1. Твердохліб Ю.М. Інформаційно-психологічні Операції у російсько-українській гібридній війні // *Дисертація.* 2019. С. 5.
2. Сьогодні Україна не програє інформаційну війну Росії, а успішно протистоїть усім інформзагрозам // АрміяInform. 2021, лист. 21. URL: https://armyinform.com.ua/2021/11/02/sogodni-ukrayina-ne-prograye-informaczijnu-vijnu-rosiyi-a-uspishno-protystoyit-usim-informzagrozam/ (дата звернення 24.09.2023).
3. Метод "гнилой селедки" // детектор медіа. 2015, серп. 11. URL: https://detector.media/withoutsection/article/110011/2015-08-11-metod-gnyloy-seledky/ (дата звернення 24.09.2023).
4. Законы о "фейковых новостях" действующие в России URL: https://cpj.org/wp-content/uploads/2022/12/TRF_CPJ-Russia-Know-Your-Rights-guide_RU.pdf (дата звернення 24.09.2023).
5. Маркова В. В Москве может пройти митинг против "пакета Яровой" // Московский комсомолець. 2016, июл. 11. URL: http://www.mk.ru/moscow/2016/07/11/v-moskve-mozhet-proyti-miting-protivpaketa-yarovoy.html (дата звернення: 24.09.2023).
6. Федеральный закон от 5 мая 2014 г. N 97-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-

телекоммуникационных сетей” // Законодательство Российской Федерации. URL: https://rg.ru/2014/05/07/informtech-dok.html (дата звернення: 24.09.2023).

7. Федеральный закон от 28 июля 2012 г. N 139-ФЗ “О внесении изменений в Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию” и отдельные законодательные акты Российской Федерации” // Законодательство Российской Федерации. URL:https://rg.ru/2012/07/30/zakon-dok.html (дата звернення: 24.09.2023).

8. Федеральный закон от 28 декабря 2013 г. N 398-ФЗ “О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” // Законодательство Российской Федерации. URL: https://rg.ru/2013/12/30/extrem-site-dok.html (дата звернення: 24.09.2023).

9. Федеральный закон от 6 июля 2016 г. N 374-ФЗ “О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности” // Законодательство Российской Федерации. URL: https://rg.ru/2016/07/08/antiterror-dok.html (дата звернення: 24.09.2023).

10. Федеральный закон от 6 июля 2016 г. N 375-ФЗ “О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения обществе” // Законодательство Российской Федерации. URL: https://rg.ru/2016/07/11/uk375-dok.html (дата звернення: 24.09.2023).

Сергій ШАЙХЕТ к.н.держ.упр.,
НУОУ
ORCID: 0000-0003-4814-775X
E-mail: s.shaixet@i.ua

АНАЛІЗ ПІДГОТОВКИ І ВЕДЕННЯ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ ЗА СТАНДАРТАМИ НАТО

Аналіз підготовки і ведення психологічних операцій на сьогодні викладений з позиції оцінювання інфраструктури операційного району. В операційному районі в інтересах психологічних операцій може бути застосоване до використання радіо, ТБ станції, типографії. Такий причинно-наслідкового аналіз є концептуальними рамками і проводиться для розуміння поведінки ЦА в контексті їх фізичного та соціального оточення.

Аналіз джерел [1-3] показав, що у ході підготовки психологічної операції головним завданням є проведення різного роду досліджень в інтересах планування

психологічних акцій, які проводяться у взаємодії з військовими частинами ПсО (за напрямами секторів (зон, районів) відповідальності) та структурами розвідки.

Метою тез є аналізі підготовки і ведення психологічних операцій відповідно до стандартів НАТО.

Планування психологічної операції має зосереджуватися на описі та оцінці інформаційного простору в системному контексті, включаючи (як мінімум) відповідних акторів, конкретні інформаційні системи та медіа (ЗМІ). Такий опис та оцінку не можна проводити ізольовано тільки персоналом ПсО, має здійснюватися координація та обмін інформацією з іншими функціональними підрозділами штабу без дублювання аналітичної діяльності інших. Отриманий продукт слід розглядати як підсумок колективного аналізу обстановки [4].

Актори включають такі категорії:

окремі особи (наприклад: особи, які приймають рішення, та лідери; лідери думок та формувачі думок; журналісти, редактори та видавці ЗМІ);

групи (населення в цілому або частково, наприклад, за регіонами, етнічною належністю, релігією, активністю або групами вищезазначених осіб);

організації (урядові установи та організації; міжнародні організації, неурядові організації, регіональні та міжнародні підприємства тощо).

Актори мають бути описані з наданням відповідних характеристик, наприклад:

особистість (включає такі фактори: психологічні профілі / риси та особиста історія; культура, мотиви, інтереси, цінності, переконання, ставлення та позиції; ставлення до ризику, чутливість);

роль у суспільстві – офіційна та неофіційна;

сприйняття, образи та думки (Як актори бачать себе та інших акторів? Як актори хочуть їх бачити? Наскільки актори довіряють міжнародній спільноті, коаліції, коаліційним партнерам, іншим суб'єктам?);

інформаційні потоки та процеси формування думок, основні джерела інформації та довіра до них;

наміри та спроможності з проведення інформаційної діяльності / захисту інформаційного середовища від діяльності противника;

співвідношення сил, включаючи військовий, економічний, соціокультурний та релігійний аспекти. Зокрема, контроль над ЗМІ, комунікаційними / інформаційними процесами, пов'язаними засобами та інфраструктурою;

безпекова ситуація, її стабільність, надійність та стійкість;

прихильники та послідовники та їхні рівні прожиткового мінімуму; мережі підтримки; стосунки з іншими суб'єктами з питань політики, безпеки, економіки тощо;

можливі політичні, стратегічні, оперативні й тактичні коротко-, середньо- та довгострокові цілі – їхні ієрархічні схеми та визначення пріоритетності цілей

(Чого хочуть досягти учасники? Як вони діятимуть в інформаційному середовищі?);

взаємозв'язки та взаємозалежності акторів – зовнішні та внутрішні;

досяжність, характеристика психологічних, технічних, фізичних можливостей актора отримувати повідомлення у будь-якому форматі (наприклад, письменність, наявність електронних пристроїв зв'язку, використання / поширення соціальних медіа); наявність зовнішнього контролю (цензури);

сприйнятливість, характеристика того, що привертає увагу акторів, незалежно від можливих наслідків, які виникають у разі споживання інформації; "сфери інтересів" для акторів (наприклад, статті з газет, які вони читали, або радіопрограми, які вони слухали); вони часто пов'язані з установками та цінностями;

вразливість, характеристика факторів, що безпосередньо впливають на раціональне мислення та емоції акторів і можуть бути використані для створення потрібних ефектів; оцінка ґрунтується на результатах соціальних досліджень і стосується тривог, страхів та потреб людей, а не їх ставлення.

Інформаційні системи включають:

обладнання зв'язку та інформаційних систем (методи та процедури і, якщо необхідно, персонал, організований для виконання функцій обробки та передачі інформації);

системи управління (обладнання, методи та процедури, включаючи інструменти планування та прийняття рішень, персонал, який дає можливість командирам та їх штабам здійснювати управління;

характеристики та компоненти систем зв'язку, ІТС та систем управління, у тому числі:

персонал (включаючи акторів у вищезгаданому сенсі);

організація управління (з точки зору процесів прийняття рішень, організації та моделей комунікації, потоків інформації, включаючи такі аспекти, як цензура та свобода слова;

технічне обладнання, методи, платформи та організаційні підходи, що використовуються, створюються та затребувані для отримання, оброблення та передачі інформації, включаючи їх функціональність, детальні функції, ємність та рівень взаємодії, надійність, надмірність тощо;

інфраструктура (державна та приватна), включаючи комерційні споруди, установки, пов'язані з телекомунікаційними компаніями та мережами, поштовими та кур'єрськими службами, засобами поширення радіомовлення чи ЗМІ, такими як стаціонарні та мобільні радіостанції, платформи;

забезпечення потреб, таких як енергія, вода, транспорт та обслуговування.

Статус власної інформаційної діяльності. Дослідження має включати огляд наявних власних спроможностей та методик ведення інформаційної діяльності, включаючи їх поточний стан готовності, участь у поточних операціях та

принципові обмеження. Цю частину дослідження мають надавати представники військ (сил), функціональні експерти або офіцери взаємодії (LNO).

Статус інформаційної діяльності противника. Дослідження також повинно містити огляд спроможностей та методів ведення інформаційної діяльності, включаючи їх (передбачувані) наміри та завдання, поточний стан готовності, участь у поточних операціях, принципові обмеження та вразливості. Цю частину дослідження мають надавати представники J2 та військ (сил), функціональні експерти або офіцери взаємодії (LNO).

Статус інформаційної діяльності нейтральних акторів. Дослідження має включати огляд спроможностей та методів ведення інформаційної діяльності, включаючи їх (передбачувані) наміри та завдання, поточний стан готовності, участь у поточних операціях, принципові обмеження та вразливості. Цю частину дослідження повинні надавати представники J2 та військ (сил), функціональні експерти або офіцери взаємодії (LNO).

Можливі ефекти в інформаційному просторі. Дослідження має завершитися переліком можливих наслідків, враховуючи інформаційні заходи, орієнтовані на таке:

збереження та захист свободи діяльності Альянсу в інформаційному просторі у будь-який час;

поведінку, сприйняття та ставлення аудиторій, затверджених Північноатлантичною радою (NAC);

протидію пропаганді противника, а також функціонуванню та спроможностям його систем управління.

Ефекти мають бути сформульовані таким чином, щоб описувати фізичний та / або поведінковий стан частини інформаційного простору, що є результатом дії або декількох дій. Вони характеризуються як бажані або небажані. Також слід враховувати можливі тенденції (події), що можуть виникати з часом без чийогось втручання.

Крім того, протягом фази 1 підрозділ ІО штабу:

інформує командирів і штаби підпорядкованих і підтримуючих військ про можливі завдання із планування ІО;

оцінює початковий обсяг інформації та ресурсів, необхідних для проведення ІО;

визначає місця розташування, стандартні оперативні процедури та порядок роботи інших штабів і структур, які потребують інтеграції та розподілу обов’язків між ними і персоналом ІО;

починає визначати інформацію, необхідну для аналізу місії та розроблення заходів;

визначає вимоги до підтримки планування ІО (зокрема щодо збільшення кількості персоналу, розроблення інформаційної продукції та надання послуг).

Таким чином, аналізі підготовки і ведення психологічних операцій відповідно до стандартів НАТО дозволив визначити основні етапи, якими є:

визначення терміновості;

видання вказівок з організації планування;

розгортання організаційних структур з кризового планування, зокрема формування об'єднаної групи планування;

видання попередніх розпоряджень підпорядкованим військам;

посилення заходів зі збору та аналізу розвідувальної інформації.

Зміст наведених етапі пришвидшить інтеграційні процеси щодо переходу до стандартів НАТО, що дозволять підвищити рівень підготовки та порядок застосування ЗС України.

Список використаних джерел

1. JP 2-01.3 Joint Intelligence Preparationof the Operational Environment, 21 May 2014. Доктрина ЗС США з аналізу оперативної обстановки.

2. JP 5-0 Joint Planning, 01 December 2020. Доктрина ЗС США з об’єднаного планування.

3. NATO Operations Assessment Handbook”, Version 3.0, посібник НАТО. 01 July 2015.

4. AJP-5 Allied Joint Doctrine for the Planning of Operations, Edition A Version 2, 24 May 2019, доктрина НАТО з оперативного планування.

Oleksandr SHCHEBLANIN, Master's degree student
University Passau
ORCID: 0009-0001-0614-6540
E-mail: Oleksandr.shcheblanin@gmail.com

CYBERSECURITY PERSPECTIVES ON THE INTERNET OF MILITARY AND BATTLEFIELD THINGS

Nowadays the topic of the Internet of Things (IoT) plays an extremely significant role, as its devices are used more and more in different spheres of our life. Importance of these devices will continue to grow the next years integrating in the daily life of any sphere. The IoT devices are already an essential part of the buildings, transportation and infrastructure, tourism and sport, crime detection and its prevention [1]. Due to the latest investigations (Jul 27, 2023) conducted by the researcher at Statista Lionel Sujay Vailshery, the number of IoT connected devices worldwide continuously grows, reaching 8.6 billion in 2019 and a potential 29.42 in 2030 [2].

As previously mentioned, IoT is actively used by the public sector. Even more, the military sector around the world also has begun investing in and integrating different kinds of IoT technologies. In 2021, the Department of Defense of the USA invested almost 6 million dollars, and in 2023, 3 million, into conduction of research and development for the Internet of Battlefield Things (IoBT) and Internet of Military Things (IoMT) [3]. This is not surprising, due to utilization of the interconnected network of sensors and actuators, IoBT/IoMT devices are considered to be very helpful for the situational awareness of the battlefield, analyzing and collecting different types of data for the further better decision making, and facilitating intelligent interaction among people, services and networks [4, 5].

However, the developers of the technology were divided from the perspective of the cybersecurity. Despite the provided beneficial advantages of these devices' usage, there is a problem of the greater cyber-attack surface. Potential directions for attacking are network, application, data and storage. Device can be just simply physically acquired due to different circumstances occurred on the battlefield.

For example, when considering the CIA triad for IoBT/IoMT [6]:

1) Confidentiality. The data collected and stored on the "edge" level (the device itself) is usually unencrypted to provide higher processing speed. However, this lack of encryption allows easily access and exfiltrate sensitive data the during attack or just physical acquirement.

2) Integrity. Since the processed data is usually not cryptographically signed on the device itself, it is challenging to be sure about the trustworthiness of the gathered and

provided by IoBT/IoMT data. Attackers can modify and corrupt data according to their own interests.

3) Availability. Device can simply lose the opportunity to send data because of the potential radio frequency jamming attack (which uses the specific signals or noise that can overwhelm the communications system or overpower legitimate signal). This can result a Denial of Service (DoS) of the IoBT/IoMT device [7].

Some of the possible solutions for preventing electromagnetic and physical attack vectors can be [8, 9]:

1) Remote-wiping capable devices.
2) Authentication.
3) Application authorization.
4) Encryption.
5) Private data storage.
6) Network structuring.

The significance and landscape of the usage of IoBT/IoMT continue to groww annually. However, with that increases also a surface of potential attacks which is the big obstacle on the way of technology development. Fortunately, there are multiple of possible techniques and solutions that allow to avoid risks of attacks. This demonstrates the potential for the successful development and effective usage of IoT devices in the military sector.

References:

1. Ulrika H. Westergren, Katrin Jonsson Ott Velsberg, “Internet of Things in the Public Sector Perspectives from Northern Europe”, March 2019, Umeå University, Sweden Department of Informatic.
2. “Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030”, available at: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.
3. “Department of Defense Fiscal Year (FY) 2023 Budget Estimates", available at:https://www.asafm.army.mil/Portals/72/Documents/BudgetMaterial/2023/Base%20Budget/rdte/vol_1-Budget_Activity_1.pdf.
4. Cyrus Mewawalla, Globaldata, “Internet of Military Things”, 2019.
5. John Zhu, Egan McClave, Quan Pham, Sujay Polineni, Sam Reinhart, Ryan Sheatsley, Andrew Toth, “US Army Research Laboratory, A Vision toward an Internet of Battlefield Things (IoBT), available at: Autonomous Classifying Sensor Network”.
6. “The Military Benefits and Risks of the Internet of Things”, 2019, Department of the Army, Office of the Deputy Under Secretary of the Army, Washington.
7. “RADIO FREQUENCY INTERFERENCE BEST PRACTICES GUIDEBOOK”, 2020, Cybersecurity and Infrastructure Security Agency, SAFECOM/National Council of Statewide Interoperability Coordinators.

8. Yurii Shcheblanin, Bohdan Oliinyk, Oleg Kurchenko, Toroshanko Oleksandr and Nataliia Korshun. Research of Authentication Methods in Mobile Applications. CPITS-2023: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine. SEUR-WS.org, vol 3421. pp. 266-271.
8. "The Internet of Military Things", available at: https://cove.army.gov.au/article/internet-military-things.

Olga RYZHCHENKO, Candidate of Philological Sciences, docent
Assistant Professor of the Department of Language Training
National University of Civil Protection of Ukraine
ORCID: 0000-0003-1693-6121
Email: ryzhchenko_olga@nuczu.edu.ua

TRAINING OF CYBER SECURITY SPECIALISTS AND DATA PROTECTION SPECIALISTS AS AN URGENT NECESSITY TODAY

Information is something which let people not only work but live as well as it can influence almost all spheres of our professional and private life. That is why it is necessary to teach people to work with information and know how to understand whether it is true or fake. Unfortunately, we have to deal with load of information and do not always have time and possibility to check it. So we have to rely on professionals who will do it for us to make our life more comfortable and less stressful. It is doubtless that modern people can't exist without information which is given to them in the form of the news which can provoke global changes in peaceful life of not only ordinary people but whole countries and even continents. That is why it is really important to rely on proved information but not fakes.

Nowadays it is goes without saying that the world is changing and we need to follow the changes. And it is also clear that information has become weapon which can hurt and threat. That is why data protection must be considered a very important if not vital demand of modern system of education which must pay special attention to providing education to such specialists. Following such demand National University of Civil Protection of Ukraine has started a new educational program which will provide special educational components to students and cadets.

Universities are supposed to give professional courses like Programming, Web Programming. Data Bases, but on the other hand it is impossible to cope with university curriculum without mastering general components like Ukrainian, the History and Culture of Ukraine, Phycology and English. Such disciplines are very important in the process of education as they help professors bring up decent citizens of the country. Moreover, English which is considered to be the international language of

communication is necessary for cyber security specialist and data protection specialists as they must follow the development of all modern strategies of it.

Luckily, we have enough information about all cons and pros of these professions, all advantages and disadvantages are described on the official sites of American and European universities [1] so it is obvious that we should take over the experience of top universities all over the world to provide such services to our country and our people to help our country develop this way and become equal among other countries in this matter.

References:

1. Moore Michelle. How to become a Data Protection Officer [Career &Salary Guide]. A University of San Diego blog. Retrieved from: https://onlinedegrees.sandiego.edu/data-protection-officer-career-guide/

Богдана КАЛЬВАРОВСЬКА
НУК ім. адмірала Макарова
E-mail: b784070@gmail.com

A WEAPON OF INFORMATION WARFARE: INFORMATION SECURITY AND INFORMATION MANIPULATION

Today, a hybrid war is being waged against Ukraine, an important component of which is information and psychological influence. Sometimes, this type of influence is more successful than the use of military force. Therefore, information security is an important element of the country's overall national security.

Protecting information security is an important task for any state in the modern world, where information plays a key role in various areas, including national defense, economy, politics, social relations and technological development. Implementation of a successful information policy can have a significant impact on the resolution of domestic and foreign policy, as well as military conflicts.

In today's realities, due to the attacks of the russian federation, it is necessary to seek active actions to ensure the national security of Ukraine. Assessment of existing and possible information threats to national security and combating them require an immediate response, given the new challenges caused by the war. The problem of information security is exacerbated by the enemy's ability to manipulate information and introduce its own narratives. Accordingly, this allows them to influence people's minds and create a convenient information space for themselves.

The main task of russian propaganda is to disseminate deliberately false information aimed at influencing public opinion and mass consciousness. For this

purpose, the media are actively used, which, on the one hand, form the necessary public attitude, and on the other hand, lead to a deterioration in the moral and psychological mood of the population, thereby reducing its information stability and ability to resist destructive ideas and attitudes [1].

The fakes spread by russians in Ukraine are aimed at sowing discord and disillusionment, which was especially noticeable during the blackouts. The growing spread of manipulations included claims that Ukrainians were already allegedly “cold, hungry and unwashed” without electricity, water and heating. Another typical pretext for russian manipulations is the language issue. Controversial videos of allegedly russian-speaking Ukrainians complaining about discrimination can be seen on social media [2].

The russian federation spreads shameless disinformation, but it makes sure that these lies are interesting and emotionally affecting, and adapts them to a strategic narrative tailored to fit the prejudices and perceptions of its audiences, combining Ukrainian nationalism with fascism and encouraging anti-American and anti-EU feelings in Europe.

To make this content appealing, russia is willing to fully fabricate stories, using photos and videos to meet the relevant needs. The full range of media, from cinema to news, talk shows, print and social media, is involved in promoting russia's official theses [3].

The current circumstances of the war clearly show that information has become a means of "mass destruction." Therefore, it is necessary to create an effective mechanism that would guarantee national information security and protect human rights without restricting freedoms and democracy.

Список використаних джерел:

1. Денисюк Ж.З. Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики. Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління. Том 32 (71) № 2 2021.

2. Продукують тисячі фейків: як працює російська пропаганда в Україні, рф та в усьому світі. URL: https://barnews.city/articles/284833/yak-pracyue-rosijska-propaganda-v-ukraini-rf-ta-v-usomu-sviti-.

3. Мета російської пропаганди - посіяти зневіру і параною. Як протидіяти. 2016 URL: https://texty.org.ua/articles/70089/Meta_rosijskoji_propagandy__posijaty_zneviru_i-70089/.

Роман АЛІЄВ, к.ю.н. доц.
НУОУ
ORCID: 0000-0002-4309-3652
E-mail: roman-aliev76@ukr.net
Людмила ПАНАСЕВИЧ
НУОУ
ORCID: 0000-0001-5899-5272
E-mail: panasevich.lydmila@ukr.net

ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ У КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ

Одним із основних засобів правового забезпечення національної безпеки є юридична відповідальність. Щоб зрозуміти поняття та значення цього правового інституту в системі правового забезпечення національної безпеки слід звернутись до його природи. Тут виявляється певна особливість – право національної безпеки, як правило не здійснює регулювання відносин з приводу конкретних прав і свобод, людини, а визначає необхідні та достатні умови для існування таких правовідносин, де реалізуються права, свободи, законні інтереси, виконуються відповідні юридичні обов'язки.

У своїх дослідженнях, однією з функцій права національної безпеки доктор юридичних наук П.П. Богуцький розглядає – регулятивну функцію, яка проявляється насамперед у переведенні фактичного змісту соціальних комунікацій, що існують у соціумі та є необхідними для забезпечення національної безпеки, у юридичний зміст з визначенням прав, обов'язків, дозволів, заборон, встановлення правових статусів [1, с. 28]. Складно з цим не погодитись, адже великого значення у діяльності сил безпеки і сил оборони набуває механізм права, поруч з яким існує інститут юридичної відповідальності, оскільки будь-яка небезпечна ситуація в державі, у тому числі правовий режим воєнного стану долається з допомогою додаткових зусиль, утримується в деяких правових рамках та обмеженнях і на цій основі трансформується в нормативну ситуацію.

В надзвичайних, небезпечних ситуаціях влада переходить від одних структур і суб'єктів до інших, тобто характер управління стає, як правило, більш авторитарним. Потреба в праві зростає. Змінюються зміст регулятивного потенціалу права та процес реалізації права [2, с. 20]. В умовах особливих режимів великого значення набуває правове забезпечення національної безпеки та оборони України основу якого становлять: Конституція України, закони України "Про оборону України" від 6 грудня 1991 року № 1932-XII, "Про національну безпеку України" 21 червня 2018 року № 2469-VIII, інші закони і нормативно-правові акти.

Саме в контексті національної безпеки та оборони України пропонується досліджувати юридичну відповідальність як складову соціальних комунікацій, що здійснює необхідний правовий вплив, регулюючи поведінкові акти певних суб'єктів сектору безпеки і оборони, спрямовуючи їх для досягнення мети, якою є національна (воєнна) безпека.

Через повномасштабне вторгнення росії на територію України тема злочинів проти основ національної безпеки та юридичної відповідальності за їх вчинення набула особливої актуальності. Так, від початку російсько-української війни внесено до Єдиного реєстру досудових розслідувань – 1677 кримінальних проваджень щодо злочинів проти національної безпеки, з них – 1315 проваджень зареєстровані за фактами державної зради, 286 – за фактами колабораційної діяльності та 23 – за статтею про пособництво державі-агресору.

Додатковим аргументом необхідності дослідження юридичної відповідальності у контексті національної безпеки та оборони України є вироблення та становлення ефективних принципів її застосування, а саме:

а) на міжнародному рівні: взаємозв'язок національної і міжнародної безпеки; дотримання Статуту ООН; норм міжнародного права й прав людини; добросовісне виконання міжнародних обов'язків; невтручання у внутрішні справи інших держав; дотримання недоторканості державних кордонів; повага суверенної рівності усіх держав; гнучке реагування на надзвичайні ситуації та їх усунення невійськовими засобами; участь у міжнародних організаціях європейської і глобальної безпеки; вступ до світових організацій з підтримання міжнародної безпеки;

б) на національному, регіональному й місцевому рівнях: законність; дотримання балансу життєво важливих інтересів людини, суспільства й держави, їх взаємна відповідальність щодо забезпечення й гарантування національної безпеки; своєчасність і адекватність заходів щодо забезпечення національної безпеки існуючим загрозам і небезпекам; конструктивне розмежування повноважень та функцій органів безпеки; дотримання пріоритету невоєнних засобів вирішення конфліктів; інтеграція з міжнародними системами безпеки.

Останнім часом в Україні набули перспективного розвитку дослідження проблем юридичної відповідальності за правопорушення, які безпосередньо посягають на інформаційні відносини, що виражаються в порушенні інформаційних прав та невиконанні або неналежному виконанні обов'язків, пов'язаних з інформацією (кіберзлочини) [3, с. 209-232], запобіганні новим проявам злочинності відносно об'єктів критичних інфраструктур, що стосується сфери водопостачання, енергетики, транспорту і палива захист яких становить основу національної безпеки країни [4, с. 139-152].

Отже, система юридичної відповідальності у контексті національної безпеки та оборони України повинна виконувати насамперед три основні функції:

1. Регулювати взаємовідносини між суб‘єктами національної безпеки, визначати їх права, обов‘язки та юридичну відповідальність.

2. Забезпечувати дії суб‘єктів національної безпеки на всіх рівнях, а саме – людини, суспільства, держави.

3. Встановлювати правовий порядок застосування різних сил і засобів забезпечення національної безпеки.

Підсумовуючи слід зазначити, що нормативну-правову базу юридичної відповідальності у контексті національної безпеки та оборони України доцільно створювати і розглядати з урахуванням її ієрархічності.

На вищому рівні концептуальні положення юридичної відповідальності у сфері національної безпеки закріплюються Конституцією України, Стратегією національної безпеки України, Стратегією воєнної безпеки України та відповідним законом України. Ці документи враховують основні положення міжнародних договорів і угод, які узгоджені Україною і стосуються її національної безпеки.

На другому рівні є конституційні закони, наприклад, Закон України “Про Кабінет Міністрів України”, де визначаються важливі положення щодо забезпечення національної безпеки та обороноздатності. Далі – закони України “Про оборону України”, “Про Збройні Сили України”, “Про державний кордон України”, “Про Державну прикордонну службу України”, “Про Національну поліцію”, “Про Службу безпеки України”, “Про Національну гвардію України” та інші, в яких закріплені основні норми відповідальності за порушення законодавства про національну безпеку України.

В ієрархії нормативної бази національної безпеки особливе місце посідають укази та розпорядження Президента України, а також акти (постанови, декрети) Кабінету Міністрів України. Вони є підзаконними й видаються з метою конкретизації та підвищення якості вирішення питань національної безпеки.

Крім того, сили безпеки і оборони України у межах своєї компетенції та відповідальності на основі чинного законодавства про національну безпеку, оборону, а також згідно з рішеннями Президента України, Кабінету Міністрів розробляють відомчі накази, інструкції, положення, які спрямовані на реалізацію програм захисту життєво важливих інтересів людини, суспільства, держави.

Список використаних джерел:

1. Богуцький П.П. Право національної безпеки та військове право: сучасні виклики : навчальний посібник / П.П. Богуцький ; Державна наукова установа “Інститут інформації, безпеки і права НАПрН України”. – Київ; Одеса : Фенікс, 2023. – 252 с.

2. Шамрай В.О. Державне управління військовими формуваннями воєнної організації: стан та тенденції розвитку в сучасній Україні : автореф. дис. … д-ра наук з держ. управління : 25.00.03. Київ, 1999. 38 с.

3. Бєляков К.І., Тихомиров О.О. Інформаційний делікт. Деліктологія : монографія / за ред. С.В. Пєткова, І.М. Копотуна. Куновіце: Академія ГУСПОЛ : 2020, Т.1. – С. 209-232.

4. Юзікова Н.С. Захист критичних інфраструктур від злочинних посягань – основа національної безпеки країни. Деліктологія : монографія / за ред. С.В. Пєткова, І.М. Копотуна. Куновіце: Академія ГУСПОЛ : 2021, Т.3. – С. 138-152.

Олександр БОРИСОВ
НУОУ
ORCID: 0009-0006-7313-0350
E-mail: borysov141@gmail.com

ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В ПІСЛЯВОЄННИЙ ПЕРІОД

Збройна агресія російської федерації проти України, що триває вже десятий рік, супроводжується регулярним створенням державою-агресором інформаційних загроз для України. Перехід збройного конфлікту до повномасштабної фази не лише підсилив протистояння сторін в інформаційному середовищі, а й створив нові актуальні проблеми, пов’язані з правовим регулюванням у сфері інформаційної безпеки.

Важливо розуміти, що правове забезпечення інформаційної безпеки України в умовах повномасштабної збройної агресії російської федерації і в умовах миру або “тліючого” чи “замороженого” збройного конфлікту може бути досить різним. Перш за все – за ступенем обмеження прав і свобод людини, до якого вдається держава в безпекових інтересах. Відповідно, перехід від воєнних механізмів правового регулювання до тих, які є характерними для соціальної, демократичної, правової держави у мирний час є досить складним організаційно-правовим процесом.

Динаміка зміни лінії бойового зіткнення, політичні заяви учасників збройного конфлікту, а також стійка тенденція до нарощування воєнних спроможностей обома сторонами зіткнення чітко вказують на те, що бойові дії між російською федерацією і Україною на разі далекі від завершення. Разом з тим, важливо розуміти, що правове регулювання найчастіше є найбільш ефективним тоді, коли регулятору суспільних відносин вдається спрогнозувати їх розвиток і можливі трансформації та підготувати відповідну правову базу або хоча б її основу заздалегідь. Окрім цього, реформування законодавства є досить тривалим процесом як в силу складності проблем, що потребують правового розв’язання, так і в силу складності формальних процедур,

відповідно до яких таке реформування здійснюється. Таким чином, попри те, що момент припинення збройного протистояння між російською федерацією та Україною невизначено віддалений у часі, проблема адаптації правових механізмів забезпечення інформаційної безпеки України до післявоєнних умов набуває актуальності вже зараз.

Серед найбільш істотних проблем правового забезпечення інформаційної безпеки України в післявоєнний період можна назвати такі:

1) незалежно від результатів і способу завершення поточної фази російсько-українського конфлікту російська федерація залишатиметься джерелом істотних інформаційних загроз для України;

2) організація правового забезпечення інформаційної безпеки в післявоєнний період потребуватиме надзвичайно виваженого підходу з тим, щоб безпекові заходи не завдавали надмірної, невиправданої шкоди правам та інтересам людини в інформаційній сфері;

3) населення звільнених територій України, яке тривалий час перебувало під окупацією російських військ і зазнало шкідливого інформаційно-психологічного впливу, потребуватиме спеціальних заходів з реінтеграції в український інформаційний простір, в суспільні відносини;

4) значна кількість учасників бойових дій, яка залишить лави сил оборони, так само потребуватиме реінтеграції в суспільство. Особовий склад сил оборони, який залишиться на службі, потребуватиме щонайменше заходів з психологічного відновлення;

5) існує ризик втрати частини зовнішньої економічної підтримки після припинення або згасання активних бойових дій на території України.

Не всі з перерахованих проблем мають суто інформаційний характер, але залишення будь-якої з них без належної уваги та врегулювання може призвести до істотної соціально-політичної дестабілізації суспільства. Водночас, така дестабілізація є безпосередньою загрозою вже для інформаційної безпеки України.

Разом з тим, за поточних обставин існує і ряд факторів, що можуть позитивно вплинути на вирішення Україною означених вище проблем, зокрема:

1) Україна, як на рівні суб’єктів владних повноважень (профільні міністерства, відомства, служби), так і на рівні інституцій громадянського суспільства (громадські організації, благодійні фонди) вже має досвід реінтеграції населення звільнених територій. Також Україна має і досвід реінтеграції до суспільства учасників бойових дій. Відповідно, якісне опрацювання зазначеного досвіду може сприяти ефективному реформуванню системи правового забезпечення інформаційної безпеки в умовах післявоєнного часу;

2) протягом протистояння збройній агресії російської федерації від самого її початку (з 2014 року) Україна витримує послідовну, правомірну лінію поведінки, що ґрунтується на нормах міжнародного та національного права. Російська федерація ж здійснює воєнну агресію проти України протиправно, безпідставно, із порушенням як норм міжнародного права, так і фундаментальних загальнолюдських засад

співіснування. У силу цього Україна має підтримку більшості цивілізованих, демократичних держав світу, що в контексті післявоєнного правового реформування дозволяє розраховувати на організаційно-дорадчу допомогу держав-партнерів. При цьому деякі з держав-партнерів вже стикалися із проблемами, подібними до вищезгаданих (реінтеграція звільнених/захоплених територій; подолання післявоєнних економічних депресій; реінтеграція учасників бойових дій до суспільства тощо) і мають значно глибший досвід відповідного правового регулювання;

3) українське суспільство як на стадії збройного конфлікту з російською федерацією в межах Донецької та Луганської областей (2014-2022), так і на етапі повномасштабного вторгнення (2022-наші дні) продемонструвало високу стійкість до викликів і загроз, створених державою-агресором. Відповідно, стійкість українського народу, його здатність до самоорганізації та відданість загальнолюдським гуманним цінностям дозволяють державі розраховувати на активне включення громадянського суспільства до роботи з напрацювання правових засад, підходів, механізмів забезпечення інформаційної безпеки України, а також до їх практичної реалізації.

Таким чином, Україна може розраховувати на потужний внутрішній і міжнародний інтелектуальний потенціал, що дозволить належним чином організувати необхідну трансформацію правових механізмів забезпечення інформаційної безпеки України в післявоєнний період.

Висновки:

1. Для забезпечення своєчасного реформування правових механізмів забезпечення інформаційної безпеки України в умовах післявоєнного часу необхідно завчасно здійснити прогнозування можливих сценаріїв припинення бойових дій та розпочати в суспільстві обговорення бачення майбутнього України.
2. Засади адаптації правового регулювання у сфері інформаційної безпеки до післявоєнних умов доцільно почати напрацьовувати заздалегідь, вивільняючи час на їх узгодження із позицією громадянського суспільства, на консультації із міжнародними партнерами тощо.
3. Своєчасне і виважене використання переваг і можливостей, наявних у України, може забезпечити ефективну трансформацію правових механізмів забезпечення інформаційної безпеки України відповідно до потреб післявоєнного періоду.

Список використаних джерел

1. Конституція України. Режим доступу: https://zakon.rada.gov.ua/laws/show/254/80#Text.
2. Стратегія інформаційної безпеки України. Режим доступу: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

Максим ГОВДА
ЖВІ ім. С.П. Корольова
ORCID: 0009-0005-7185-5887
E-mail: maksgovda@gmail.com

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ІНФОРМАЦІНА ЗБРОЯ В ХОДІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Соціальну інженерію, як зброю почали використовувати вже давно для особистого збагачення, шантажу, розваги, залякування тощо. Соціальна інженерія не вимагає знання програмування чи інших технічних знань, тобто агресором може бути навіть самий неосвічений злодій. Існують різні методи та форми соціальної інженерії, найважливіші хочу відмітити: фішинг, вішинг та смішинг, видавання себе за іншу особу та звичайно кібершахрайство. Розберемо кожну з них.

Фішинг – це форма кібератаки, під час якої зловмисник намагається підірвати довіру жертви з метою отримання конфіденційної інформації. Для досягнення цієї мети атакуючі можуть використовувати методи, що включають створення відчуття терміновості або вживання загрозливих заходів. Важливо відзначити, що фішингові кампанії можуть бути спрямовані на велику кількість випадкових користувачів або конкретну особу чи групу.

Вішинг та смішинг – це соціально-інженерні методи, аналогічні фішингу, але проводяться без використання електронної пошти. Зокрема, вішинг виконується за допомогою обманливих телефонних дзвінків, а смішинг включає в себе відправку текстових SMS-повідомлень, що містять шкідливі посилання або контент.

Видавання себе за іншу особу – є метод соціальної інженерії, при якому кіберзлочинці вдаються, ніби вони є певною особою, щоб ввести в оману потенційних жертв. Звичайним прикладом є ситуація, коли зловмисник видає себе за генерального директора конкретної компанії, укладає та затверджує шахрайські угоди в той час, коли справжній генеральний директор перебуває у відпустці.

Кібершахрайство – це схеми зловмисників, у яких часто використовують один або навіть декілька методів соціальної інженерії, описаних у цьому розділі. Кожна з них форм або методів наносила збитків не тільки особам, а й цілим компаніям або структурам. Аналізуючи проблематику в захищеності в інформаційному просторі можна прийти до висновку, що не всі ще вміють захищати себе від подібних атак або завчасно їх виявляти.

Метою доповіді є дослідження методів та способів виявлення ознак роботи соціальної інженерії та вміння їй протидіяти.

Враховуючи умови сьогодення в нашій країні, можна впевнено стверджувати, що під дію соціальної інженерії попадає більшість українців. Об’єкти впливу можна поділити на безпосередніх об’єктів комбінованого впливу (військові, члени

їх сімей біженці, населення на окупованих територіях, волонтери тощо) та усіх інших об’єктів класичного впливу. Тому опанування шляхів виявлення та протидії роботи соціальної інженерії повинно бути на високому рівні.

Ознаки за якими можна виявити соціальну інженерію:

1. погана граматика. Зловмисник не приділяють увагу деталям та надсилають повідомлення з помилками, пропущеними словами та поганою граматикою, часто з російським акцентом або погано переведеними словами;

2. незвичний профіль або адреса відправника. Більшість зловмисників не витрачають час на створення правдоподібного імені або домена відправника;

3. терміновість відправника. Злочинці часто намагаються залякати жертв за допомогою фраз, які викликають тривогу, наприклад “терміново надішліть нам свої дані, або ваша посилка буде скасована” або “якщо ви не оновите свій профіль зараз, ми його видалимо”;

4. запит конфіденційних даних;

5. розіграші подарунків.

Розібравшись з потенційними загрозами можна виділити ряд рекомендацій щоб не потрапити під вплив соціальної інженерії:

1. бережіть особисту інформацію: Утримуйте конфіденційні дані, такі як паролі, номери кредитних карт, коди доступу, від незнайомих осіб. Завжди пам'ятайте, що зловмисники можуть намагатися отримати цю інформацію шляхом підкупу або обману;

2. зберігайте пильність при спілкуванні: Будьте особливо обережні при спілкуванні з невідомими людьми, особливо в онлайн-середовищі. Багато атак соціальної інженерії відбуваються через соціальні мережі, електронну пошту та телефонні дзвінки;

3. перевіряйте ідентифікацію: Перед тим як надавати інформацію або здійснювати фінансові операції, завжди перевіряйте, хто саме запитує ці дані. Запитуйте про ідентифікацію іншої сторони, особливо у важливих ситуаціях;

4. уникають посилань та вкладень від невідомих: Не клікайте на сумнівні посилання в електронних повідомленнях і не відкривайте вкладення, якщо вони приходять від невідомих джерел. Це може бути способом поширення вірусів і шкідливих програм;

5 поширюйте обізнаність серед себе та своїх близьких: Розповідайте ці поради своїм родичам і друзям, особливо тим, хто може бути вразливим перед атаками соціальної інженерії;

6 .використовуйте надійні паролі та активуйте двофакторну аутентифікацію: Важливо мати складні паролі для своїх облікових записів та, де це можливо, включати двофакторну аутентифікацію для додаткового рівня безпеки;

7. будьте обережні при обробці телефонних дзвінків і повідомлень: Не приймайте поспішливі рішення відразу після отримання телефонних дзвінків або

повідомлень. Завжди можна перевірити ідентифікацію іншої сторони та обміркувати запити;

8. встановіть антивірус та антишпигунське програмне забезпечення: Використовуйте актуальне програмне забезпечення для захисту вашого комп'ютера та мобільних пристроїв від різних видів загроз.

Узагальнюючи вище викладене, в подальших дослідженнях необхідно зосередити увагу на уточненні рекомендацій щодо самозахисту від спроб застосування соціальної інженерії. Також основну увагу слід зосередити на розробці рекомендацій щодо самозахисту населення від поширюваних росією негативних прикладів соціальної інженерії, особливо на тимчасово окупованих територіях.

Список використаних джерел:

1. Рекомендації кібербезпекової організації Cybersecurity and Infrastructure Security AgencyURL:https://www.cloudflare.com/ (дата зверенення:18.09.2023).

2. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування: монографія / О.В.Левченко. Житомир : Видавець ПП “Євро-Волинь”, 2021. – 172с.

Роман ГРИБЕНКО
НУОУ
ORCID: 0009-0009-5507-8378
E-mail: r.grubenko@i.ua

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ У ВОЄННІЙ СФЕРІ

Сьогодні, до загроз інформаційній безпеці України у воєнній сфері слід відносити ті загрози, яким ще кілька років тому навіть не приділялася увага, оскільки вони були настільки маловірогідними, що їх плив на воєнну безпеку навіть не брався до уваги. Не в останню чергу це пов’язано з тими змінами, які відбуваються в способах та формах збройної боротьби сучасності та використовуваних при цьому засобах реалізації воєнних загроз. Також на зміну характеру воєнних загроз впливають процеси трансформації, які відбуваються в збройних силах та воєнізованих угрупованнях протиборчих сторін і які, останнім часом, зміщуються у бік високої технологічності озброєнь військ (сил). Тому ефективний захист та ефективна протидія новим викликам та загрозам у воєнній сфері неможливі без оцінювання й прогнозування рівня таких загроз та своєчасності вжиття при цьому усього наявного комплексу політичних, економічних та інших заходів протидії.

Сучасні загрози інформаційній безпеці України у воєнній сфері набувають комплексного характеру. Так, поступово набуває умовного характеру поділ загроз на воєнні та не воєнні, оскільки останні, за певних умов, можуть бути легко трансформовані у воєнні. Скажімо, буквально з десяток років тому кібернетичні загрози не були предметом дослідження військової науки. Але в епоху кібернетичних війн реальними загрозами у воєнній сфері стають кібернетичні загрози. Тому, однією з умов забезпечення ефективного збройного захисту є виявлення джерел воєнної небезпеки і кібернетичних загроз національним інтересам в даній сфері.

Прояв інформаційній безпеці України у воєнній сфері у воєнний час не завжди має тісний зв'язок з початком військових приготувань протиборчою стороною до воєнних дій. Спровокувати виникнення джерел кібернетичних загроз у воєнній сфері можуть найрізноманітніші явища та процеси й не завжди такі, що несуть воєнні ознаки. Наприклад, до таких джерел виникнення кібернетичних загроз воєнній сфері можна віднести: розробку, застосування та нарощування в світі потенціалу кібернетичних озброєнь; протиріччя, що виникають між державами на економічному, соціальному, етнічному, політичному або релігійному підґрунті; наявність і розгортання високотехнологічних армій та високотехнологічного оснащення сектору безпеки та оборони держав у тому числі й нарощування сил та засобів кібернетичних військ (сил); загроза виникнення техногенних катастроф на об'єктах з критичною кібернетичною інфраструктурою, у тому числі і військових, у результаті цілеспрямованих кібернетичних впливів тощо.

До основних ознак існування інформаційній безпеці України у воєнній сфері можна віднести наступні: наявність на регіональному та міжнародному рівні гострих протиріч у різних сферах, розв'язання яких можливе, але не доцільне лише із застосуванням воєнної сили; наявність у однієї з протиборчих сторін зразків кібернетичної зброї, а також відповідних сил і засобів для розв'язання протиріч, що існують безпосередньо з використанням елементів кібернетичного простору; відсутність політичної волі у керівництва держави для створення армії нового зразка, у якій не останню роль відіграватимуть підрозділи з кібернетичної безпеки, а також на застосування такої армії й визначених підрозділів за призначенням у разі загрози виникнення та подальшої ескалації збройного конфлікту; сприятливі геополітичні умови й реальна (або прогнозована) військово-політична обстановка для реалізації кібернетичних впливів.

Таким чином, перелік існуючих та прогнозованих загроз інформаційній безпеці України у воєнній сфері на сьогодні ще не сформований у повній мірі. Інколи, помилково, він збігається до однієї сутності–кібернетична загроза і є загрозою воєнній сфері. Зважаючи на відсутність подібного переліку, спираючись на положення Закону України "Про основи національної безпеки України", до переліку основних кібернетичних загроз національній безпеці у воєнній сфері слід віднести такі: загроза поширення кібернетичної зброї та технологій її виготовлення; загроза, яка проявляється у недостатній ефективності існуючих структур і механізмів

забезпечення міжнародної кібернетичної безпеки та глобальної й регіональної стабільності; загроза пов'язана з примусовим втягуванням держав в інформаційні війни та кібернетичні конфлікти, що призведуть до загострення протистояння в кіберпросторі між державами; нарощування іншими державами угруповань кібернетичних військ та кібернетичних озброєнь, які порушують співвідношення й розстановку сил у світі, що склалося; загроза прихованому управлінню військами та зброєю; загрози зриву процесів управління між військово-політичним керівництвом держави та збройними силами.

Список використаних джерел

1. Інформаційна безпека держави у воєнній сфері: Навч. посібник / Ю.Г. Даник, М.М. Биченок, В.О. Кацалап, та ін.– К.: НУОУ ім. І. Черняховського, 2019. − 301 с.

2. Наказ Генерального штабу Збройних Сил України від 07.10.2016 р. № 374 "Про затвердження Інструкції з реалізації стратегічних комунікацій у Збройних Силах України".

Тетяна ГРУБІ, к.с.н., доцент
НАДПСУ ім. Богдана Хмельнитцького
ORCID: 0000-0002-8844-5842
E-mail: bitavi_21@ ukr.net

СИСТЕМНО-ФУНКЦІОНАЛЬНИЙ ПІДХІД ДО РЕАЛІЗАЦІЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Більшість сучасних дослідників проблеми забезпечення національної безпеки акцентують увагу на необхідності розгляду її як явища системного. Адже останнє дозволить відповісти на запитання – чи може бути керованим цей процес? Відсутність аргументованої відповіді позбавляє всякого сенсу подальші роздуми довкола головної функції держави – забезпечення національної безпеки. Підкреслимо, що на сьогодні, відсутня єдина думка із зазначеного питання. Деякі вчені не вбачають у відшуканні системності забезпечення національної безпеки ніяких проблем. Інші пропонують зовсім відмовитися від розгляду забезпечення національної безпеки як об'єкта управління.

Так, Г. Ситник та В. Олуйко вважають, що діалектична єдність усіх складових "системи національної безпеки" обумовлена нерозривністю процесу розвитку суспільства у просторі й часі. Об'єднуючись у процесі вирішення завдань забезпечення національної безпеки, суспільство, на думку авторів, спрямовує свої

зусилля на отримання бажаного результату під час реалізації інтересів, які в інтегрованому вигляді сприймаються як інтереси національні [2, с. 93].

Отже, для того, щоб переконатися у системності забезпечення національної безпеки, достатньо з'ясувати, чи складається згаданий процес із взаємозалежних і взаємодіючих елементів? З яких саме? І чи взаємодіють ці елементи між собою настільки, щоб зміна одного з них спричиняла заздалегідь передбачувані зміни інших, а також усієї системи в цілому?

Дослідники соціальних систем стверджують, що елементами соціальних систем, які утворять ту чи іншу сферу, в тому числі й сферу забезпечення національної безпеки, є різноманітні прояви поведінки людей. Разом з тим навряд чи коли-небудь вдасться забезпечити передбачуваність розвитку всієї функціональної системи "забезпечення національної безпеки", виходячи тільки з того, що вона вичерпно представлена таким елементом, як "поведінка людей" [1, с. 124]. Для того, щоб вести мову про відповідність реальної поведінки конкретних осіб визначеним суспільством очікуванням, вважаємо варто спочатку означити вказані очікування. Останні означені в політичних і правових нормах. Вони містять описи того, як необхідно поводитися особі, щоб її поведінка була прийнятною для суспільства.

Таким чином, суспільством встановлено орієнтири для забезпечення національної безпеки як співвідношення між реальною поведінкою людей та компетентних органів і тією її моделлю, яка описана в політичних і правових нормах. Інакше такі описи можна назвати нормативно запропонованою поведінкою. Остання, служить орієнтиром, з одного боку, для конкретних осіб, а з іншого - для суб'єктів забезпечення національної безпеки. Якщо є норма, можна завжди визначити, чи відповідає їй реальна поведінка суб'єкта. У цьому контексті слід відзначити, що існування нормативних орієнтирів поведінки породжує ілюзію можливості вирішення проблем забезпечення національної безпеки за допомогою розширення меж і підвищення "щільності" нормативної регламентації соціально значимої поведінки. Вважається, що чим детальніше буде регламентовано соціально значиму поведінку особи, тим ефективнішим буде забезпечення національної безпеки.

На нашу думку, пошук системної якості забезпечення національної безпеки потребує розгляду цього процесу на основі поєднання відповідності й невідповідності конкретних проявів людської поведінки конкретним нормативним вказівкам. Звідси випливає, що національну безпеку в системно-функціональному плані можна ототожнити з сукупністю конкретних соціально значимих випадків поведінки конкретних осіб. Понад те, представити інакше зміст національної безпеки в системно-функціональному плані досить складно. Це означає, що кожен конкретний прояв поведінки, який виявився в тій чи іншій ситуації соціально значимим, є конкретним ситуаційним проявом стану національної безпеки.

Отже, оволодіння методами управління соціально значимою поведінкою у масштабі конкретної ситуації у сфері національної безпеки неминуче приведе до освоєння керованості процесом забезпечення національної безпеки в цілому,

переходу від пасивного спостереження за процесами у сфері національної безпеки та реагування на їхні наслідки до активного, керованого, цілеспрямованого впливу на згадану сферу. Але чи можна керувати поведінкою людей, яка є ситуаційно соціально значимою? Так, якщо вона - система. Якщо це так і якщо в масштабі конкретної ситуації соціально значима поведінка розкриває зміст національної безпеки, достатньо з'ясувати, взаємодії яких елементів зобов'язана своїм існуванням така система. При забезпеченні національної безпеки взаємодіють такі елементи, як життєво важлива цінність і норма, яка регламентує доступ до неї або її існування.

Однак якби згаданих елементів для забезпечення національної безпеки було б достатньо, то, відповідно, достатньо було б нормативно закріпити перелік життєво важливих цінностей і порядок здійснення доступу до них або їх існування. Але чому, наприклад, одні й ті ж відомості, які становлять державну таємницю, втрачаються в одній установі і не втрачаються в іншій? Адже державна таємниця в обох установах однаково захищається нормою, яка передбачає відповідальність за її розголошення. У результаті більш детального аналізу цих двох ситуацій виявляється, що норма, яка охороняє державну таємницю у кожній з цих двох установ, діяла в різних умовах – у першому випадку порушувалися правила поводження з відомостями, що становлять державну таємницю, в іншому - ні. Приклад умовний і може викликати багато зауважень, але наведений він лише для ілюстрації того, що в масштабі кожної конкретної ситуації визначені умови можуть сприяти формуванню певної моделі соціально значимої поведінки.

Тому ще однією важливою складовою забезпечення національної безпеки можна вважати умови, які формують соціально значиму поведінку. Наявність вказаних трьох ("цінність" - "норма" - "умови") складових процесу забезпечення національної безпеки можна спостерігати в кожній конкретній ситуації. Але в одному випадку державна таємниця залишається в недоторканості, а в іншому, - точно така ж державна таємниця, яка захищається тією ж самою нормою, але в інших умовах, стає предметом злочинного посягання. Тобто пояснити конкретний стан захищеності національної безпеки з появою третього елемента – "умов" вдається точніше і переконливіше. Виокремлення згаданого елемента процесу забезпечення національної безпеки відкриває нові можливості осмислення сутності взаємодії утворюючих його елементів. Необхідно погодитися, що коригуючий зв'язок соціально значимої поведінки з умовами конкретної ситуації простежується набагато легше, ніж її зв'язок із правовою нормою.

Вище наведене дозволяє зробити три висновки:

по-перше, "конкретна ситуація", в якій проявляється соціально значима поведінка особи, що здійснює доступ до життєво важливих цінностей, має чітко виражені якості системи. Отже, така система є ситуаційною. У зв'язку з цим "соціально значима поведінка", яка проявляється і спостерігається в конкретній ситуації, може розглядатися як певна системна якість. Вказана якість здатна проявлятись у цій ситуації лише за наявності трьох елементів ("цінність" - "норма" -

“умови”). Виключення будь-якого з них позбавляє можливості передбачувано змінювати поведінку особи у результаті цілеспрямованого впливу на неї. Таким чином, введення поняття “ситуаційна система” може сприяти вираженню об’єктивної сутності забезпечення національної безпеки, яка проявляється в конкретних ситуаціях;

по-друге, елементи “норма”, “цінність” і “умови”, об’єктивно взаємодіючи між собою, забезпечують принципову можливість захисту (забезпечення) національної безпеки;

по-третє, соціально значимою поведінкою, яка проявляється в кожній конкретній ситуації, можна управляти за допомогою цілеспрямованої корекції умов. Спостереження конкретних ситуацій у сфері забезпечення національної безпеки дозволяє дійти висновку, що наявність життєво важливих цінностей та норм права орієнтує соціально значиму поведінку, а наявність конкретних умов - формує її. При цьому, національна безпека може розглядатися як сукупність об’єктивно існуючих ситуаційних систем, системна властивість яких – соціально значима поведінка - залежить від умов, у яких вона формується.

Список використаних джерел:

1. Данільян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: структура та напрямки реалізації: Навч. посіб. Харків: Фоліо, 2002. 285 с.

2. Ситник Г.П., Олуйко В.М. Організаційно-правові засади забезпечення національної безпеки України. Навчальний посібник. Хмельницький: Вид-во ХУУП, 2005.-236 с.

3. Сучасна глобалістика: провідні концепції і модерна практика: Навч. посібник. К.: МАУП. 2006.802 с.

Ксенія ЄРГІДЗЕЙ, канд. пед. наук
Національний університет оборони України
ORCID: 0000-0003-4634-133X
E-mail: kseniia.yerhidzei@edu.nuou.org.ua
Олександр ЄРГІДЗЕЙ
Національний університет оборони України
E-mail: ergidzey@ukr.net

ОСНОВНІ ФУНКЦІЇ УПРАВЛІННЯ СИСТЕМОЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

При реалізації єдиної державної політики у сфері інформаційної безпеки основні функції управління інформаційною безпекою полягають у наступному:

• збирання, систематизація, узагальнення інформації про стан процесів інформаційної безпеки на об'єктах управління, оцінка стану інформаційної безпеки у регіоні (області, місті, районі), виявлення невирішених проблем, надання необхідної інформації про стан інформаційної безпеки керівництву;

• контроль стану інформаційної безпеки на об'єктах управління;

• визначення пріоритетних напрямів забезпечення інформаційної безпеки у регіоні (області, місті, районі);

• розробка та контроль за виконанням цільових програм із забезпечення інформаційної безпеки (розділів програм розвитку суб'єктів держави);

• організація науково-технічних досліджень та розробок в інтересах забезпечення інформаційної безпеки у регіоні (області, місті, районі), виконання вимог нормативних документів з інформаційної безпеки;

• розробка та затвердження нормативних та методичних документів з інформаційної безпеки (концепцій, положень, вимог, норм, моделей, методик, рекомендацій, інструкцій та інших документів);

• надання методичної допомоги підрозділам, установам, підприємствам та організаціям у підготовці до ліцензування, у діяльності, пов'язаної з наданням послуг у галузі інформаційної безпеки, створенням засобів інформаційної безпеки, а також засобів технічного контролю їх ефективності;

• здійснення методичного керівництва підготовкою, професійною перепідготовкою та підвищенням кваліфікації фахівців у галузі інформаційної безпеки.

При здійсненні координації та функціонального регулювання діяльності щодо забезпечення інформаційної безпеки держави, основними функціями є:

• створення та вдосконалення організаційно-технічного механізму захисту інформаційного простору суб'єктів держави;

• здійснення на плановій основі міжгалузевої координації діяльності щодо забезпечення інформаційної безпеки в апаратах органів державної влади, органах місцевого самоврядування, на підприємствах, в установах, організаціях та підрозділах шляхом регулярного обговорення загальних проблемних питань та прийняття за ними погоджених рішень;

• здійснення методичного керівництва в області інформаційної безпеки щодо апаратів органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, підрозділів шляхом організації видання, поширення та впровадження в практичну діяльність концепцій, положень, вимог, норм, моделей, методик, рекомендацій, інструкцій та інших документів з інформаційної безпеки;

• сприяння міжрегіональному в державі співробітництву в галузі інформаційної безпеки.

Таким чином, важливими особливостями управління системою інформаційної безпеки держави є:

• по-перше, те, що таке управління здійснюється в регіонах, областях, містах, районах в рамках державної системи інформаційної безпеки;

• по-друге, як основні методи управління-використовується координація та функціональне регулювання діяльності із забезпечення інформаційної безпеки;

• по-третє, найважливішим завданням управління системою інформаційної безпеки є створення та вдосконалення механізмів інформаційної безпеки у сфері компетенції суб'єктів держави.

Ігор ЗАЙЦЕВ, доктор філософії
ВА (м. Одеса)
ORCID: 0000-0002-0619-8148
E-mail: zaicev2017@ukr.net

ОКРЕМІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ НАВЧАННІ МАЙБУТНІХ ОФІЦЕРІВ МОРСЬКОЇ ПІХОТИ В ВВНЗ

Швидкий розвиток сучасних інформаційно-комунікаційних технологій в Україні та у світі загалом обумовлює важливість переосмислення інформаційної складової в питаннях підготовки кадрів для Збройних сил України, особливо для підрозділів морської піхоти.

Для підвищення ефективності діяльності ВВНЗ у сфері навчання та підготовки до виконання бойових завдань за призначенням, відтворювання тактики дій підрозділів морської піхоти в різних видах бою (особливо в умовах ведення бойових дій в місті, висадка морського десанту на морське узберіжжя, форсування водних перешкод та оборона берегової смуги, організації заходів антиснайперської боротьби, застосовування стандартних операційних процедур планування, які використовуються в арміях провідних країн світу, проведення тактичних розрахунків (в тому числі за допомогою ПЕОМ), використання бойових можливостей підрозділів морської піхоти, їх штатного озброєння і бойової техніки, застосовування індивідуальної і групової зброї та бойової техніки в складних умовах бойової обстановки на різноманітній місцевості у взаємодії з підрозділами інших родів військ), не в останню чергу впливає використання сучасних інформаційних комунікаційних технологій (ІКТ) та автоматизованих інформаційних систем.

Проте слід констатувати, що впровадження інформаційних технологій у військову освіту в процесі підготовки майбутніх морських піхотинців передбачає удосконалення існуючої системи операцій з накопичення, зберігання, обробки та передачі інформації, які здійснюються за допомогою спеціальних каналів зв’язку з використанням комп’ютерної техніки [1].

На перше місце виходить Інформаційна безпека (ІБ), особливо фактори що впливають на неї.

Так, до факторів, що впливають на ІБ ВВНЗ, належить:

відсутність цілісної системи інформаційно-аналітичного забезпечення військово навчального закладу (систему захисту інтелектуальної інформаційної власності навчального закладу від зовнішніх і внутрішніх агресивних впливів і систему управління доступом до інформації та захисту від агресивних інформаційних просторів);

низький загальний рівень розвитку інформаційної інфраструктури, що створює передумови експансії іноземних компаній на ринку інформаційних послуг [1];

упровадження в ВВНЗ комп'ютеризованих засобів та засобів зв'язку з відповідним програмним забезпеченням іноземного виробництва, що створює передумови витоку інформації з обмеженим доступом, становлячи реальну загрозу інформаційній безпеці;

недостатня кількість наявних комп'ютеризованих засобів в ВВНЗ, як правило на основі мізерного фінансування (це комп'ютери, сервери, мережеве обладнання, засоби зв'язку і телекомунікації, системи програмного забезпечення, призначені для вирішення завдань і ведення освітньої діяльності);

великий обсяг інформації з обмеженим доступом, відсутність в достатній кількості комп'ютеризованих засобів та засобів зв'язку з відповідним програмним забезпеченням для роботи з відповідними обмеженнями (ДСК, Т, ЦТ);

обмеження доступу в ВВНЗ до інформації через нестачу фінансів для роботи в закритих інтернет-ресурсах;

домінування психоемоційних факторів в інформаційному просторі (особливо в телевізійному просторі та мережі "Інтернет");

відсутність єдності інформаційних потоків усередині ВВНЗ з відповідним доступом для всіх хто навчається;

низький рівень медіаграмотності переважної більшості абітурієнтів (перший курс) [1];

відсутність в достатній кількості фахівців що працють з відповідним програмним забезпеченням;

відсутність тренажерів, наприклад VBS-3 (комп'ютерних класів з достатньою кількістю робочих місць, обладнаних сучасною технікою і програмним забезпеченням із безпечним доступом до мережі Інтернет, для опановування нових технологій та здобуття навичків за відповідною спеціалізацією), щодо розвитку критичного мислення [2].

Список використаних джерел:

1. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія /О. В. Левченко. – Житомир, 2021. 172 с.

2. Bykov I. A., Balakhonskaya L. V., Gladchenko I. A., Balakhonsky V. V. Verbal aggression as a communication strategy in digital society. Proceedings of the 2018 IEEE Communication Strategies in Digital Society Workshop. Saint-Petersburg, 2018. P. 12–14.

Олександр ЗАЙЦЕВ, к.т.н., доцент
ВА ім. Євгенія Березняка
ORCID: 0000-0003-2475-3800
E-mail: a.zaycev@gmail.com
Михайло ПОПОВ, д.т.н., професор,
член-кореспондент НАН України
ДУ "Науковий центр аерокосмічних досліджень Землі
Інституту геологічних наук НАН України"
ORCID: 0000-0003-1738-8227
E-mail: mpopov@casre.kiev.ua
Сергій СТЕФАНЦЕВ
ВА ім. Євгенія Березняка
ORCID: 0000-0002-7629-7563
E-mail: stefancevss@gmail.com

ПРОБЛЕМА ЙМОВІРНІСНОЇ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА УМОВ НЕВИЗНАЧЕНОСТІ

Постановка проблеми в загальному вигляді. Інформаційний ризик – це імовірність виникнення втрат в зв'язку з зловмисним або випадковим виводом з ладу елементів інформаційної системи або викрадення інформації з інформаційної системи. Оцінка ризику – це визначення даної імовірності. Ризик інформаційної безпеки (ІБ) – це потенційна можливість використання вразливостей активів конкретної загрози для заподіяння шкоди організації [1].

Чим раніше виявляється ризик ІБ, тим більше ресурс часу та можливостей в організації, щоб його нейтралізувати або вжити інших необхідних заходів.

У повсякденній діяльності виявлення та оцінка можливих ризиків ІБ ускладнюються, як правило, наявністю багатьох невизначеностей. Ця обставина пояснює, чому, незважаючи на значні успіхи у створенні різних систем автоматизації управління ризиками ІБ (наприклад, ITRM), оцінка ситуації виконується спеціалістами–експертами [2].

У зв'язку з цим важливе значення надається добору експертів у відповідній галузі знань. Однак необхідно мати на увазі, що оцінки експерта є суб'єктивними, з елементами неточності, причому рівень неточності суто індивідуальний. Передбачити помилки, яких може припуститися експерт, особливо в умовах

інформаційної недостатності, досить складно і важко внести корективи до оцінок, які ним надаються [3].

Постає необхідність у підвищені точності ймовірнісних оцінок експерта, особливо в умовах присутності фактора інформаційної недостатності. Одним із варіантів вирішення цього завдання є введення в процедуру формування оцінок показника надійності експерта. Для цього автори пропонують використати експертно-розрахункову модель формування ймовірнісної оцінки [4].

Виклад основного матеріалу. Наприклад, було поставлене завдання вивчити певну ситуацію під кутом можливого ризику ІБ. При вирішенні цього завдання експерт має оцінити факт існування / відсутності ризику ІБ і навести відповідне значення ймовірності.

Оцінка експерта факту існування / відсутності ризику ІБ може бути вірною (позначимо таку оцінку як T_e) або помилковою ($\overline{T_e}$).

При співставленні оцінки експерта з реальною ситуацією існують чотири варіанти:

1. Ризик ІБ існує і експерт вказує на це; ймовірність такого варіанту позначимо як $p(T \wedge T_e)$.

2. Ризик ІБ існує, але експертом не виявлений; ймовірність позначимо $p(T \wedge \overline{T_e})$.

3. Ризику ІБ реально немає, й саме таким є висновок експерта; ймовірність позначимо $p(\overline{T} \wedge T_e)$.

4. Ризику ІБ реально немає, проте експерт фіксує її наявність; ймовірність позначимо $p(\overline{T} \wedge \overline{T_e})$.

Ймовірності, наведені у першому і третьому варіантах, сумарно дають ймовірність правильного оцінювання ситуації. Другий варіант характеризується ймовірністю пропуску ризику ІБ. Ймовірність, наведена у четвертому варіанті, характеризує хибну тривогу.

Очевидно, що

$$p(T \wedge T_e) + p(T \wedge \overline{T_e}) + p(\overline{T} \wedge T_e) + p(\overline{T} \wedge \overline{T_e}) = 1. \quad (1)$$

Завдання експерта – надати ймовірність правильного оцінювання ризику ІБ $p(T_e)$, але, як відзначалося вище, точність такої оцінки залежить, у тому числі, від надійності експерта, а також від ситуацій з розподілами ймовірностей всіх можливих ситуацій.

Для оцінки надійності експерта будемо використовувати результати його попередньої діяльності, тобто, визначається повна кількість оціночних процедур, в яких брав участь даний конкретний експерт на протязі певного періоду часу, а також визначається, яка кількість з цих процедур виявилась успішною [5].

Тоді надійність r зазначеного експерта розраховується як:

$$r = \frac{\textit{кількість успішних оціночних процедур}}{\textit{повна кількість оціночних процедур}}.$$

Припустимо, експерт, який має надійність r, оцінив ймовірність ризику ІБ $p(T_e)$. Тоді ймовірність виявлення експертом з надійністю r присутності ризику ІБ виражається формулою:

$$p(T \wedge T_e) = p(T_e) \cdot r \qquad (2)$$

Відзначимо, що в рамках сукупності наведених вище варіантів і відповідних ймовірностей надійність може бути визначена за виразом:

$$r = p(T \wedge T_e) + p(\overline{T} \wedge T_e) \qquad (3)$$

Висновки. В роботі описано підхід до оцінювання загрози ІБ в умовах невизначеності, особливістю якого є включення в експертно-розрахункову модель формування ймовірнісної оцінки показника надійності експерта.

Запропонований підхід до обчислення ймовірнісної оцінки ризиків ІБ може бути використаний в широкому спектрі практичних задач з невизначеністю, особливо у сфері забезпечення національної безпеки та оборони.

Список використаних джерел:

1. Поліщук Д. В., Захарова М. В., Люта М. В. Модель оцінки ризиків інформаційної системи. *Сучасні електромеханічні та інформаційні системи* : монографія / за ред. І. В. Панасюка. Київ, 2021. С. 102–106.
2. Система автоматизації управління ризиками інформаційної безпеки ITRM. *TechExpert*. URL: https://techexpert.ua/solutions-it/itrm-systema-avtomatyzatsii-upravlinnya-ryzykamy-ib/ (дата звернення: 18.09.2023).
3. Попов М.О., Топольницький М.В., Стамбірська Р.Г. Підхід до визначення достовірності розвідувальної інформації при наявності кількох джерел різної надійності. *Вісник воєнної розвідки*. 2020. № 62. С. 47–54.
4. Зайцев О. В., Попов М. О., Стефанцев С С. Щодо ймовірнісної оцінки загрози в умовах невизначеності. *Актуальні питання протидії загрозам застосування вибухонебезпечних предметів в умовах гібридної війни* : матеріали науково-практичного семінару, м. Київ, 22 серп. 2023 р. / НУОУ, 2023. С. 30–37.
5. Beer M., Gong Z., Kreinovich V. How Accurate Are Expert Estimations of Correlation? : *Proceedings of the 2017 IEEE Symposium on Computational Intelligence for Engineering Solutions CIES'2017*, Honolulu, Hawaii, November 27 - December 1, 2017. P. 883–891.

Віктор ІВАНІВ
НУОУ
ORCID: 0009-0004-3881-9991
E-mail: v.ivaniv@i.ua

АНАЛІЗ ЧИННИКІВ, ЯКІ ВПЛИВАЮТЬ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ЗБРОЙНИХ СИЛ УКРАЇНИ

Під час проведення досліджень визначені найбільш впливові дві групи чинників, які впливають на інформаційну безпеку Збройних Сил України. Ними є відношення провідних країн світу та міжнародних безпекових організацій до України та сприйняття населенням України державної інформаційної політики.

Аналіз джерел [1, 2] показав, що, Україна у середньостроковій перспективі постійно буде знаходиться під інформаційним впливом рф. Це обумовлене тим, що інформаційний простір України недостатньо захищений від інформаційних впливів рф. Також впливовою залишається ситуація, коли в українському суспільстві ще не сформована концепція перемоги. Саме тому необхідно здійснювати комплекс заходів щодо забезпечення інформаційної безпеки України, реалізація якого дозволить створити умови для сталого та гарантованого задоволення національних інтересів держави, упередження та нейтралізації загроз національним інтересам та національній безпеці України в інформаційній сфері.

Соціальні мережі активно застосовуються для інформаційних маніпуляцій, розповсюдження фейків, формування викривленого сприйняття у людей. Найпопулярніша соціальна мережа в Україні – Facebook. Дана соціальна мережа, як і YouTube, використовує розумну стрічку. Facebook акумулює дописи з усіх акаунтів друзів та тих сторінок, на які людина підписалась. Те, що найбільш вірогідно зацікавить користувача, Facebook показує йому першочергово. Тож, інформаційний месседж, який вкинутий до мережі, швидко поширюється серед певної групи користувачів. YouTube з 2019 року розпочав боротьбу з відео, які містять мову ворожнечі, але гігантський обсяг інформації, який потрапляє на дану платформу, повністю очистити від фейків неможливо. Месенджер Telegram є безумовним лідером щодо розповсюдження фейкової інформації, що обумовлюється анонімністю публікацій. Telegram-канали стали першоджерелом псевдоінсайдів та зливів інформації. Зараз функціонують цілі сітки анонімних каналів [3].

Більшість проблем, що накопичилися в інформаційній сфері Збройних Сил України, мають системний і хронічний характер, але події та процеси, спричинені російською агресією змушують нині терміново шукати шляхи їх вирішення. Для чого необхідно також враховувати і вплив зовнішніх та внутрішніх чинників. До зовнішніх більш притаманні такі інформаційні чинники як:

відношення провідних країн світу до України та до рф (сприйняття конфлікту);

ступінь присутності українських (проукраїнських) і російських (проросійських) інформаційних джерел в інформаційному просторі провідних країн світу;

захищеність інформаційного простору провідних країн світу від кібератак російських (проросійських) хакерів;

спільність історії, культури, мови, мистецтва України з провідними країнами світу і з рф;

підрив довіри до НАТО та ЄС;

фальсифікація історії з метою заперечення існування окремої української нації та історичної тривалості української державності;

вплив церкви на національну свідомість.

До внутрішніх інформаційних чинників можна віднести наступні:

сформованість національної ідеї України;

ступінь самоідентифікації громадян України;

єдність поглядів громадян України на питання релігії;

єдність поглядів громадян України на питання мови (провідного статусу української мови у всіх регіонах України);

рівень життя населення в Україні;

захищеність інформаційного простору України від інформаційних впливів;

авторитет та рівень довіри населення України та Росії до керівництва держави, державних інститутів та силових структур;

втомленість населення України та РФ від воєнного конфлікту.

Отже, аналіз чинників, які впливають на інформаційну безпеку Збройних Сил України показує, що в дійсності кожен із чинників буде визначати певні ознаки інформаційно-психологічного впливу противника.

Список використаних джерел

1. Горбулін В. Тези до другої річниці російської агресії проти України: [Електрон. Ресурс]. – Режим доступу: https://docviewer.yandex.ua/view/

2. Leigh Armistead “Information Operations. Warfare and the Hard Reality of Soft Power”, Potomac Books, INC, Washington D.C.

3. Стратегическое прогнозирование международных отношений : кол. монография / под ред. А. И. Подберезкина, М. В. Александрова; [А. И. Подберезкин и др.]; Моск. гос. ин-т междунар. отношений (ун-т) М-ва иностр. дел Рос. Федерации, Центр военно-политических исследований. — М.: МГИМО–Университет, 2022. - 743 с.

Олександр ІЖКО
НУОУ
ORCID: 0009-0004-0574-492X
E-mail: o.ichko@i.ua

КОНЦЕПЦІЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ОБРОБКИ ПОПЕРЕДНЬОЇ ІНФОРМАЦІЇ

Головним призначенням концепції інформаційного забезпечення системи обробки попередньої інформації є отримання та первинна обробка інформації про особу (пасажира) та надання її до зацікавлених інстанцій з метою забезпечення належного рівня Національної безпеки України. При цьому загально прийнята в Європейських країнах послідовність обробки попередньої інформації про пасажирів (API/PNR) буде відповідати умовам воєнного стану в якому зараз знаходиться Україна, коли застосовувані заходи будуть адекватні наявним (потенційним) небезпекам. Останні ж мають мінливий характер, який визначається складнофункціональними залежностями багатьох чинників, серед яких:

широкомасштабна агресія рф проти України;

стан військово-політичної, соціально-економічної та інших видів обстановки між країнами, що мають потенційну загрозу;

наявність і стан мережі шляхів сполучення та інших елементів інфраструктури;

погодні умови та багато інших.

Зазначене обумовлює унікальність числового вираження ймовірності знаходження інформації про пасажира, який може виявитись правопорушником у певних просторово-часових координатах. Відповідно, щоб система обробки попередньої інформації про пасажирів (API/PNR) виконувала своє призначення (забезпечувала мінімально достатній рівень ймовірності виявлення правопорушника), мала необхідну стійкість функціонування та не була занадто затратною, її структура повинна мати адаптивною відповідно до змін обстановки [1].

Отже, метою тез є обрис концепції інформаційного забезпечення системи обробки попередньої інформації (API/PNR).

Взаємодіючими елементами системи обробки попередньої інформації про пасажирів (API/PNR) є різноманітні бази даних. Це обумовлює необхідність часового розподілу запитів до різних систем, що відбувається під впливом постійної зміни числового значення ймовірності знаходження правопорушника у різні періоди часу, а також залежністю достовірної та релевантної інформації в базах даних [2].

Основними етапами концепції інформаційного забезпечення системи обробки попередньої інформації про пасажирів (API/PNR) є:

I. Побудова кібернетико-лінгвістичної і концептуальної моделі системи обробки попередньої інформації про пасажирів (API/PNR).

II. Формалізація мети та умов (характерних особливостей) функціонування компонентів системи обробки попередньої інформації про пасажирів (API/PNR).

III. Обґрунтування інформаційної основи оцінки ефективності системи обробки попередньої інформації про пасажирів (API/PNR) (розробка методики оцінки ефективності функціонування компонентів системи обробки попередньої інформації про пасажирів (API/PNR), побудова моделі їх вартісного ресурсу, обґрунтування критерію ефективності системи).

IV. Розробка методики побудови системи обробки попередньої інформації про пасажирів (API/PNR).

V. Оцінювання складових системи обробки попередньої інформації про пасажирів (API/PNR).

VI. Узагальнення та оформлення результатів функціонування системи обробки попередньої інформації про пасажирів (API/PNR).

У рамках першого етапу встановлюються умови невизначеності проектування системи обробки попередньої інформації про пасажирів (API/PNR), які, зокрема, обумовлені такими особливостями: 1) наявністю великої кількості факторів різного характеру, що впливають на ефективність; 2) відсутністю кількісних достовірних початкових даних про ці фактори; 3) обмеженістю формальних (математичних) методів отримання оптимальних рішень. Крім цього, неможливість застосування існуючих методів для обґрунтування компонентного складу системи обробки попередньої інформації про пасажирів (API/PNR) обумовлена тим, що вони не враховують ряд принципових особливостей, котрі притаманні для правоохоронних органів. Зазначені проблемні питання здебільшого пов’язані з розбіжністю концепцій побудови систем такого класу, що, у свою чергу, обумовлює необхідність обґрунтування доцільності елементів системи обробки попередньої інформації про пасажирів (API/PNR) [3].

Розв’язання задачі побудови системи обробки попередньої інформації про пасажирів (API/PNR) в умовах невизначеності стає можливим при застосуванні системного підходу, головною задачею якого є створення загальної методології вивчення й моделювання складних систем, а також керування ними в умовах неповної інформації й різного роду обмежень.

Вплив усієї множини детермінант важко формалізувати, тому й початкова модель структурного синтезу систем вбачається в параметрично-вербальному (кібернетико-лінгвістичному) виді. Конкретний набір сукупності вхідних параметрів визначається з урахуванням забезпечення принципу показності (валідності) критерію ефективності структур систем, що полягає у необхідності оцінювати лише ступінь досягнення головної мети, вирішення основних, а не

другорядних завдань.

Таким чином, формалізоване подання концепції інформаційного забезпечення системи обробки попередньої інформації про пасажирів (API/PNR) та особливостей її функціонування надає можливість окреслити область оцінювання її ефективності в умовах багатофакторності та невизначеності, а також адекватно підійти до питання встановлення ознак оптимальності системи.

Список використаних джерел

1. Філіппов С. О. Окремі аспекти використання даних про пасажирів (API/PNR) в інтересах прикордонної безпеки. Правова держава. 2021. № 43. С. 169-176.1.
2. Гуткин Л. С. Оптимизация радиоэлектронных устройств по совокупности показателей качества / Л. С. Гуткин. – М.: Сов. радио, 1975. – 123 с.
3. ДСТУ 2860 – 94. Надійність техніки. Терміни та визначення; Чин. від 01.01.96. – К.: Держстандарт України, 1996. – 92 с.

Віроніка КАЛАЧОВА, к.т.н., снс
ORCID: 0000-0003-3477-0858
E-mail: vkadres@ukr.net
Олег МІСЮРА, к.т.н., снс
ORCID: 0000-0002-3025-3477
E-mail: vvti_hups@ukr.net
Денис ЗАПАРА, к.в.н.
ORCID: 0000-0003-3949-7555
E-mail: vvti_hups@ukr.net
Дмитро СІЗОН
ORCID: 0000-0003-0544-1625
E-mail: ssdimass80@ukr.net
Віталій ПИЛИПЕНКО
ХНУПС ім. Івана Кожедуба
ORCID: 0000-0002-3912-4372
E-mail: pilipenko_v75@ukr.net

ПОШУК ШЛЯХІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДЧАС ОРГАНІЗАЦІЇ ТА ЗДІЙСНЕННЯ ДН У ВВНЗ УКРАЇНИ В УМОВАХ ДІЇ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

2022 рік став роком величезних випробувань для всіх навчальних закладів України з приводу їх здатності до швидкої організації дистанційного варіанту

навчального процесу (ДН) в зв'язку з широкомасштабною збройною агресією рф проти України, розпочатою 24 лютого 2022 року з метою знищення нашої країни та її народу. Всі ці події призвели до суттєвих змін пріоритетів у виборі форм надання освітніх послуг в навчальних закладах України в умовах дії правового режиму воєнного стану. 25 лютого 2022 року МОН України рекомендувало ввести в усіх закладах освіти тимчасові канікули, після яких, запропонувало в умовах воєнного стану продовжувати навчальний процес у дистанційному або змішаному форматі (за попереднім погодженням з місцевою військово-цивільною адміністрацією) [1]. МО України було прийнято ряд рішень щодо внесення змін до організації освітньої діяльності у ВВНЗ, ВНПЗВО та ЗФПВО та ухвалене рішення щодо широкого застосування в ВНЗ технологій ДН для надання освітніх послуг в умовах воєнного стану. ДН дозволило протягом незначного часу, здійснити швидке відновлення навчального процесу з мінімальними фінансовими витратами на його організацію і, що найважливіше, зменшило загрозу безпеці життя мільйонів українців, задіяних в цих процесах. В цих умовах МОН та МО України рекомендували ЗВО та ВВНЗ для надання освітніх послуг, застосовувати наступні інформаційні технології (ІТ) та Internet-ресурси: системи управління навчанням (LMS), на кшталт, MOODLE, Google Workspace for Education/Google Suite for Education, Microsoft Office 365 Education, LMS власної (ЗВО та ВВНЗ) розробки, з, відповідною до вимог інформаційної безпеці, системою захисту даних та ін.; месенджери (WhatsApp, Signal та ін.); програмні додатки для здійснення відеоконференцій та вебінарів (Microsoft Teams, ZOOM, Google Meet, BigBlueButton та ін.); додатки Google ClassRoom, TeamViewer, YouTube; ресурси освітніх платформ Coursera, Udemy та EdX; електронні документи про освіту в мобільному додатку "Дія" для забезпечення рівних можливостей доступу до освіти та працевлаштування всіх громадян України за підтримки проекту EU4DigitalUA (Академія електронного урядування (e-Governance Academy)); спецмережі з обмеженним доступом та мережі типу Intarnet; програмні додатки для здійснення паролювання доступу, ретельної ідентифікації користувачів, криптографічного захисту інформації (ЗІ). Повертаючись до збройної агресії рф проти України, треба зазначити, що їй притаманні ознаки гібридної війни, одним з типових компонентів якої є використання методів, що сприяють виникненню та поглибленню в державі, обраній для агресії, внутрішніх конфліктів, зокрема, створення внутрішніх суспільних протиріч через пропаганду з її переходом у інформаційну війну. Тому, в цих умовах, питання пошуку шляхів забезпечення інформаційної безпеки підчас організації та здійснення ДН у ВВНЗ України в умовах дії правового режиму воєнного стану є як ніколи актуальним. ХНУПС ім. Івана Кожедуба є одним з провідних ВВНЗ України з питань застосування та розробки новітніх ІТ для автоматизації навчального процесу і, зокрема, для організації та здійснення ДН. На даний момент в умовах воєнного стану основними ІТ, які застосовуються навчальним закладом є: месенджери WhatsApp

та Signal, які є більш захищеними від можливого несанкціонованого доступу хакерів рф до інформаційних ресурсів користувачів; LMS з відкритим кодом MOODLE для здійснення ДН, яка, доречі, зазнала на початку 2023 року теж хакерської атаки; платформи ZOOM, BigBlueButton, які використовуються Університетом як майданчики для проведення конференцій в режимі on-line; навчально-тренажерні комплекси; власні розробки ХНУПС: інформаційно-освітнє середовище (ІОС) "ДІАЛОГ", універсальна система розробки та проведення комп'ютерних тестів, комплекс проектування навчального розкладу "КАСКАД" [1]. У результаті проведення досліджень щодо підвищення ефективності бойової підготовки шляхом використання технологій ДН науковцями ХНУПС у 2008 році було розроблено ІОС "ДІАЛОГ", яке дозволяє: планувати навчання шляхом розподілу предметів по видах підготовки; навчатися у складі груп за визначеними для них предметами навчання; організовувати заняття згідно вимог наказів МО України стосовно підготовки військових фахівців; здійснювати автоматизований контроль тестування тих, хто навчається з автоматичною фіксацією часу та результатів проходження тестів; контролювати процес навчання за середнім балом для групи, курсу завдяки системі формування статистичних даних. В цій ІОС програмно реалізовано власну систему ЗІ. Кожна людина, що використовує комп'ютер для доступу у внутрішню інформаційну мережу ІОС, є користувачем цієї мережі. Будь-який користувач мережі, що зайшов в середу ДН, реалізованої у вигляді web-додатку, є учасником процесу ДН. Будь-який учасник процесу ДН повинен володіти певними правами при роботі в ІОС. Права користувачів – це перелік завдань, які користувачу дозволено виконувати в системі. Права користувачів є так званими дозволами, тобто набором правил, пов'язаних з певним об'єктом, і які використовуються для управління доступом до цих об'єктів. Дозволи призначаються власниками цих об'єктів - адміністраторами. Кожен користувач може належати до будь-якої групи користувачів ІОС для ДН з бойової підготовки. Групи необхідні для того, щоб надати декільком користувачам ідентичні права доступу до об'єктів системи. Група включається у виборчі таблиці управління доступом, які визначають тип доступу до об'єкту. У середовищі дистанційного навчання передбачено 8 груп (категорій) користувачів: "КУРАТОР", "ІНСПЕКТОР", "АДМІНІСТРАТОР", "МЕТОДИСТ", "ВИКЛАДАЧ", "СТУДЕНТ", "ГІСТЬ", "ЦЕНЗОР". Саме користувачі групи "ЦЕНЗОР" відповідають за ЗІ: планування (планування заходів із ЗІ в ІОС); організацію (розробку інструкції із ЗІ в ІОС для кожної з категорій учасників ДН; організацію дотримання режиму ЗІ в ІОС; блокування використання інформації в системі з грифом вище дозволеного); контроль (контроль обміну інформацією між центрами; контроль за реєстрацією користувачів ІОС та відповідністю надання прав доступу до інформаційних ресурсів; контроль за обігом документів з обмеженим доступом; контроль за технічними засобами придушення випромінювання електронної ОТ); облік (збір інформації про спроби

несанкціонованого доступу до системи; облік користувачів ІОС та даних про них); аналіз (аналіз інформації про спроби несанкціонованого доступу до системи; аналіз журналів системних подій; розробка пропозицій щодо вдосконалення ІОС з напряму ЗІ) [1]. Таким чином, враховуючи гібридний характер російсько-української війни, систематичні кібератаки на органи військового управління, центральні та місцеві органи влади, а також на автоматизовані системи управління навчанням ВВНЗ України, питання пошуку шляхів забезпечення інформаційної безпеки підчас здійснення ДН у ВВНЗ України є дуже актуальним, а існуючі на сьогоднішній день ІТ, що реалізують широкий спектр ефективних алгоритмів і методів ЗІ, мають бути максимально задіяні при організації навчання на відстані у ВВНЗ в умовах дії правового режиму воєнного стану з обов'язковим залученням до цього процесу досвідченних фахівців з питань інформаційної безпеки навчального закладу.

Список використаних джерел:

1. Калачова В. В., Місюра О. М., Пилипенко В. М., Дуденко С. В., Третяк В. Ф., Коломійцев О. В., Хворост О. Г. Аналіз ефективних рішень та позитивного досвіду застосування технологій ДН цивільними та військовими ЗВО України в умовах воєнного стану. Системи обробки інформації. 2022. № 4 (171). С. 17-31.

Сергій КОНДРАТЮК
ЖВІ ім. С.П. Корольова
ORCID: 0009-0000-9103-0368
E-mail: kondratyuk27.2002@gmail.com

ПРОБЛЕМНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАСЕЛЕННЯ УКРАЇНИ

Постановка проблеми. В умовах війни Інформаційна безпека населення України є в край важливою. Сучасні інформаційні технології розширюють можливості обміну інформацією, проте також відкривають можливості для негативного інформаційно-психологічного впливу (ІПсВ) на найменш інформаційно грамотні верстви населення України, що створює актуальні завдання і вимагає вивчення та розв'язання проблем в інформаційній безпеці. Однією з важливих тенденцій, які виявилися актуальними в сучасних умовах, є швидкий розвиток методів і технологій впливу на свідомість (включаючи підсвідомість) та психічний стан населення, порівняно з розвитком заходів для протидії цьому впливу. Ця проблема є надзвичайно важливою для українського суспільства, особливо під час конфлікту з Росією, і потребує належної уваги та

вивчення. Тому інформаційна грамотність є одним з перших пунктів в розв'язуванні проблеми інформаційної безпеки населення України, а в період війни набуває особливої актуальності.

Аналіз останніх досліджень і публікацій. Протягом останніх років було проведено ряд досліджень українських вчених, таких як М.М. Нікіфоров, Ю.В. Турченко, І.Ю. Юзова, П. Пацек, В.І. Алещенко, В.Г. Сербін і інші, що стосувалися захисту населення від негативного інформаційно-психологічного впливу. У їх дослідженнях були розглянуті механізми, цілі, технології та методи російської пропаганди в Україні, з особливим акцентом на аналізі стратегій впливу на свідомість через засоби масової комунікації. Також було досліджено вплив інформаційно-психологічної війни на військовослужбовців, які перебувають в зоні активних бойових дій, а також на населення, що проживає на окупованих територіях.

Незважаючи на актуальність цієї теми та наявність значної кількості наукових досліджень і практичних методик захисту від негативного інформаційно-психологічного впливу, питання підвищення інформаційної грамотності населення України як одного з механізмів захисту не отримало належної уваги.

Метою цієї доповіді є дослідження можливостей захисту населення України від негативного інформаційно-психологічного впливу шляхом підвищення рівня інформаційної грамотності. У доповіді розглянуто практичні аспекти інформаційної грамотності та запропоновано шляхи її нарощування серед населення України.

За практичним досвідом відомо, що для здійснення інформаційно-психологічної війни проти населення України противник використовує різні засоби і технології, такі як аудіовізуальні та візуальні матеріали, розповсюджені через друковані засоби масової інформації, телебачення та Інтернет. Також можуть бути задіяні спеціально навчені агенти, які працюють на масових заходах. Наслідком такого впливу може бути незадоволення населення своїм соціальним статусом, політичним керівництвом, а також зміна свідомості та поведінки населення, що є загрозливими наслідками для суспільства. Інформаційно-психологічний вплив зазвичай здійснюється приховано, і люди навіть не завжди розуміють, що перебувають під впливом дезінформації, паніки, страху та недовіри.

Для захисту населення від негативного інформаційно-психологічного впливу в доповіді запропоновано реалізувати стратегію підвищення рівня інформаційної грамотності. Інформаційна грамотність в даному контексті розглядається як здатність людини розрізняти правдиву інформацію від фейкової, вміння обирати надійні джерела інформації в Інтернеті, а також навички перевірки інформації на достовірність та бути обачливим з чутками які надходять до людини від її знайомих, родичів чи інших людей та знати як і де цю інформацію перевірити.

Підвищення інформаційної грамотності передбачає розвиток у населення навичок критичного аналізу інформації, що надходить з різних джерел, та здатність перевіряти її достовірність, а також виявлення та оцінка першочергового інформаційного ресурсу який опублікував інформацію.

Висновки. Таким чином, в умовах активної військової агресії проти України, інформаційно-психологічна вплив стає серйозною загрозою для населення нашої країни. Впровадження підходу, який було запропоновано в тезах доповіді, сприятиме підвищенню рівня інформаційної грамотності серед населення України. Це в свою чергу сприятиме збереженню волі українського народу для активного спротиву та підвищить стійкість нашого суспільства перед інформаційним впливом агресора.

Список використаних джерел:

1. Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька ; за заг. ред. Р. В. Грищука. – Житомир : ЖНАЕУ, 2019. – 280 с.

2. Грищук Р. Технологічні аспекти інформаційного протиборства на сучасному етапі. / Р. В. Грищук, І. О. Канкін, В. В. Охрімчук // Захист інформації, Том 17, № 1, С. 80 – 86, 2015.

3. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування: монографія / О. В. Левченко. Житомир: Видавець ПП ”Євро-Волинь”, 2021. – 172 с.

Юлія КОРДУНОВА
ORCID: 0000-0003-0151-8285
E-mail: kordunovayulia@gmail.com
Олександр ПРИДАТКО, к.т.н., доцент
ЛДУ БЖД
ORCID: 0000-0002-0719-9118
E-mail: o_prydatko@ukr.net

КОНЦЕПТУАЛЬНА МОДЕЛЬ ПРОЦЕСУ УПРАВЛІННЯ ЖИТТЄВИМ ЦИКЛОМ СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У сучасному світі інформаційні технології відіграють важливу роль в усіх галузях діяльності, включаючи рятувальну сферу. Особливо актуальним є розроблення безпеко-орієнтованих сервісів для Державної служби України з надзвичайних ситуацій, які спрямовані на забезпечення безпеки та підтримку рятувальників при виконанні службових обов'язків. Ці сервіси відіграють важливу

роль у запобіганні надзвичайним ситуаціям, покращенні реагування на них, збільшенні шансів на врятовані життя та мінімізації збитків.

Розроблення безпеко-орієнтованих програмних систем вимагає специфічних підходів та методів, які притаманні критично важливим сервісам. Саме тому постає потреба у розробці нових та удосконаленні вже відомих підходів до управління життєвим циклом програмного забезпечення, враховуючи специфіку роботи служби порятунку.

На рисунку 1 запропонована концептуальна модель, яка корелює із принципами гнучкої методології розробки програмного забезпечення та адаптована під специфіку роботи служби порятунку.

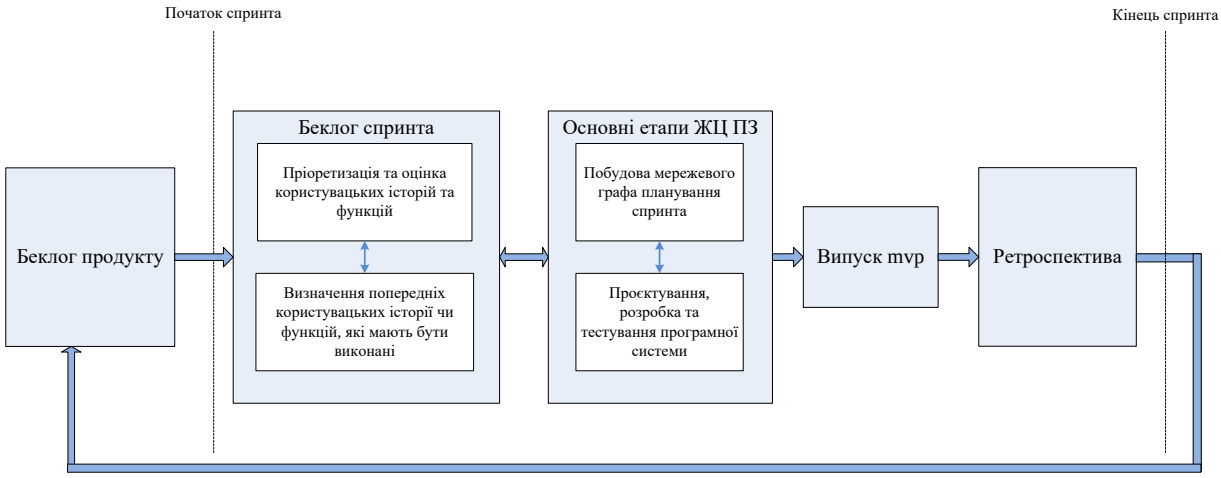


Рис. 1. Розроблена концептуальна модель процесу управління життєвим циклом БОС

З огляду на вище представлену концептуальну модель, процес розробки БОС починається із формування беклогу продукту. У даному випадку беклог містить всі завдання (користувацькі історії) та функції, які необхідно виконати для розробки цілої програмної системи. Після його формування весь процес розробки як і в звичній Scrum команді розбивається на ітерації (спринти), кожна з яких повинна завершуватись випуском готового функціоналу (mvp) та ретроспективою.

Зважаючи на специфіку розробки безпеко-орієнтованих сервісів беклог спринта формується наступним чином:

1. Пріоретизуються та оцінюються користувацькі історії та функції, які необхідно виконати за спринт.

2. Визначаються попередні користувацькі історії чи функції, які мають бути виконані, оскільки існують такі задачі, виконання яких можливе лише після завершення попередніх.

Між цими пунктами існує двосторонній зв'язок, оскільки при зміні пріоритету користувацької історії може змінюватись також і попередня користувацька історія.

Після формування беклогу спринта відбувається розроблення самої системи. Для автоматизації етапу планування запропоновано побудувати мережевий граф планування спринта та обчислити його основні показники (критичний шлях, ранні та пізні терміни виконання подій, резерви на виконання завдань). Даний підхід надасть проєктній команді можливість відслідковувати в режимі реального часу стан розробки системи та, за потреби, змінювати хід виконання завдань. Мережеве планування дає змогу ефективно розподіляти час на розробку та автоматизувати процес визначення критично важливих функцій для випуску mvp.

Після планування відбуваються звичні етапи життєвого циклу програмного забезпечення (далі – ЖЦ ПЗ), такі як: проектування, розроблення, тестування програмної системи. На концептуальній схемі між плануванням та наступними етапами ЖЦ ПЗ зображений двосторонній зв'язок, оскільки залежно від процесу розробки, складності завдань, досвіду проєктної команди та інших чинників час на розробку може змінюватись, тому може виникнути потреба у перепланування мережевого графа. Двосторонній зв'язок існує також і між формуванням беклогу спринта та основними етапами ЖЦ ПЗ, оскільки залежно від визначеного критичного шляху під час мережевого планування, завдання та користувацькі історії беклогу спринта можуть змінюватись. І навпаки.

Завершується спринт випуском готового продукту, який вже може бути використаний у службовій діяльності працівниками ДСНС та ретроспективою, на якій обговорюється, що можна було б зробити краще та вносяться корективи на наступну ітерацію.

Як висновок, у динамічних умовах вибір методології розробки спеціалізованого програмного забезпечення є надзвичайно важливим. Як показав досвід подібної розробки, існуючі підходи та методи управління життєвим циклом таких програмних систем не корелюють з умовами, в яких проводиться розроблення безпеко-орієнтованих сервісів, де окрім змінних вимог принципово важливим є час виконання.

Розроблена концептуальна модель процесу управління життєвим циклом спеціалізованого програмного забезпечення (безпеко-орієнтованих сервісів), є адаптованою під специфіку роботи Державної служби України із надзвичайних ситуацій та корелює із принципами гнучкої методології управління життєвим циклом програмного забезпечення.

В подальшому на її основі запропоновано розробити інформаційну систему підтримки прийняття рішень, щодо управління життєвим циклом розробки програмних систем безпеко-орієнтованого спрямування, що своєю чергою дасть змогу автоматизувати роботу проєктних команд та удосконалити процес розробки спеціалізованого програмного забезпечення безпекового спрямування.

Список використаних джерел:

1. Agile-маніфест розробки програмного забезпечення [Електронний ресурс] – Режим доступу до ресурсу: https://agilemanifesto.org/iso/uk/manifesto.html.
2. The Scrum Guide [Електронний ресурс] – Режим доступу до ресурсу: https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-US.pdf
3. Cole R., Scotcher E. Brilliant Agile Project Management: A Practical Guide to Using Agile, Scrum and Kanban. Edinburg: Pearson, 2015. 187 p.
4. Кордунова Ю. С., Придатко О. В., Смотр О. О. Переваги використання Agile- методології під час розробки програмного забезпечення в умовах сучасного ринку. Інформаційна безпека та інформаційні технології : зб. наук. праць IV Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів. м. Львів 27 листопада 2020 р. Львів, 2020. С. 206-207
5. Kordunova Y., Prydatko O., Smotr O., Golovatyi R. Expert Decision Support System Modeling in Lifecycle Management of Specialized Software. Lecture Notes in Data Engineering, Computational Intelligence, and Decision Making. ISDMCI 2022. Lecture Notes on Data Engineering and Communications Technologies, 149, https://doi.org/10.1007/978-3-031-16203-9_22

Катерина КОРОТКОВА
ВА ім. Євгенія Березняка
E-mail: korotkova_k@ukr.net

МЕДІАГРАМОТНІСТЬ ТА МЕДІАКОМПЕТЕНТНІСТЬ: ІНФОРМАЦІЙНА БЕЗПЕКА

Стрімкий розвиток інформаційних технологій значною мірою актуалізує проблематику інформаційно-психологічної безпеки в сучасних соціокультурних вимірах. Значна частина активності особистості в сучасному світі здійснюється у віртуальному просторі, а дискурс осягнення дійсності, що закладається впливом медіа, спрямовують найбільш загальні тенденції людського осмислення життя, вибору стратегій поведінки.

Особливої ваги така ситуація набула в Україні у контексті подій з 2014 року та загострення подій 24 лютого 2022 року, перебування в умовах повномасштабної війни, що поєднує у собі ознаки відкритого військового втручання та чітко спрямованої та агресивної інформаційної агресії. Спеціально використані країною-агресором технології маніпулювання суспільною свідомістю реалізуються саме у віртуальному просторі і значною мірою викривляють наявну у громадян нашої країни інформацію. Стрімке та всезагальне використання

інформаційних технологій додає медіа та віртуальному простору ознак інформаційно-психологічної небезпеки. У такому контексті єдиним засобом досягнення інформаційно-психологічної безпеки та благополуччя особистості виступає формування у неї медіаграмотності, спроможності усвідомлено фільтрувати та сприймати інформацію у віртуальному просторі та сфері медіа, приймати на цій основі психологічно виважені рішення, що не піддаються маніпулятивним впливам з боку країни-агресора чи інших кіберзагроз.

Тож проблема вивчення особливостей медіаграмотності особистості в контексті забезпечення інформаційно-психологічної безпеки в умовах повномасштабної війни, безумовно, є актуальною та потребує вирішення.

Як зауважує Л. Дорош [1, с. 110], реалізація інформаційної безпеки налічує три складові частини, такі як:

1) нормативно-правова, яка забезпечує формування та удосконалення системи правових норм, які закріплюють протидію загрозам інформаційно-психологічній безпеці та механізмам їх реалізації;

2) інституційна, що регулює становлення функціональної структури суспільних організацій та державних органів, які займаються реалізацією правових норм у цій сфері, та їх відносини як між собою, так і з громадянами;

3) технологічна, що забезпечує можливість вільного та безпечного інформаційного обміну між громадянами та соціальними групами.

У контексті проблеми, що розглядається, медіаграмотність постає у контексті реалізації принципів інформаційної безпеки особистості, залишаючи переважно поза увагою специфіку самого процесу формування медіаграмотності, що належить педагогічним дослідженням із даної теми.

Закономірно, що рівень медіаграмотності визначає спроможність особистості протистояти маніпуляціям у сфері медіа, що особливо актуально для нашої країни в умовах повномасштабної війни та агресії.

Як зазначає Д.О. Яровий [4, с. 309], усі наявні політичні групи інтересів з різним ступенем успішності використовують маніпулятивні технології для формування необхідної їм думки. Усі вони схильні до маніпулювання емоціями, перекручування фактів, використання частково правдивої інформації, використання символів і архетипів тощо.

Здійснення інформаційного впливу в умовах повномасштабної війни досягається за рахунок інформаційно-психологічних операцій. Ю. Мороз, Ю. Твердохліб [3, с. 102] зауважують, що сучасні війни є війнами нового, змішаного, поєднаного, “гібридного типу”, головною ознакою якого, окрім поєднання формальних і не формальних військових дій, є широке використання засобів інформації, інформаційно-психологічних операцій як специфічного застосування інформаційних та психологічних методів і технологій, спрямованого на досягнення мети військового конфлікту. Узагальнюючі різні наукові дефініції даного поняття, Ю. Мороз, Ю. Твердохліб визначають інформаційно-

психологічну операцію як комплекс заздалегідь спланованих, узгоджених та реалізований дій та заходів професійно підготовленими агентами держави-супротивника, що використовують для захоплення і забезпечення абсолютного контролю над свідомістю суспільства держави та здійснення подальших впливів на нього методом психологічних тисків і маніпуляцій із застосуванням істинної чи неправдивої інформації задля його дестабілізації, дезорієнтації та підготовки до проведення подальших політичних та воєнних дій.

Ю. Мороз, Ю. Твердохліб [3, с. 103] зауважують, що метою інформаційно-психологічних операцій виступає нав'язування своєї правди, її вкорінення у свідомість громадян, сіяння в них невпевненості у завтрашньому дні, примушення діяти не так, як раніше, підірвати довіру до уряду їх держави, довести психологічними засобами суспільство до стану готовності до здійснення бойових дій. Унаслідок успішно проведеної інформаційно-психологічної операції об'єкт стає повністю керованим агенту, що її проводить.

Медіаграмотність у такому випадку виступає як фільтр – оборонний засіб від різноманітних інформаційно шкідливих подразників, а наявність у населення ідеологічної соціокультурної свідомості – як наступальне знаряддя для формування проукраїнського суспільства і розвитку успішної держави.

В умовах повномасштабної війни та сучасного віртуального середовища загалом переважна частина інформаційного простору нашарована негативною, деструктивною, заангажованою, однобічною, спотвореною, неточною, неповною, нецілісною, невизначеною інформацією. Водночас людина сьогодні за день отримує стільки інформації завдяки засобам масових комунікацій і інтернет-технологіям, скільки людина покоління минулого століття за півжиття.

Тому формування в людини достатньо високого рівня медіаграмотності є необхідним та вагомим чинником інформаційно-психологічної безпеки.

Таку думку підтримує і О.В. Литвиненко [2, с. 260], зауважуючи, що засоби масової комунікації припиняють бути лише "сторонніми спостерігачами за подією" й починають самі виступати каталізаторами, а інколи й авторами ідеї щодо створення певної події. За таких умов виникає висока ймовірність порушення засадничих принципів інформаційної безпеки людини.

Прояви порушення інформаційно-психологічної безпеки в умовах повномасштабної війни актуалізують проблематику підвищення медіаграмотності населення, особливо молоді, зважаючи на її життєву невизначеність та залежність від медіа простору. Медіаграмотність особистості передбачає знання закономірностей сприйняття і розуміння інформації, психологічних аспектів впливу медіа на спосіб життя, стосунки та цінності особистості, використання ключових концепцій медіаосвіти для аналізу медіатекстів, тощо.

У гібридній війні широко застосовуються різноманітні маніпулятивні техніки у мас-медіа та кібернетичному просторі, що провокують в особистості асоціалізацію, засвоєння особистістю хибних норм і цінностей, нав'язаних

агресором для вироблення таких стереотипів поведінки, які б більше загострювали конфлікт і породжували деформацію системи суспільних відносин як у площині стосунків “особистість-суспільство”, так і в площині “особистість-держава”.

Разом із тим питання ролі медіаграмотності в забезпеченні інформаційної безпеки сучасної особистості залишається остаточно не вирішеним та потребує подальшого дослідження.

Список використаних джерел:

1. Дорош Л. Інформаційно-психологічна безпека особи, суспільства та держави: новітні виклики міжнародній безпеці. Українська національна ідея: реалії та перспективи розвитку. 2013. Вип. 25. С.107–112.
2. Литвиненко О.В. Медіаграмотність громадян у контексті гібридних воєн: приклад України. Молодий вчений. 2018. № 3(55). С. 259–263.
3. Мороз Ю., Твердохліб Ю. Інформаційно-психологічні операції в умовах ведення повномасштабної війни. Вісник Львівського Університету. Серія “Міжнародні відносини”. 2016. Вип. 38. С. 97–105.
4. Яровий Д.О. Конструювання громадянського протистояння як форми ескалації соціального конфлікту в Україні. Вісник Чернігівського національного педагогічного університету. Серія “Психологічні науки”. 2015. № 128. С. 307–311.

Тарас КРАВЕЦЬ, к.г.н., доцент
НАСВ ім. гетьмана Петра Сагайдачного
ORCID: 0000-0001-5398-7441
E-mail: taras-kravets@ukr.net

ПРОБЛЕМНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВИЩИХ ВІЙСЬКОВИХ НАВЧАЛЬНИХ ЗАКЛАДІВ

В сучасному світі інформаційна безпека стала однією з найактуальніших та найбільш складних проблем, які стоять перед вищими військовими навчальними закладами. З появою цифрових технологій і швидким розвитком інформаційних систем, інформаційна безпека стала невід'ємною частиною нашого сучасного життя. Це особливо важливо для військових навчальних закладів, оскільки вони відіграють важливу роль у підготовці кадрів для збройних сил та у забезпеченні національної безпеки країни.

У дослідженні ми розглянули проблемні питання, пов'язані з інформаційною безпекою вищих військових навчальних закладів та виклики, які вони зустрічають у сфері збереження та захисту конфіденційної інформації, використання сучасних інформаційних технологій в навчальному процесі, а також забезпечення

кібербезпеки курсантів і викладачів. Ми також розглянули важливість співпраці між вищими військовими навчальними закладами і військовими організаціями у сфері інформаційної безпеки та обміну досвідом.

Питання інформаційної безпеки не тільки впливають на ефективність навчання та підготовку військових фахівців, але й мають стратегічне значення для забезпечення національної безпеки та обороноздатності. Для вищих військових навчальних закладів ця проблема стала викликом, який потребує уважного аналізу, пошуку ефективних рішень та постійного вдосконалення підходів до забезпечення інформаційної безпеки. Ми розглянули ключові аспекти цієї проблеми та намагатимемося знайти відповіді на актуальні питання, пов'язані з інформаційною безпекою вищих військових навчальних закладів.

У зв'язку зі стрімким розвитком інформаційних технологій і постійними загрозами кібербезпеці, вищі військові навчальні заклади стикаються з низкою проблемних питань, які вимагають негайного вирішення та системного підходу. Основні з цих проблем включають: захист конфіденційної інформації: Однією з ключових функцій військових навчальних закладів є збереження та передача конфіденційної інформації. Важливо розробити та впровадити надійні системи криптозахисту, контролю доступу та моніторингу, щоб уникнути витоку важливих даних. Кібербезпека: Зараз військові навчальні заклади активно використовують цифрові технології у навчальному процесі. Це створює загрозу для кібербезпеки, оскільки цільовими об'єктами можуть стати як курсанти чи викладачі, так і інфраструктура навчальних закладів. Розробка та впровадження стратегій кіберзахисту є надзвичайно важливою задачею. Підготовка персоналу: Кадровий потенціал вищих військових навчальних закладів повинен бути належним чином підготовлений до вирішення завдань інформаційної безпеки. Необхідно забезпечити навчання та підвищення кваліфікації фахівців у сфері кібербезпеки та інших аспектів інформаційної безпеки. Міжнародне співробітництво: У сфері інформаційної безпеки важливо прагнути до співробітництва з іншими військовими навчальними закладами та організаціями, які займаються проблемами кібербезпеки. Обмін досвідом та інформацією може сприяти більш ефективному реагуванню на загрози. Засоби та обладнання: Важливо забезпечити вищі військові навчальні заклади сучасними засобами та обладнанням для виявлення та запобігання кібератакам і для здійснення кіберзахисту. Правова база: Наявність чіткої та актуальної правової бази для регулювання питань інформаційної безпеки також має велике значення. Необхідно враховувати законодавчі норми та регуляції, які стосуються збереження та обробки інформації військового значення.

На основі цього можна запропонувати основні рекомендації щодо забезпечення інформаційної безпеки вищих військових навчальних закладів:

розробка імовірних сценаріїв загроз: Важливо провести аналіз імовірних загроз для вищих військових навчальних закладів і розробити сценарії подій, щоб мати можливість вчасно реагувати на кібератаки, витоки інформації і інші загрози;

системи контролю доступу: Забезпечте впровадження надійних систем контролю доступу до конфіденційної інформації, що обмежують доступ лише до авторизованих користувачів;

кібернавчання: Організація системи навчання та інструктажів з кібербезпеки для всього персоналу і студентів. Підвищення обізнаності та навичок у сфері кібербезпеки допоможе зменшити ризики;

аудит інформаційної безпеки: Проведення регулярних аудитів інформаційної безпеки для виявлення слабких місць і вразливостей у системах та процесах;

реагування на інциденти: Розробка плану реагування на кіберінциденти, який включає в себе кроки щодо виявлення, зупинки і відновлення роботи після інциденту;

захист мережі і інфраструктури: Застосування сучасних технології захисту мережі, такі як мережеві брандмауери, антивірусні програми і системи виявлення вторгнень;

шифрування даних: Застосування шифрування для захисту конфіденційної інформації в пересиланні та зберіганні.

регулярні оновлення та патчі: Постійне оновлення програмного забезпечення та системи, встановлюючи патчі для вирішення відомих вразливостей;

міжнародне співробітництво: Активна співпраця з іншими вищими навчальними закладами і організаціями в галузі кібербезпеки для обміну досвідом та інформацією щодо нових загроз і технологій;

створення культури інформаційної безпеки: Залучення всіх співробітників і курсантів до процесу забезпечення інформаційної безпеки, формуючи в них свідоме ставлення до цього питання.

Отже забезпечення інформаційної безпеки вищих військових навчальних закладів вимагає постійної уваги, ресурсів та координації зусиль. Реалізація цих рекомендацій допоможе зменшити загрози та підвищити рівень захисту конфіденційної інформації та інфраструктури закладів. Інформаційна безпека вищих військових навчальних закладів є надзвичайно важливою та актуальною проблемою, яка вимагає системного та постійного підходу. Сучасний світ, населений інформаційними технологіями, несе як безліч можливостей, так і загроз, і важливо готувати наступне покоління військових фахівців до ефективного управління цими ресурсами та захисту від загроз.

Ми надали огляд ключових проблем, пов'язаних із забезпеченням інформаційної безпеки в цих навчальних закладах, і запропонували конкретні рекомендації щодо їх вирішення. Ці рекомендації включають в себе розвиток культури інформаційної безпеки, підвищення обізнаності персоналу та студентів, застосування сучасних технологій захисту інформації, та співпрацю з іншими військовими та навчальними організаціями.

Інформаційна безпека є невід'ємною частиною забезпечення національної безпеки та обороноздатності країни, і вищі військові навчальні заклади відіграють

ключову роль у цьому процесі. Маючи на увазі ростучу складність та різноманітність інформаційних загроз, нам слід постійно адаптуватися та вдосконалювати свої підходи до забезпечення інформаційної безпеки, щоб зберегти нашу національну безпеку і захистити конфіденційні дані та ресурси вищих військових навчальних закладів.

Список використаних джерел:

1. Smith, John A. “Cybersecurity in Higher Education: A Review of Modern Challenges and Trends.” International Journal of Cybersecurity Education, Research, and Practice, vol. 2, no. 1, 2019, pp. 25-40.
2. Jones, Emily B. “Information Security Management in Higher Education: Current Practices and Future Trends.” Journal of Higher Education Technology Research, vol. 18, no. 3, 2020, pp. 187-204.
3. Anderson, James R., and Karen L. Williams. “Cybersecurity in Military Education: Challenges and Strategies.” Journal of Military and Strategic Studies, vol. 19, no. 3, 2020, pp. 53-74.

Сергій КУЛІБАБА
ORCID: 0000-0002-7316-1214
E-mail: kulibseryyy@gmail.com
Юрій ЩЕБЛАНІН, к.т.н., с.н.с.
ORCID: 0000-0002-3231-6750
E-mail: sheblanin@ukr.net
Олег КУРЧЕНКО, к.т.н, доцент
КНУ ім. Тараса Шевченка
ORCID: 0000-0002-3507-2392
E-mail: kurol@ukr.net

ОБРОБКА ВИХІДНОГО КОДУ ДЛЯ ЗАХИСТУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ

Сучасні технології наразі стрімко розвиваються. За рахунок різноманітних мов програмування та бібліотек даних, які призначені для розробки програмного забезпечення, можна створити інноваційну модель, яка вирішуватиме ряд проблем вихідного коду. Вихідний код можна перетворити у виконуючий файл, який може виконувати збірку компонентів незалежно від встановлених компонентів системи користувача.

Для забезпечення безпеки даних, які передаються по відкритій мережі, можуть застосовуватись різноманітні методи їх захисту. Як для прикладу, можуть

використовуватись симетричні або асиметричні методи шифрування, а також хеш-функції [1]. Робиться це для того, щоб зменшити ймовірність успішного отримання дійсних даних зловмисником, або для зменшення ймовірності компрометації системи.

Ряд компаній можуть обробляти дані певним чином, зокрема вихідний код застосунків для забезпечення безпеки конфіденційної інформації або захисту інтелектуальної власності. Додатковим способом підвищення рівня захисту даних може бути застосування методів обфускації до вихідного коду застосунку. Обфускатор – зміна структури вихідного коду або проекту за певними алгоритмами [2, 3]. Існуючі застосунки перетворення вихідного коду можуть проводити обробку за різними методами, але без можливості деобфускації. Відсутність деобфускації змушує зловмисника витрачати більше часу для аналізу коду, щоб виявити вразливості та експлуатувати їх. Але іноді може бути так, що необхідно надати даним високий рівень безпеки із можливістю отримання оригінальних даних – дешифрувати та деобфускувати дані. На сьогоднішній день наявна обмежена кількість програмних рішень спроможних реалізувати обробку вихідного коду із забезпеченням технологій обфускації та деобфускації. Аналогічна ситуація склалася і з мовами програмування спроможними вирішити дане завдання [4]. Так, наприклад, для мови Python відсутнє єдине рішення.

Мета роботи полягає у розробці алгоритму обфускації вихідного коду на мові Python із можливістю деобфускації, який може застосовуватись для досягнення різних цілей. Такий підхід дозволить забезпечити безпеку даних, які передаються по локальній мережі, а також захистити інтелектуальну власність розробника програмного забезпечення.

Для цього необхідно знайти усі зв’язки, завдяки яким може проводитись глибокий аналіз проекту розробки застосунку. В роботі проаналізовано та визначено наступні інформаційні зв’язки:

1) папки та файли;
2) класи;
3) методи;
4) змінні та їх значення;
5) коментарі.

Папки та файли. Так, як проект складається із папок та файлів, то вони можуть підлягати аналізу працездатності та принципу роботи як в загалом певного проекту.

Класи. Класи являються сукупністю інших об’єктів, які можуть виконувати різні задачі застосунку.

Методи. Метод може бути як і клас – виконувати відповідну задачу.

Змінні та значення. Такі об’єкти вважаються надзвичайно важливими, адже завдяки ним можна керувати потоком виконання програми. Також змінні можуть вміщати в собі деяку конфіденційну інформацію.

Коментарі. Розробники залишають коментарі у вихідному коді, щоб орієнтуватись у подальшому, що виконує відповідна частина. Також коментарі можуть бути в нагоді іншим розробникам.

На рисунку 1 наведено зв’язки між загальною структурою умовного проекту розробки застосунку. Дана схема допомагає зрозуміти, наскільки важливим є врахування усіх деталей до обробки вихідного коду для забезпечення безпеки.

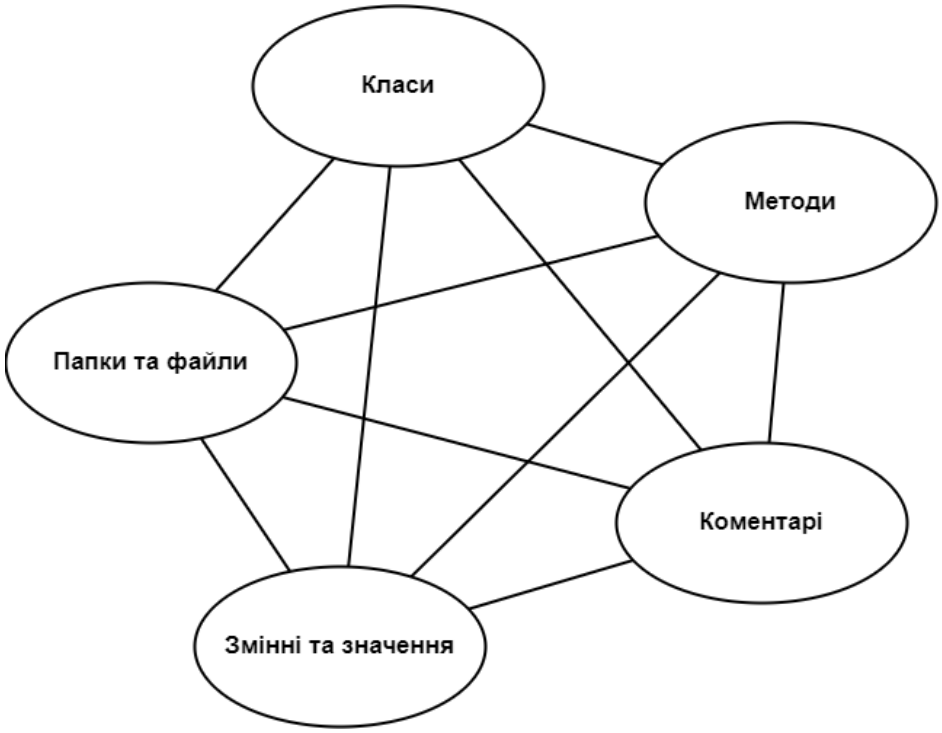


Рисунок. 1. Зв’язки між загальною структурою проекту по розробці застосунку

Можна помітити, що усі компоненти пов’язані між собою, тому необхідним є обфускація усіх даних, які можуть належати до проекту. Утворюється гіпотеза, що кожен зв’язок складає 25% інформації.

Таким чином, якщо зловмисник буде обробляти усі зв’язки однаковим алгоритмом, то йому знадобиться значно менше часу, щоб отримати усі дані в оригінальному форматі. Тому застосунок має реалізувати технологію обробки кожного зв’язку за окремим алгоритмом.

Списки використаних джерел:

1. S. Koteshwara, C. H. Kim and K. K. Parhi, “Functional encryption of integrated circuits by key-based hybrid obfuscation,” 2017 51st Asilomar Conference on Signals,

Systems, and Computers, Pacific Grove, CA, USA, 2017, pp. 484-488, doi: 10.1109/ACSSC.2017.8335386.

2. Finn Brunton; Helen Nissenbaum, “Understanding Obfuscation,” in Obfuscation: A User's Guide for Privacy and Protest, MIT Press, 2015, pp.44-44.

3. Serhii Kulibaba, Svitlana Popereshnyak, Yurii Shcheblanin, Oleg Kurchenko and Nataliia Mazur. Advanced Communication Model with the Voice Control and the Increased Security Level. CPITS-2022: Cybersecurity Providing in Information and Telecommunication Systems, October 13, 2022, Kyiv, Ukraine. SEUR-WS.org, vol 3288. pp. 64-72.

4. R. Guo, Q. Liu, M. Zhang, N. Hu and H. Lu, “A Survey of Obfuscation and Deobfuscation Techniques in Android Code Protection,” 2022 7th IEEE International Conference on Data Science in Cyberspace (DSC), Guilin, China, 2022, pp. 40-47, doi: 10.1109/DSC55868.2022.00013.

Володимир ПОЛЕВИЙ
НУОУ
ORCID: 0000-0001-9212-2475
E-mail: v.polevyi@edu.nuou.org.ua
Ярослав ЛАШИН
НУОУ
ORCID: 0009-0008-3025-7890
E-mail: y.lashin@edu.nuou.org.ua
Лілія ТЮТЮННИК, д.ф.
НУОУ
ORCID: 0000-0001-8480-0475
E-mail: l.tiutiunnyk@edu.nuou.org.ua

РЕКОМЕНДАЦІЇ ЩОДО РОЗВИТКУ СПРОМОЖНОСТЕЙ ЗІ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ЩОДО ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ УКРАЇНИ

В результаті проведеного дослідження щодо обґрунтування пріоритетних напрямів (заходів) розвитку спроможностей сил оборони (СО) зі стратегічних комунікацій, у той час – щодо європейської інтеграції України, було сформульовано наступні рекомендації:

спроможності СО мають бути описані у формі ефектів, спрямованих на зміну характеристик об’єкту впливу;

базова вимога буде відображати основну вимогу, мету спроможності (який вплив ми очікуємо?). Основні вимоги – ефекти, які нам необхідно досягнути для досягнення впливу і які їх ключові показники (як і з якою

метою ми змінюємо характеристики об'єкту впливу?). Додаткові вимоги – перелік дій і процесів з визначеними результатами, спрямовані на досягнення ефектів (що ми для цього робимо і з яким результатом?);

при плануванні розвитку спроможностей слід урахувати широке коло неврахованих сьогодні точок контакту, які мають бути синхронізовані зі загальними наративами стратегічних комунікацій;

каталог спроможностей СО містить низку спроможностей, які стосуються сфери комунікацій СО. Зазначені спроможності не систематизовані та не об’єднані в підгрупу/типову групу та єдиним задумом;

існуючі спроможності у сфері стратегічних комунікацій слід поєднати у окрему типову групу спроможностей С2-4. “Стратегічні комунікації” (ФГС №3 “Командування та управління” (Command & Control або С2), окремі спроможності якої мають залишитися в структурі своїх функціональних груп;

кожна окрема спроможність потребує уточнення в частині носіїв цієї спроможності, з урахуванням їх рівня управління (стратегічний, операційний, тактичний);

синхронізація комунікацій, яка є частиною військового лідерства та суттю стратегічних комунікацій, може бути описана у вигляді окремої спроможності С2-4.1.1. “Здатність синхронізувати комунікаційні та кінетичні заходи”;

існуючі комунікаційні спроможності варто сформулювати чіткіше, з акцентом на бажану зміну характеристики об’єкту.

Пропонується наступний перелік спроможностей зі впливу на визначені цільові аудиторії:

здатність формувати підтримку дій СО;

здатність переконувати вступити до лав СО;

здатність підтримувати високий бойовий дух військовослужбовців;

здатність синхронізувати комунікаційні та кінетичні заходи;

здатність впливати на рішення і дії ворога некінетичними засобами.

Спроможності реалізовують шляхом здійснення процесів. Кожна зі зазначених вище спроможностей має містити чіткий перелік процесів, які спрямовані на досягнення необхідного ефекту та впливу. Розвиток конкретної спроможності може розглядатися як окремий проєкт. Сукупність проєктів складає програму проєктів. Так, сукупність проєктів зі розвитку спроможностей стратегічних комунікацій можуть бути об’єднані у програму.

Список використаних джерел:

1.Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» Указ Президента України № 392/2020 від 14 вересня 2020 року. Ресурс доступу: https://zakon.rada.gov.ua/laws/card/121/2021#doc_info

2. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року “Про Стратегію воєнної безпеки України” [Електронний ресурс]:, Указ Президента України № 121/2021 від 25 березня 2021 р. Ресурс доступу: https://zakon.rada.gov.ua/laws/card/121/2021#doc_info

3. Розвиток теоретичних основ удосконалення системи стратегічних комунікацій у Міністерстві оборони України та Збройних Силах України Звіт про НДР(остаточний) / НУОУ – К., 2021. – 252 с.

Андрій ЛОЗОВЕНКО
НУОУ
ORCID: 0009-0008-6899-5442
E-mail: a.lozovenko@i.ua

АНАЛІЗ ФАКТОРІВ, ЯКІ ВПЛИВАЮТЬ НА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ

Сьогодні одним із найбільш актуальних завдань в інформаційно-аналітичному забезпечені заходів інформаційної безпеки Міністерства оборони України є швидкості та якості обробки й аналізу великих обсягів структурованих і неструктурованих даних в інтересах інформаційної безпеки Збройних Сил України.

Ґрунтовні зміни у зовнішньому та внутрішньому безпековому середовищі держави, а також вочевидь довготривалий характер російської загрози вимагають здійснення докорінного перегляду, а швидше – створення абсолютно нової системи забезпечення інформаційної безпеки.

Аналіз джерел [1, 2] показав, що до пріоритет інформаційної безпеки Збройних Сил України став ключовим, а комплексне реформування системи забезпечення національної безпеки та створення ефективного сектора безпеки і оборони стає життєво необхідним завданням української держави.

Зважаючи на це, питання щодо забезпечення інформаційної безпеки є одним із основних у системі забезпечення національної безпеки, якому, разом із питаннями державної та зовнішньополітичної безпеки, у найближчій перспективі мають підпорядковуватися питання, що стосуються економічної, енергетичної, інформаційної, науково-технологічної, екологічної та інших складових національної безпеки держави.

Слід зазначити, що інформаційна безпека Міністерства оборони України не може розглядатися окремо від інших складових національної безпеки, які тісно пов’язані та доповнюють одна одну. Крім того, інформаційна безпека Міністерства оборони України не може бути забезпеченою за слабкої та

неефективної економіки, так само не може одночасно повною мірою забезпечуватися економічна і воєнна безпека в державі, що має суспільні конфлікти.

Під інформаційна безпека Міністерства оборони України розуміють реалізованість життєво важливих національних інтересів держави у воєнній сфері для забезпечення гарантій захисту країни від воєнних загроз, збройної агресії та інших посягань із застосуванням військової сили [2].

Проведений аналіз свідчить про те, що інформаційна безпека Міністерства оборони України має внутрішній і зовнішній аспекти:

зовнішній аспект інформаційної безпеки Міністерства оборони України відображає спроможність стримувати воєнну силу ззовні або протистояти їй. Така спроможність передбачає наявність сучасних та професійних збройних сил, національної та колективної системи безпеки, воєнно-політичних союзів. Найбільш дієвим способом збереження та зміцнення воєнної безпеки є формування загальної та всеосяжної міжнародної безпеки на принципах рівноправності, однакової безпеки та взаємної співпраці всіх її учасників;

внутрішній аспект інформаційної безпеки Міністерства оборони України охоплює систему заходів, спрямованих на створення й підтримку готовності громадянина, суспільства й держави до попередження й відвернення воєнних загроз шляхом забезпечення стабільного функціонування воєнної організації держави, здійснення мобілізаційної підготовки населення й економіки держави.

Нормативно-правова база в сфері інформаційної безпеки Міністерства оборони України потребує удосконалення шляхом проведення виваженої державної політики згідно з прийнятими доктринами, стратегіями, концепціями і програмами у різних сферах діяльності держави.

Тому інформаційна безпека Міністерства оборони України досягається шляхом реалізації воєнної політики, засади якої визначаються у Стратегії воєнної безпеки України як системі керівних поглядів на причини виникнення, сутність і характер сучасних воєнних конфліктів, принципи і шляхи запобігання їм, підготовку держави до можливого воєнного конфлікту, а також на застосування воєнної сили для захисту державного суверенітету, територіальної цілісності, інших життєво важливих національних інтересів.

Зазвичай, можна виокремити фактори, що негативно впливають на інформаційну безпеку Міністерства оборони України:

розбалансованість і незавершеність системних реформ у сфері інформаційної безпеки;

неефективність системи програмно-цільового планування їх розвитку, ухвалення управлінських рішень на всіх рівнях державної влади;

Отже, головною метою забезпечення заходів інформаційної безпеки Міністерства оборони України є набуття інформаційної переваги над

противником, а рівень інформаційної безпеки критерієм ефективності реалізації воєнної політики держав.

Список використаних джерел

1. Микусь А.С., Кацалап В.О., Войтко О.В. “Інформаційні технології інформаційно-аналітичного забезпечення органів управління військами (силами)”, НУОУ ім. І. Черняховського, Київ, 2020.

2. Open-Source Intelligence (ATP 2-22.9) July 2012. Headquarters, Department of the Army.

Людмила МАЗУРЕНКО, к.пол.н.
ІВМС НУ Одеська морська академія”
ORCID: 0000-0003-3189-8215
E-mail: ruzam11_@ukr.net

ІНФОРМАЦІЙНА БЕЗПЕКА ГРОМАДЯНИНА В УМОВАХ ВОЄННОГО СТАНУ: ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ

В умовах воєнного стану захист суспільства від деструктивного інформаційного впливу з боку держави-агресора та ряду терористичних організацій є першочерговим завданням.

Негативні явища інформаційного характеру ставлять під загрозу основні принципи забезпечення безпеки громадян, в основі яких лежать чинні норми права. І тому основним завданням державної політики безпеки в інформаційній сфері є забезпечення мов для надання кожному громадянину права на інформаційну безпеку.

Інформаційну безпеку громадянина як поняття можливо розглядати в сукупності із національною, державною та суспільною інформаційної безпекою. Таку класифікацію наведено в праці Золотар О.О.[1], де головну роль відіграє саме інформаційна безпека людини. Ряд статей Конституції (50, 31, 34, 32) вказує на гарантії права на поширення усної інформації; захисту від поширення не достовірної інформації; захист від втручання в приватне життя і таємницю листування, кореспонденцію; можливість судового захисту права не спростовувати не досвідну інформацію, а також вимагати її вилучення; права на доступ до публічної інформації[2]. Норми Основного Закону України гарантують належне забезпечення інформаційної безпеки громадянського суспільства, але поняттю інформаційної безпеки громадянина або людини не приділено достатньо уваги в інших нормативно-правових документах, що призвело до безсистемності українського законодавства у сфері інформаційної

безпеки особистості. Нині його базові положення належать до інформаційної безпеки держави та суспільства загалом.

Так, Правдюк А.Л. визначає поняття інформаційної безпеки громадянина як стан захищеності особистості від інформаційних загроз, ризиків та небезпек[3]. Інформаційну безпеку громадянина як складову системи забезпечення інформаційної безпеки держави подає в своїх працях Г. Сащук[4]. Одним із трьох класифікаційних видів інформаційної безпеки О.О. Золотар виділяє інформаційну безпеку громадянина[5]. Проте питання інформаційної безпеки громадянина висвітлюються недостатньо.

Потребує юридичного уточнення рівень обмеження прав і законних інтересів громадян в інформаційній сфері під час воєнного стану, що передбачені ч. 1 ст. 8 Закону України "Про правовий режим воєнного стану" [6]. Є потреба уточнити види персональної інформації в період дії воєнного стану, покликана необхідністю розпізнавання агентів ворога. Об'єктами інформаційної безпеки визначено громадян, державу та суспільство. Елементами інформаційної безпеки громадян є їхні права та свободи, що гарантуються Конституцією. Отже, в чинному законодавстві України інформаційна безпека громадянина трактується в широкому розумінні та охоплює майже всі аспекти діяльності держави.

Але ж використання законодавчих норм в інформаційній сфері для громадян не можуть повністю діяти у воєнний час тому, що пріоритети в боротьбі із загрозами зміщуються до захисту держави, її територіальної цілісності, незалежності та державних інтересів. Тому інформаційна безпека громадянина під час воєнного стану зумовлена особливими обставинами. Громадяни отримують право захищати країну будь-яким способом, хоча при цьому проводяться заходи правового режиму воєнного стану, що регламентує ст. 8 Закону України "Про правовий режим воєнного стану". Деякі його норми можуть обмежувати конституційні права громадян, що пов'язані з їх інформаційною безпекою. Так, конституційні права, передбачені статтями 31, 32, 34, 41 та іншими, що стосуються інформаційної безпеки громадян, у воєнний час можуть не діяти тому, що під час війни надання переваги інтересам держави допоможе повніше забезпечити основні права громадян через підтримку державної безпеки. Окремо варто визначити загрози кібербезпеці громадян, оскільки сучасні війни ведуться не тільки на землі, в повітрі та на морі, а й в інформаційній сфері і в кіберпросторі. Коли бойові дії точаться на полі бою і атаки ворога приймають на себе силові структури, загрози кібербезпеки безпосередньо стосуються кожного громадянина, який користується цифровими технологіями, які під'єднані до глобальної мережі Інтернет.

Хоча ряд нормативних положень, що регламентують безпеку громадян у кіберпросторі були розроблені в період мирного часу, то вже в перші місяці

війни в нашій країні було оптимізовано кримінально-процесуальне законодавство, а саме вдосконалено механізми притягнення до відповідальності кіберзлочинців. До того ж, Закон України "Про основні засади забезпечення кібербезпеки України"[7] спрямований на забезпечення ефективного застосування ЗСУ для належної відповіді кіберзагрозам у системі державної безпеки. Роль інформаційної безпеки особистості, що закріплена рядом конституційних норм, таких, як свобода пересування, право на отримання інформації, свобода висловлювань, обмежуються на період дії воєнного стану. Як бачимо, інформаційна безпека громадян не зникає, а тільки змінює норми поведінки органів державного управління враховуючи воєнні реалії.

Таким чином, під час дії воєнного стану інформаційна безпека громадянина суттєво змінюється, тоді вона спрямована більше не на захищеність його особистих прав, а на першочерговий захист саме держави, її територіальної цілісності та незалежності в цей період.

Список використаних джерел:

1. Золотар О.О. Класифікація інформаційної безпеки. *Інформація і право*. 2011. № 2(2). С. 109-113.
2. Конституція України. Верховна Рада України. Офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/print (дата звернення: 17.09.2023).
3. Правдюк А.Л. Конституційні гарантії інформаційної безпеки людини і громадянина. *Юридичний науковий електронний журнал.* 2021. № 12. С. 303-305.
4. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.
5. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: ТОВ "Видавничий дім "АртЕк", 2018. 446 с.
6. Закон України "Про правовий режим воєнного стану". Верховна Рада України. Офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/389-19/print (дата звернення: 17.09.2023).
7. Закон України "Про основні засади забезпечення кібербезпеки України". Верховна Рада України. Офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/2163-19/print (дата звернення: 17.09.2023).

Олена МАРЦИНКЕВИЧ
ЖВІ ім. С.П. Корольова
ORCID: 0009-0003-0903-9286
E-mail: marcunkevich02@ukr.net

ІНФОРМАЦІЙНИЙ ВПЛИВ НА УКРАЇНУ ПІД ЧАС ПОВНОМАСШТАБНОЇ ВІЙНИ: АНАЛІЗ ТА СТРАТЕГІЇ ПРОТИДІЇ

Питання інформаційної війни, стала невід'ємною складовою повномасштабних конфліктів між державами. Україна, яка переживає повномасштабну війну на своїй території, не залишається осторонь від цього явища. Під час конфлікту Україна стикається із серйозним негативним інформаційним впливом (ІВ), який суттєво впливає на суспільство, політичну ситуацію та загальний стан безпеки в країні. ІВ іноземних джерел може бути різним за своїм характером: позитивним, нейтральним або негативним. На жаль, Україна стикається зі значним обсягом негативної інформації з-за кордону, особливо у зв'язку зі складною політичною ситуацією, майже, по всій країні.

Основні джерела негативної інформації - це медіа, соціальні мережі та впливові особистості, які активно використовують інформаційний простір (ІП) для розпалювання конфліктів і дестабілізації ситуації в Україні. Цей тиск здійснюється як із боку Російської Федерації, так і з боку окремих держав світу, зокрема США, Німеччини, Великої Британії, Франції, а також і від суміжних з Україною держав, насамперед Польщі, Угорщини, Румунії. Безперечно, найбільший вплив на населення України здійснюють медіа Росії, які зосередили протягом останніх десятиліть свої зусилля на послабленні позицій України на світовому ринку.

Головна мета психологічного впливу полягає у впливі на установки особистості та використанні маніпуляцій для впровадження цілеспрямованої дезінформації. Мешканці тимчасово окупованих територій щодня зазнають великих обсягів дезінформації, призначеної переконати їх у "агресивності", “недемократичності” та “нелюдяності” легітимної влади в Україні.

Зі сторони західних держав, не зважаючи на їх беззаперечну підтримку України в її боротьбі за незалежність проти російського агресора, зокрема потужну медіапідтримку, також спостерігається достатньо відчутний негативний психологічний тиск переважно щодо впливу на розвиток суспільно-політичної ситуації в нашій країні та просування окремими державами власних інтересів у міждержавних відносинах. Негативна інформація щодо України в західних медіа, насамперед США, Великобританії, Франції та Німеччини, поширюється переважно у контексті жорсткої критики ходу проведення в Україні внутрішньополітичних реформ та боротьби з корупцією. Водночас

медіа багатьох країн-членів ЄС, зокрема тієї ж Німеччини, Іспанії, Італії, Австрії, Греції та ряду інших, тиражують інформацію з невдоволенням від негативних наслідків західних санкцій проти Росії для економік зазначених країн.

Можна зазначити, що медіа є найбільш ефективними засобами для здійснення ПсВ на великі групи людей. Також за допомогою телебачення часто відбувається маніпулювання даними, це проявляється в несприйнятті актуально важливої інформації через маскування сигналу, відволікання уваги, перевищення значень пропускної здатності прийому інформації людиною. Ще на сьогодні, великою популярністю користуються соціальні мережі. За останні роки соціальні мережі стали майже невід'ємною частиною нашого життя та здійснюють значний вплив на економічну та соціально-політичну складову сучасного суспільства. Більшість людей, користується соціальними мережами для спілкування та в розважальних цілях, але не зважають на великий ризик потрапити під матеріал ПсВ агресора. Щоб успішно протистояти інформаційному впливу, Україні необхідно розробити комплексну стратегію, яка об'єднає зусилля державних органів, громадськості та міжнародної спільноти. Розвиток незалежних медіа, моніторинг і аналіз дезінформації, міжнародна співпраця та підвищення інформаційної грамотності громадян є ключовими компонентами успішної боротьби з впливом агресора.

Україна має потенціал для успішної протидії інформаційному впливу та збереження своєї інформаційної незалежності. Проактивний підхід до протидії дезінформації, розвиток сильних і незалежних медіа, залучення громадськості та міжнародних партнерів допоможуть підвищити національну безпеку та стійкість України перед інформаційною агресією. Інформаційна війна на Україну підкреслює важливість захисту національного інформаційного простору та підсилює необхідність розвитку інформаційної грамотності та свідомості громадян для ефективної боротьби з цим впливом. Спільними зусиллями Україна зможе зберегти свою інформаційну незалежність та захистити свої національні інтереси у складному інформаційному середовищі.

Список використаних джерел:

1. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія /.Левченко О. В. – Житомир : Видавець ПП "Євро-Волинь", 2021. – 172с.

2. URL:https://dnipr.kyivcity.gov.ua/files/2016/3/22/vpliv.pdf(дата звернення: 17.09.2023).

Сергій НУЖНИЙ, к.т.н., доцент
НУК ім. адмірала Макарова
ORCID: 0000-0002-7706-0453
E-mail: s.nuzhniy@gmail.com

УДОСКОНАЛЕННЯ ПРИНЦИПІВ ПОБУДОВИ СИСТЕМ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ МОВОПОДІБНИХ ЗАВАД

Анотація: В Україні та інших країнах білий шум використовуються для активних систем постановки завад в каналах витоку мовної інформації. Однак, такі системи мають ряд суттєвих недоліків, що дозволяє зловмисникам перехоплювати конфіденційну /таємну інформацію. Запропоновано структуру системи захисту мовної інформації (СЗМІ) на базі генератора завад скремблерного типу. Перехід в СЗМІ до такої структури дозволяє відмовитися від енергетичного зашумлення мовної інформації та перейти до енерго-інформаційного маскування. Аналіз такого типу завад показує їх високу стійкість до сучасних методів математичної обробки цифрових фонограм, фільтрації завад, реінжинірингу та виділення голосів дикторів. Запропоновано вдосконалену методику оцінювання рівня захищеності мовної інформації, що враховує можливість застосування зловмисниками сучасних методів цифрової обробки сигналів.

Ключові слова: Захист мовної інформації, постановка активної завади, мовоподібний сигнал.

Вступ: Мова є найбільш уживаним засобом обміну інформацією. При цьому озвучується інформація обмеженого доступу – конфіденційна (військова, політична, економічна, організаційна, know-how та інша), а в багатьох випадках, і таємна інформація. Існуючі в Україні, та й в більшості країн світу, СЗМІ засновані на використанні систем постановки активних завад (СПАЗ) в акустичному та вібраційному каналах витоку інформації. Основою таких систем є генератор сигналу завади. Згідно нормативних документів, в Україні це виключно генератори “білого” шуму або його “кольорові” клони [1]. Однак, на даний час, таке рішення є застарілим і не забезпечує необхідного рівня захищеності інформації. В роботі розглянуто особливості побудови та функціонування СЗМІ, а також запропоновано рішення, яке дозволяє розробляти більш ефективні системи захисту мовної інформації.

Аналіз літературних джерел та постановка проблеми: Технології виявлення та розпізнавання мови диктора в останні десятиріччя отримала новий імпульс. Це зумовлено декількома факторами:

- Широким використанням цифрових технологій для запису та обробки фонограм.
- Використання цифрових фонограм в системах ідентифікації та контролю доступу.
- Перехід на цифрові технології в радіозв’язку та телефонії.

• Використання цифрових методів та технологій фільтрації завад та покращення якості цифрових фонограм.

Найбільш актуальними загрозами є:

• Можливість виявлення зловмисником наявності мови в фонограмі.

• Фільтрація зловмисником сигналу завади та розпізнавання мови диктора (отримання несанкціонованого доступу до лінгвістичної складової фонограми).

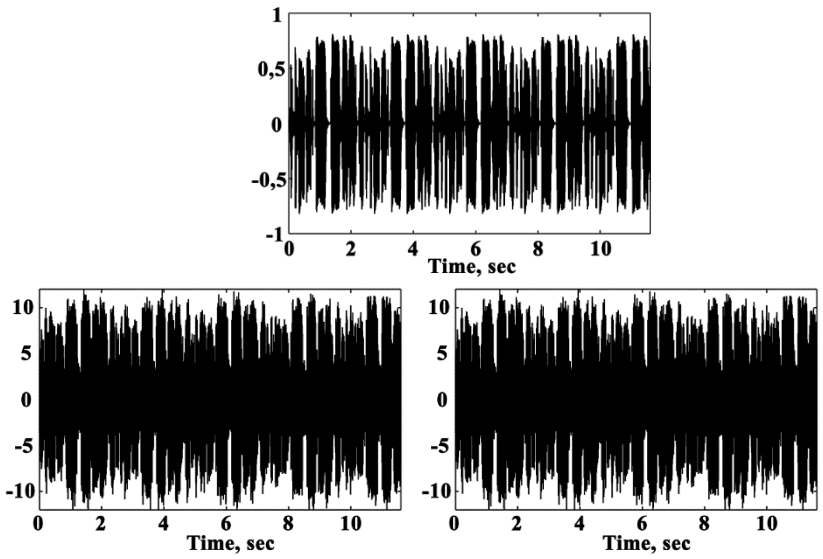
• Ідентифікація зловмисником дикторів за особливостями їх мовлення по фонограмі/перехопленій розмові.

Мета дослідження: Метою дослідження є розробка нових/удосконалення існуючих методу та технології створення СЗМІ від витоку акустичними та вібраційними каналами за межі контрольованої зони з урахуванням об'єктивних та суб'єктивних факторів.

Система постановки активних завад: Аналіз сучасних методів та технологій виявлення і відновлення мови диктора при значних рівнях шумових завад (як типу білий (гаусовий) шум та і при використанні завад типу "мовний хор" / "cocktail party") показує їх високу ефективність. Одночасно, це показує низьку ефективність методів та технологій, які є нормативними на даний час, а також недоліки методів визначення рівня захищеності мовної інформації [2,3].

Дослідження моделі СЗМІ: Моделювання СЗМІ виконано у середовищі Matlab 15 R2015a/Simulink [2,3]. При моделюванні використано спрощену структурну схему каналу поширення акустичної/вібраційної інформації – розглянуто випадок з одним диктором, коефіцієнт загасання сигналу прийнятий рівним 1, а фонові шуми не враховуються. Так само, за аналогією з [3], в генераторі шуму речоподібного не використовуються зовнішні джерела мовних сигналів (багатоканальний ресивер і флеш-пам'ять). Такий режим є критичним з точки зору системи безпеки і забезпечує мінімальний рівень безпеки, який можливий при використанні даного генератора. Однак він дозволяє дослідити граничні можливості СЗМІ на мінімальних режимах стійкості до реінжинірингу – виділення мовної інформації із загального потоку в акустичному/вібраційному каналі.

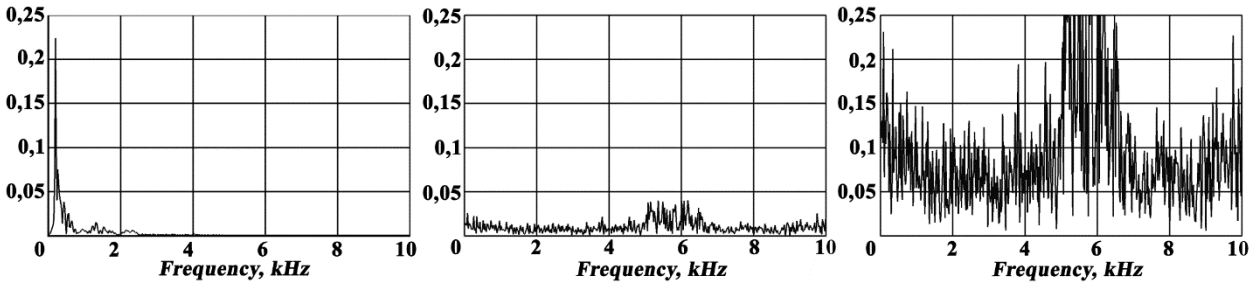
Результати моделювання наведені на рис.1, рис.2 та в [2,3].



а б в

Рис. 1 – Результати моделювання –часові діаграми (осцилограми):

а – вхідний сигнал A(t); б – вихідний сигнал генератора завади SG(t); в – акустический сигнал в каналі SA(t).



а б в

Рис. 2 – Результати моделювання – частотні спектрограми:

а – вхідний сигнал A(t); б – вихідний сигнал генератора завади SG(t); в – акустический сигнал в каналі SA(t).

Аналіз отриманих результатів моделювання: 1. Для переходу системи захисту в робочий режим після закінчення пускових процесів необхідно виділяти від 4 до 10 сек. Цей час необхідний для формування масивів змінних у блоці тимчасових перестановок в генераторі.

2. У системі використовується метод інформаційного (лінгвістичного) маскування мови диктора, що дозволяє отримати більш високий рівень (стосовно енергетичних методів) захисту мовної інформації. Так, наведені на рис.1 часові діаграми характерні для типового мовного сигналу (розмови). Але аналіз спектрограм (рис.2) показує неможливість фільтрації та/або відновлення сигналу, у тому числі

сучасними методами цифрової обробки фонограм (вейвлет-перетворення, спектрально-кореляційний аналіз, адаптивні та нейромережеві фільтри).

3. Використання генераторів такого типу дозволить зменшити рівень акустичного /вібраційного шумового фону в контрольованому приміщенні та навколишньому просторі на 6…9 дБА, що суттєво покращить біоакустичні параметри об'єкта та демасуючий фон. Для стороннього спостерігача/зловмисника об'єкт відповідатиме критеріям "відкритого" громадського заходу.

Висновки: Запропонувати нові принципи побудови системи постановки активних завад та її вузлів шляхом використання в системі постановки активних акустичних та вібраційних завад генераторів мовоподібного сигналу скремблерного типу, що дає змогу розробляти системи захисту мовної інформації, стійких до її відновлення методами фільтрації та реінжинірингу.

Список використаних джерел:

1. Наказ Адміністрації Держспецзв'язку від 19.06.2015 року № 023.

2. Blintsov, V., Nuzhniy, S., Kasianov, Y., Korytskyi, V. "Development of a mathematical model of scrambler-type speech-like interference generator for system of prevent speech information from leaking via acoustic and vibration channels". Technology Audit and Production Reserves, 5 (2 (49)), (2019). 19–26. Doi: 10.15587/2312-8372.2019.185133.

3. Blintsov, V., Nuzhniy, S., Kasianov, Y., & Korytskyi, V. "Mathematical model of the system of active protection against eavesdropping of speech information on the scrambler generator". Eureka: Physics and Engineering, (3), (2020). 11-22. Doi: 10.21303/2461-4262.2020.001241.

Роман ПАВЕЛКО
Слухач навчальної групи 8204
Інститут стратегічних комунікацій
НУОУ
ORCID:0009-0007-2012-9476
E-mail: Poma193@i.ua

АНАЛІЗ УМОВ І ЧИННИКІВ, ЯКІ ВПЛИВАЮТЬ НА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ.

Сьогодні інформаційна безпека та регулювання використання інформаційного простору не лише широко розповсюджені в національному житті

держави, але й стали одним з основних напрямків діяльності державних діячів, аналітиків та військовослужбовців. Усвідомлюючи важливість забезпечення інформаційної безпеки та можливі наслідки недостатньої уваги до її забезпечення, наша країна ратифікувала Конвенцію про кіберзлочинність та активно приймає участь у різних конференціях з кібербезпеки поряд з розвиненими країнами світу. Не вдаючись до аналізуючи питання інформаційної безпеки в глобальному вимірі, зосередимося на тому, як органи військового управління (як у випадку з Генеральним штабом Збройних Сил України) забезпечують інформаційну безпеку.

Відповідно до наказу Міністерства оборони України, як Генеральний штаб Збройних Сил України так і інші органи військового управління входить до переліку органів військового управління, юрисдикція яких поширюється на визначену територію України та діють на підставі Положення про Генеральний штаб Збройних Сил України (відповідними органами військового управління), яким передбачено повноваження щодо забезпечення інформаційної безпеки у Збройних Силах України.

До них належать: 1) здійснення розвідувально-аналітичної діяльності з метою підтримання стану бойової готовності та боєздатності Збройних Сил України; 2) визначення потреб у розвідувальних ресурсах та розвідувальних даних; 3) здійснення комплексу заходів із захисту інформації з обмеженим доступом, що перебуває у володінні держави, включаючи шифрування та технічний захист інформації; 4) опрацювання та надання Головнокомандувачу Збройних Сил України та органам державної влади інформаційно-аналітичних матеріалів щодо стану та підготовки Збройних Сил України; 5) використання сучасних інформаційних технологій у діяльності органів військового управління; 6) участь в організації використання державного інформаційного простору та контроль за його використанням.

Компетенція Генерального штабу Збройних Сил України (відповідними органами військового управління) у сфері інформаційної безпеки характеризується повнотою та спроможністю забезпечувати більшість елементів інформаційної безпеки з метою захисту та зміцнення державної безпеки, обороноздатності, територіальної цілісності та недоторканності кордонів. Однак реальність така, що повноваження органів державної влади чи управління є ефективними лише тоді, коли створені відповідні механізми для їх реалізації. Особливо це стосується повноважень, наданих Генеральному штабу Збройних Сил України у сфері інформаційної безпеки як невід'ємної складової глобальної безпеки. Для безперешкодного використання цих повноважень та досягнення ефективних результатів необхідно на законодавчому рівні та в науковому середовищі вирішити питання взаємодії органів військового управління у сфері інформаційної безпеки, а також порушити питання судової відповідальності за будь-які дії, спрямовані на порушення інформаційної безпеки у Збройних Силах України.

Отже, Генеральний штаб Збройних Сил України, використовуючи свої повноваження щодо забезпечення інформаційної безпеки, повинен забезпечувати інформаційний суверенітет України, удосконалювати державне регулювання розвитку інформаційного простору, наповнювати локальний та світовий інформаційний простір достовірною інформацією про Україну, захищати локальний інформаційний простір, вживати комплексних заходів та сприяти протидії монополізму комерційних організацій України в інформаційному просторі (в межах своїх повноважень).

Список використаних джерел

1. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року « Про Стратегію інформаційної безпеки" №685/2021 від 28.12.2021 р. : за станом на 02.11.2023р. / - Офіц.вид. – УК. – 9 с.;

2. Наказ МО "Про затвердження переліків органів військового управління, юрисдикція яких поширюється на всю територію України" від 20.05.2016 №270: за станом на 02.11.2023р./ Мін'юст України. – Офіц.вид. – К.: 2016. – 5 с.

Ірина ПЕРЕМИБІДА
НАСВ ім. гетьмана Петра Сагайдачного
ORCID: 0009-0009-1511-4688
E-mail: irishka30031@ukr.net

КІБЕРБЕЗПЕКА ЯК СКЛАДНИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПРОБЛЕМНІ ПИТАННЯ

Кібербезпека як складник інформаційної безпеки будується на основі комплексного підходу, що містить не тільки технічні засоби захисту, а й організаційні заходи, правові норми та освітні програми. Однак, головною складовою є розвиток інноваційних технологій і методів виявлення та запобігання кібератакам. Окреслена складова особливо актуалізувалась в умовах гібридної російсько-української війни. Коли виникли нові виклики для інформаційної безпеки.

Слушними вважаємо резюмування В. Аніщук, що "нове звучання інформаційна безпека набула через повномасштабне вторгнення російської федерації в Україну. Держава-агресор проводить жорстокі підступні військові дії не лише на території нашої держави, але й в інформаційному просторі. Відповідно до Указу Президента України "Про рішення Ради національної безпеки і оборони

України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"" було встановлено, що "інформаційна політика російської федерації – загроза не лише для України, але й для інших демократичних держав. Спеціальні інформаційні операції російської федерації спрямовуються на ключові демократичні інституції (зокрема, виборчі), а спеціальні служби держави-агресора намагаються посилити внутрішні протиріччя в Україні та інших демократичних державах. Застосовані російською федерацією технології гібридної війни проти України, у тому числі моделі і механізми інформаційного втручання, поширюються на інші держави, швидко адаптуючись до локальних контекстів та регуляторних політик. Обмежувальні заходи (санкції) та ефективний механізм моніторингу і відповідальності за їх порушення є одним із дієвих механізмів відповіді на дезінформаційну активність російської федерації як держави-агресора [1, с. 141]".

Продовжуючи, автор зазначає, що не зважаючи на це "в Україні досі триває процес становлення системи стратегічних комунікацій. Органами державної влади України здійснено низку організаційних та практичних заходів зі зміцнення власної інституційної спроможності у сфері стратегічних комунікацій, однак не створено дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до здійснення заходів із протидії загрозам в інформаційній сфері. Зазначене послаблює можливості до розбудови комплексного стратегічного планування інформаційного потоку, здійснення системної комунікативної діяльності Кабінету Міністрів України, об'єднання всіх ключових суб'єктів у сфері інформаційних відносин, суб'єктів формування і реалізації державної політики щодо ефективного захисту національного інформаційного простору, утвердження позитивного іміджу України, реалізації цілей захисту національної безпеки України в інформаційній сфері. Регулювання відносин у сфері інформаційної діяльності не відповідає сучасним викликам та загрозам. Це перешкоджає розвитку українського медіаринку, ускладнює ведення бізнесу у цій сфері, зберігає залежність засобів масової інформації від їх власників, не забезпечує додержання професійних стандартів діяльності журналістів" [1, с. 141-142].

Нині фахівці в галузі кібербезпеки працюють над створенням нових алгоритмів шифрування даних, систем контролю та моніторингу, а також методів аутентифікації та ідентифікації користувачів. Вони також розробляють нові системи протидії соціальній інженерії та фішингу, щоб усунути вразливості в поведінці користувачів і запобігти витоку конфіденційної інформації. Однак, розвиток кібербезпеки не може йти у відриві від розвитку кіберзлочинності. Кіберзлочинці постійно вдосконалюють свої методи атак і тому необхідне постійне оновлення та вдосконалення інформаційного захисту. Тільки так фахівці зможуть оперативно реагувати на нові загрози та запобігати їхньому виникненню.

Адже, за словами О. Тернового, О. Шкуренко та М. Міненко "кіберзагрози дедалі почастішали, стали більш організованими і збитковими для державної

економіки в цілому та об’єктів критичної інфраструктури зокрема. Вони здатні досягти небезпечного рівня і негативно вплинути на національний розвиток та євроатлантичні прагнення нашої держави, безпеку і стабільність європейської спільноти. Джерелами таких загроз можуть бути іноземні військові й розвідувальні служби, організовані злочинні угруповання, терористичні та екстремістські групи тощо. За сформованих умов, основним завданням державних органів безпеки та оборони України, є застосування заходів, спроможних зменшити, а іноді, й цілком унеможливити негативні наслідки кіберзагроз” [5, с 23].

Очевидно, що розвиток і застосування кібербезпеки у сфері інформаційних технологій є необхідною умовою для забезпечення безпеки інформації та надійного функціонування ІТ-інфраструктури нашої країни [2]. Це вимагає співпраці різних структур [4], включно з державними органами, компаніями, навчальними закладами та суспільством загалом. Разом з тим, нині відбувається в ускладнених умовах. Погоджуємось з висновками З огляду на це, науковці В. Дідик., А. Гончарук та І. Сімоненкова, що “для надійного протистояння кіберзлочинам у ЗС України, завдяки використанню надсучасних програмних алгоритмів, має бути створена система протидії, яка здатна протистояти атакам і втручанням в роботу інформаційно-телекомунікаційних систем. Дослідники переконані, що на різних рівнях кіберпростору необхідно застосовувати систему захисту інформації, що гарантуватиме здійснення таких заходів: розмежування доступу користувачів до ІТС із використанням криптографічного захисту інформації під час зберігання та обміну нею; застосування міжмережевого екранування з одночасним використанням маршрутизаторів та фаєрволів; забезпечення створення й практичного застосування віртуальних приватних мереж; системне використання антивірусного захисту; унеможливлення застосування програмних продуктів потенційними опонентами; застосування системи виявлення вторгнень (IDS) за умови використання підсистеми профілактики вторгнень (IPS); встановлення механізму автентифікації й авторизації; забезпечення резервного зберігання даних на носіях інформації, до яких обмежений будь-який несанкціонований доступ” [3, с . 94].

Список використаних джерел:

1. Аніщук В. В. Інформаційна безпека як об’єкт посягання злочинів проти основ національної безпеки України. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/284126/278265 (дата звернення: 15.09.2023 р.).
2. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ : ДУТ, 2015. 288 с.
3. Дідик В. О., Гончарук А. А., Сімоненкова І. В. Кіберзахист в Збройних Силах України для протидії можливим варіантам кіберзлочинності. *Кібербезпека в*

Україні: правові та організаційні питання: матер. Всеукр. наук.-практ. конф. (м. Одеса, 17 листопада 2017 р.). Одеса: Одес. держ. ун-т внутр. спр., 2017. С. 94–95.

4. Кирилюк Р., Шелест Є. Кібервійська як складова трансформації системи національної безпеки. *Оборонний вісник : Центр воєнної політики та політики безпеки*. 2021. № 9. С. 4–10.

5. Терновий О. В., Шкуренко О. М., Міненко М. Л. Проблемні аспекти кібероборони: місце та роль кіберзахисту в ЗСУ. URL: http://sit.nuou.org.ua/article/view/278116/276052 (дата звернення: 15.09.2023 р.).

Леонід ПОБЕРЕЖНИЙ
ORCID: 0009-0002-6648-512X
E-mail: leoleo77@ukr.net
Олександр ОЛЕКСЕНКО, д. філос.
ORCID: 0000-0002-6853-9630
E-mail: oleksenko-02@ukr.net
Микола КОВАЛЕНКО
ХНУПС ім. Івана Кожедуба
ORCID: 0000-0003-1512-2812
E-mail: nik1905@ukr.net

СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Громадська підтримка Збройних Сил (ЗС) України має велике значення під час ведення воєнних операцій та конфліктів. Без цієї підтримки виникають проблеми з морально-психологічним станом військовослужбовців та їх здатністю виконувати завдання. Засоби масової інформації (ЗМІ) грають важливу роль у впливі на свідомість громадськості та формуванні їх ставлення до подій [1].

Недостатня співпраця між ЗМІ та воєнними структурами в Україні може спричинити негативне ставлення до ЗС України та порушити інформаційне поле. Важливо підтримувати високий моральний дух військовослужбовців, що є ключовим фактором у цивільно-воєнній взаємодії. Співпраця та взаємна довіра між ЗМІ та ЗС України є важливими аспектами для передачі точної та об'єктивної інформації. Для покращення цієї взаємодії можна використовувати різні інструменти, такі як брифінги та інформаційні заходи. Важливо також підкреслювати інформаційну підтримку ЗС України серед громадськості та міжнародних партнерів, щоб забезпечити потребу в ресурсах для боротьби з агресією та зміцнення незалежності України.

Але окрім інформування громадськості про ключові події, хід бойових дій та обстановку, що склалась, вітчизняні ЗМІ суттєво впливають ще й на свідомість своєї аудиторії формуючи відповідне відношення до подій і фактів, про які вони

сповіщають. У разі, низького рівня взаємодії ЗМІ та структур зв'язків з громадськістю у ЗС України відбувається процес, який призводить до негативного забарвлення значної частини інформації. Вона буде містити критику, а відтак підриватиме авторитет Сил оборони та формуватиме негативне відношення населення до силових структур [1-3].

Стратегія та тактика дій противника показує, що боротьба українців за свою свободу, незалежність і повернення захоплених Російською Федерацією українських територій набуває затяжного характеру. На одному рівні з фізичною силою виступає й моральна. Вона також впливає на результат такої боротьби. Військовослужбовець має вірити в себе, в свого командира, в свою державу. Високий моральний дух кожного воїна – головна мета цивільно-воєнної взаємодії. Так відбувалося під час проведення антитерористичної операції, а згодом операції об'єднаних сил, коли, попри численні збої в управлінні, забезпеченні, взаємодії та підготовці, завдяки народній підтримці, передусім моральній, українська армія відновлювалася, розвивалася та чинила значний опір більш сильному противнику. Нині чинити опір російській агресії Силам оборони допомагають не тільки самі українці, а й увесь цивілізований світ. І настрої та бажання цивільних людей, для нас військовослужбовців, надзвичайно важливі.

Журналісти, підхоплюючи негативні настрої суспільства, загальне погане ставлення народу до держави та більшості політиків, нерідко викривають реальні факти корупції і самих корупціонерів. Але буває й таке, що звинувачення спростовуються, а недовіра до силових структур залишається або зростає. Впровадивши зрозумілі, взаємоприйнятні правила взаємодії між військовими і цивільними можна позбутися цього негативу. Наразі добре працює напрямок з організації брифінгів фахівців з воєнних питань. На них представники ЗМІ можуть почути офіційну позицію керівництва ЗС України та інших силових структур з приводу обстановки, стану підпорядкованих їм військ (сил), а також уточнити деталі порушеного питання.

Ще одним потужним заходом, спрямованим на зростання жаги до перемоги над російською агресією, її наближення та розширення діяльності українців, громадян та урядів інших держав щодо збільшення загальної допомоги Силам оборони України має бути організація доведення всім простої народної мудрості, що які б труднощі на шляху до перемоги над ворогом не виникали, у будь-якому випадку, краще годувати свою армію, аніж чужу. Ця істина, яка підтверджена людьми, що перебували в тимчасовій окупації на уже звільнених територіях, усім досить зрозуміла і не викликає ні в кого ніяких сумнівів. Таке гасло має бути у першому рядку будь-якої реклами, воно має постійно звучати в усіх ЗМІ, майоріти на багатьох білбордах і місцях для реклами кожного закладу та підприємства.

Список використаних джерел:

1. Бакуменко Р.О. Проблеми комунікаційно-контентної безпеки через призму системи зв'язків з громадськістю ЗСУ. *Контентно-потокові моделі як тактичні інструменти комунікаційно-контентної безпеки:* Мат. Міжнар. форуму з кризовості комунікацій (м. Київ, 22-23 трав. 2017 р.). Київ: ВІКНУ, 2017. С. 275-278.
2. Благодарний А.М., Кононець О.О. Стратегічнікомунікації у секторі безпеки і оборони України. *Науковий журнал "Молодий вчений"*. 2023. № 1 (113). С. 5-9. https://doi.org/10.32839/2304-5809/2023-1-113-2.
3. Концепція стратегічних комунікацій Міністерства оборони та Збройних Сил України. Міністерство оборони України. URL: http://www.mil.gov.ua/content/mou_orders/612_nm_2017.pdf.

Орест ПОЛОТАЙ, к.т.н., доц.
ЛДУ БЖД
ORCID: 0000-0003-4593-8601
E-mail: orest.polotaj@gmail.com

КОМП'ЮТЕРНА КРИМІНАЛІСТИКА – ЯК ІНСТРУМЕНТ ДОСЛІДЖЕННЯ ЗЛОЧИНІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Комп'ютерна (цифрова) криміналістика (форензика) – це судова наука практичного спрямування, започаткована у 1970-80-х рр., яка вивчає відновлення та дослідження у цифрових пристроях даних, пов'язаних з кіберзлочинністю [1].

Комп'ютерна криміналістика традиційно охоплює не лише рекомендації, прийоми і засоби викриття та розслідування уже вчинених кіберзлочинів та інших цифрових зловживань, а й рекомендації щодо їх запобігання й випередження – тобто кібербезпеку. Крім цього, закономірності розслідування кіберзлочинів рівною мірою використовуються й у спорах між компаніями та/або фізичними особами (в рамках цивільного права), коли цифрового спеціаліста залучають до відшукання інформації про особу чи компанію, перевіривши їх комп'ютер. Для опису цього типу розслідувань використовується спеціальний термін "eDiscovery". Кібербезпека і кіберрозслідування тісно взаємопов'язані, проте суттєво відрізняються. Кіберрозслідування досліджує незаконну та/або шкідливу поведінку в Інтернеті, її рушійні сили, а кібербезпека – прогнозування, уникнення та реагування на ці дії [1].

Предметами комп'ютерної криміналістики є [3]:

кримінальна практика – способи, інструменти здійснення відповідних злочинів, їх наслідки, що залишаються сліди, особистість злочинця;

оперативна, слідча і судова практика по комп'ютерним злочинам;

методи дослідження комп’ютерної інформації, зокрема програм для персональних комп’ютерів;

досягнення галузей зв'язку та інформаційних технологій (ІТ), їх вплив на суспільство, а також можливості їх використання як для вчинення злочинів, так і для їх запобігання і розкриття.

Майже всі сліди, з якими доводиться працювати фахівцю з форензики, мають вигляд комп'ютерної інформації, регулярної чи побічної. Їх досить легко знищити – як навмисне, так і випадково. Часто їх легко підробити, бо підроблений байт нічим не відрізняється від справжнього. Фальсифікація електронних (цифрових) доказів виявляється або за змістовим змістом інформації, або за залишеними в інших місцях слідами, також інформаційними. Цифрові докази не можна сприйняти безпосередньо органами почуттів людини, але лише за допомогою складних апаратно-програмних засобів. Тому ці сліди складно продемонструвати іншим особам – понятим, прокурору, судді. Не завжди легко забезпечити незмінність слідів за її зберіганні. І не лише забезпечити, а й довести суду цю незмінність.

Сфери застосування комп’ютерної криміналістики є такими:

1. Розкриття та розслідування кримінальних злочинів, у яких фігурують комп'ютерна інформація як об'єкт зазіхання, комп'ютер як знаряддя скоєння злочину, і навіть якісь цифрові докази.

2. Збір та дослідження доказів для цивільних справ, коли такі докази мають вигляд комп'ютерної інформації. Особливо це актуально у справах про порушення прав інтелектуальної власності, коли об'єкт цих прав представлений у вигляді комп'ютерної інформації – програма для ЕОМ, інший твір у цифровій формі, товарний знак у мережі Інтернет, доменне ім'я тощо.

3. Страхові розслідування, які проводять страхові компанії щодо можливих порушень умов договору, страхового шахрайства, особливо коли об'єкт страхування представлений у вигляді комп'ютерної інформації або таким об'єктом є інформаційна система.

4. Внутрішньокорпоративні розслідування інцидентів безпеки щодо інформаційних систем, а також роботи щодо запобігання витоку інформації, що містить комерційну таємницю та інші конфіденційні дані.

5. Військові та розвідувальні завдання щодо пошуку, знищення та відновлення комп'ютерної інформації в ході надання впливу на інформаційні системи противника та захисту своїх систем.

6. Завдання щодо захисту громадянами своєї особистої інформації в електронному вигляді, самозахисту своїх прав, коли це пов'язано з електронними документами та інформаційними системами.

Комп’ютерна криміналістика використовує спеціальні методи дослідження, властиві тільки їй. Серед цих методів можна виділити наступні:

створення і застосування спеціалізованих криміналістичних інформаційних систем; перенастроювання і використання в своїх цілях систем подвійного призначення;

використання з метою виявлення або дослідження доказів публічних пошукових систем (таких як “Google”), а також пошукових систем спеціального призначення (типу “Ешелон”);

створення віртуальної особистості для цілей проведення з її допомогою ОРЗ і агентурної роботи;

збір “хеш” функцій відомих файлів для відділення їх від файлів, з тримають оригінальну призначену для користувача або модифіковану інформацію;

архівування повного вмісту носіїв для цілей повного розслідування можливих інцидентів;

емуляція мережевих сервісів для дослідження поведінки підозрілих програм в лабораторних умовах.

Види комп’ютерної криміналістики залежать від типу проблем і належать до якої частини комп’ютера. Нижче наведені різні види комп’ютерної криміналістики [5].

Диск-криміналістика: цей тип займається вилученням даних із носія даних комп’ютера, що дозволяє здійснювати пошук активних, змінених або видалених файлів.

Мережева криміналістика: це ще один вид цифрової криміналістики, що дозволяє відслідковувати та аналізувати мережевий трафік комп’ютера та збирати важливу інформацію, що веде до юридичних доказів.

Криміналістика бази даних: він визначає вивчення та перевірку відповідних баз даних та їх збережених метаданих.

Криміналістика шкідливих програм: це дозволяє ідентифікувати шкідливий код для виконання роботи над їх корисним навантаженням, вірусами, хробаками тощо.

Криміналістика електронною поштою: це допомагає перевірити відновлення електронних листів, охоплюючи всі видалені листи, календарі та контакти.

Отже, зростання кіберзлочинності вимагає для її розслідування залучення спеціальних технічних знань. Без належно знайдених, зібраних та оформлених доказів неможливо висунути певній особі обвинувачення та притягнути її до відповідальності. Розвиток технологій ускладнює ситуацію: соціальні мережі, мобільні пристрої та Інтернет використовуються для вчинення злочинів багатьма досі невідомими способами. За цих умов комп’ютерна криміналістична експертиза дуже потрібна, а фахівців з сучасними знаннями не вистачає.

Список використаних джерел:

1. Комп’ютерна криміналістика [Електронний ресурс] Режим доступу з https://law.lnu.edu.ua/course/digitalforensics.

2. Кримінальний кодекс України [Електронний ресурс]. – Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/2341-14.

3. Федотов Н.Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – 432 с.

4. Що таке комп'ютерна криміналістика? - Підказка щодо Linux . [Електронний ресурс] Режим доступу з https://ciksiti.com/uk/chapters/4152-what-is-computer-forensics---linux-hint.

Юрій ПРІБИЛЄВ, д.т.н., професор
ORCID: 0000-0003-1941-3561
E-mail: pribilev@meta.ua
Сергій БАЗАРНИЙ, ад'юнкт
НУОУ
ORCID: 0000-0001-9545-1960
E-mail: gans251080@gmail.com

УДОСКОНАЛЕННЯ СТОХАСТИЧНОЇ МОДЕЛІ СОЦІАЛЬНОЇ МЕРЕЖИ

Соціальні мережі (далі СМ), як суспільне явище, з'явилися досить давно і стали широко поширеним засобом прямого та опосередкованого впливу на свідомість, підсвідомість та емоційний стан агентів СМ з метою стимулювання певних змін у поведінці визначених цільових аудиторій (далі ЦА). Для просування наративів у СМ використовуються різні інформаційні технології (ІТ) онлайн-платформ зі застосуванням мікротаргетингу, ботів та діпфейків [1].

Актуальним завданням є проведення аналізу методів психологічного впливу (далі ПсВ) на структуру та динаміку змін поведінки агентів СМ [2], який здійснюється за допомогою ботів в інформаційних операціях (далі ІО). Активне використання ботів в інтересах проведення ІО для проведення ПсВ на агентів СМ шляхом поширення спеціальної інформації вимагає дослідження та розробки адекватних математичних моделей СМ.

На ефективність ведення ПсВ за допомогою штучного інтелекту (artificial intelligence) впливає правильний розрахунок результативності ПсВ ботів на агентів СМ. Сучасне програмне забезпечення з голосовою активацією, наприклад Siri від Apple і Alexa від Amazon, використовує алгоритми для обробки запитів від користувачів. Для ускладнення спроб видалення ботів з платформ соціальних медіа, програмне забезпечення ботів використовує технології нейролінгвістичного програмування [3], в результаті чого публікації в Інтернеті виглядають навіть більш автентично, ніби їх написали справжні агенти СМ.

Боти здатні генерувати контент, вступати у взаємодію з реальними агентами СМ, поширювати спеціальну інформацію з метою ПсВ [4]. За рахунок використання ботів значно підвищується ефективність розповсюдження спеціальної інформації, коли вона потрапляє в медіа-середовище. Боти запрограмовані для поширення матеріалу з певного облікового запису та при використанні їх у достатньої кількості [5], спеціальна інформація стає вірусною. Боти також використовуються для створення видимості підтримки певної інформації справжніми людьми [6]. Після виконання завдання, ботів можна використовувати багатократно, що робить їх універсальним і потужним інструментом для виконання завдань при проведенні ІО.

У доповіді проаналізовано математичні моделі, які можуть бути застосовані для дослідження ПсВ ботами у СМ [7], що дозволяє змоделювати динаміку змін поведінки агентів СМ, а саме:

модель випадкових графів, де мережа соціальних зв'язків моделюється за допомогою випадкових графів, а взаємодії між агентами СМ задаються ймовірнісними розподілами;

модель передачі інформації між агентами СМ, що заснована на теорії передачі інформації, де вплив ботів визначається ймовірностями передачі інформації від ботів до агентів СМ;

модель ігор, що відображає агентів, які розглядаються як гравці, що обирають стратегії взаємодії на основі впливу ботів та своїх інтересів. Застосування моделі ігор вивчає взаємодію агентів, їхню участь у дискусіях та реакції на спеціальну інформацію.

Якщо мета дослідження спрямована на вивчення структури СМ та виявлення ехо-камер, то модель випадкових графів є більш адекватною. Якщо досліджувати передачу інформації та поширення фальсифікованих даних, то модель передачі інформації є більш доцільною. Використання моделей ігор є корисною для проведення аналізу взаємодії агентів СМ. Порівняння різних моделей та їхні відповідності динаміці змін поведінки агентів СМ описує вплив ботів, зокрема на формування ехо-камер та фільтрацію інформації. За допомогою моделей СМ досліджується реакція агентів СМ на інформацію, яку поширюють боти, аналізується, як ця інформація впливає на думки, переконання та поведінку агентів СМ. Моделі СМ дозволяють кількісно розрахувати кількісні показники ПсВ ботів на агентів СМ (участь агентів СМ у онлайн-дискусіях, результати впливу на ставлення ЦА).

Для моделювання процесу впливу штучних електронних облікових записів на агентів СМ запропоновано використовувати удосконалену стохастичну модель СМ на основі теорії випадкових графів з урахуванням топології мережі та індивідуальних особливостей агентів СМ. Враховуючи топологію мережі та індивідуальні характеристики агентів СМ для оцінювання

ефективності ПсВ на ЦА противника в інтересах проведення ІО, подальші дослідження можуть бути спрямовані на вдосконалення моделі шляхом додавання додаткових можливостей та використання алгоритмів штучного інтелекту на рівні регулювання, моніторингу та розвитку використання ботів для ПсВ на ЦА противника.

Список використаних джерел:

1. СТАНДАРТ НАТО AJP-10. ОБ'ЄДНАНА ДОКТРИНА СОЮЗНИКІВ ДЛЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ. Видання А Версія 1 березень 2023р. С.7-11.
2. Базарний С.В. Метод виявлення агентів соціальних мереж, що мають найбільший вплив. / С.В. Базарний. Сучасні інформаційні технології у сфері безпеки та оборони: наук. журн. Нац.ун-т оборони України. Київ. 2023. №1(46)/2023 с.145-150.
3. Naja Bentzen. EPRS / European Parliamentary Research Service, Members' Research Service PE 628.284 – October 2018 https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/628284/EPRS_ATA(2018)628284_EN.pdf.
4. Стариков А. Боти і тролі в інформаційно-психологічних війнах // Вісник ЛНУ. Серія: Журналістика. 2021. Т. 34. No 44. С. 42–45.
5. McKenzie Himelein-Wachowiak. Brenda Curtis Bots and Misinformation Spread on Social Media: Implications for COVID-19 Published on 20.5.2021 in Vol 23 , / McKenzie Himelein-Wachowiak, S. Giorgi, A. Devoto, M.Rahman, L. Ungar, A. Schwartz, D. Epstein, L. Leggio. No 5 (2021):May Preprints (earlier versions) of this paper are available at https://preprints.jmir.org/preprint/26933, first published January 04, 2021.
6. Samuel C. "Bots and Computational Propaganda: Automation for Communication and Control," in eds. Nathaniel Persily & Joshua A. Tucker, Social Media and Democracy: The State of the Field, Prospects for Reform (Cambridge: Cambridge University Press, 2020), pp. 89-110.
7. Базарний С.В. Класифікація методів аналізу та моделей соціальних мереж в інтересах інформаційної операції. Vol. 29 No. 2 (2023): Ukrainian Scientific Journal of Information Security / С.В. Базарний Cybersecurity & Critical Information Infrastructure Protection (CIIP). С. 61-66.

Олександр ПРОКОПЕНКО, д.ф.
НУОУ
ORCID: 0000-0002-5482-0317
E-mail: o.prokopenko@edu.nuou.org.ua
Олександр КУЛЬЧИЦЬКИЙ
НУОУ
ORCID: 0000-0002-4901-0192
E-mail: o.kulchytskyi@edu.nuou.org.ua
Ольга ОНОФРІЙЧУК
НУОУ
ORCID:0000-0003-3609-7732
E-mail: o.onofriichuk@edu.nuou.org.ua

ПІДХІД ЩОДО УДОСКОНАЛЕННЯ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ І АНАЛІЗУ ІНФОРМАЦІЙНИХ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Сучасні реалії визначаються переходом до етапу становлення глобального інформаційного простору, де ключовою рисою цього процесу є використання інформації як засобу досягнення поставлених цілей. Ця тенденція активізує розвиток інформаційних технологій для задоволення комунікаційних потреб у політичній, економічній, військовій, соціальній та інших сферах діяльності людства. Інформаційна відкритість світу надає можливості використовувати інформацію як знаряддя впливу. Звідси виникає загроза проведення противником інформаційних атак (операцій). Викладання інформації у спосіб, який приносить користь організатору інформаційної пропаганди, дозволяє формувати потрібні погляди та думки в суспільстві, впливати на громадську думку і розвивати послідовні логічні аргументи.

В умовах розгорнутої російською федерацією проти України повномасштабної війни, питання інформаційної безпеки стає однією з найважливіших складових національної безпеки України. Починаючи з 2014 року, Україна зазнає надзвичайно великому тиску від інформаційних атак, спрямованих на ослаблення державності, демократії, суверенітету та територіальної цілісності нашої країни. Серед основних форм інформаційних загроз для України, які поширюються через російські державні ЗМІ та агентів впливу, слід виділити спотворення інформації у вигляді відкритої пропаганди, інформаційний тероризм і дезінформацію. Головною метою цих дій є формування у міжнародному співтоваристві негативного образу України, представлення її як нестабільної, корумпованої та неспроможної до проведення реформ держави. Інформаційні атаки спрямовані на психологічну деморалізацію українського населення, збільшення соціально-політичної поляризації та поглиблення розбрату між Україною та її західними партнерами. Ця стратегія

призводить до посилення внутрішніх суперечностей та зростання негативних настроїв серед населення, що створює небезпечне середовище для національної єдності та стабільності країни.

У цих умовах підвищення рівня інформаційної безпеки постає пріоритетним завданням першочергового значення, що вимагає комплексного підходу, який включає в себе підвищену інформаційну обізнаність населення, захист від інформаційних атак і зміцнення національного інформаційного простору. Поточні виклики та загрози національній безпеці України підкреслюють важливість впровадження комплексу ефективних заходів для втілення стратегічних наративів держави, реалізації механізмів щодо своєчасної інформаційної протидії і нейтралізації деструктивного інформаційного впливу як на особистість, так і на державу в цілому.

З огляду на вищезазначене, значна роль в інформаційній протидії противнику належить оцінюванню інформаційного простору у системі стратегічних комунікацій, основу якого становить моніторинг. Застосування у моніторингу інформаційного простору сучасних теоретичних підходів та інформаційних технологій дозволить суттєво покращити виявлення та аналіз інформаційних загроз національній безпеці України.

Ознаки негативного ІПВ виявляються на основі аналізу контенту інформації, отриманої шляхом моніторингу інформаційного простору, який здійснюється за певними етапами:

1) підготовчий;
2) добування даних;
3) класифікація і типізація даних;
4) аналіз даних;
5) прийняття рішень.

На *першому* етапі, визначається цілі і завдання, які повинен вирішити моніторинг. При цьому враховується охоплення (масштабність) виконання завдань: географічні, соціальні, політичні, на які цільові аудиторії слід зосереджувати увагу, тощо. Визначаються обмеження досліджень (тематика досліджень) і обираються перелік інформаційних ресурсів, які підлягатимуть моніторингу: веб-сторінки, Telegram, Facebook, Instagram, Twitter, тощо. Отже, всі ключові особливості і завдання, які виконувались за аналізом попереднього моніторингу, можуть уточнятись для проведення наступного.

На *другому* етапі, визначаються правила обробки даних. Визначаються шляхи отримання даних з інформаційних ресурсів, наприклад, яка саме технологія парсингу даних, наприклад, web scraping, web crawling, буде використовуватись і яким чином її налаштовувати під кожен окремий інформаційний ресурс.

Парсинг –це метод швидкої обробки інформації, точніше синтаксичний аналіз даних, розміщених на веб-сторінках. Він використовується для оперативного опрацювання великої кількості текстів, цифр, зображень.

Третій етап є найбільш відповідальним, в ході якого виконується класифікація (відповідність) повідомлень за певними темами (наратив або складова частина наративу), а також встановлюється тональність і семантика текстів повідомлень (типізація даних).

На *четвертому* етапі, проводиться аналіз кількісно-якісних показників, отриманих на попередніх двох етапах. З цією метою розробляються інтерактивні інформаційні панелі, на яких здійснюється їх візуалізація у вигляді графіків, діаграм, зведених таблиць, тощо. Зазначене, значно спрощує сприйняття інформації, дозволяє проводити аналіз тональності повідомлень і їх кількості за визначеними темами, проводити часові зрізи інформації.

На *п'ятому* етапі, проводиться розробка і вжиття заходів щодо протидії негативному інформаційно-психологічного впливу, уточнення цілей і завдань моніторингу і контроль стану реалізації державної інформаційної політики.

Кожен описаний вище етап включає виконання ряду процедур, деталізувати які в рамках написання однієї статті неможливо. Водночас, систематизація знань про методи і способи, які використовують при моніторингу інформаційного простору, вказують на певну послідовність дій щодо комплексного уявлення цього процесу.

Висновки: Таким чином, запропонований підхід моніторингу інформаційного простору, надає комплексне представлення про необхідний і дієвий інструментарій своєчасного виявлення і аналізу негативного інформаційно-психологічного впливу противника в інтернет ресурсах, соціальних мережах. Зазначене може стати концептом для розроблення інформаційно-аналітичної системи моніторингу інформаційного простору, з подальшим її використанням в інформаційно-аналітичному забезпеченні органів військового управління, підрозділів Збройних Сил і Міністерства оборони України, на які покладаються зазначені функції. Це дозволить підвищити обґрунтованість рішень і ефективність вжиття заходів для протидії негативному інформаційно-психологічному впливу противника з одного боку, так і інформаційного супроводження діяльності уряду, державних інституцій і публічних осіб через комунікативні можливості держави з іншого.

Олександр СКЛЯР
НУОУ
ORCID: 0000-0003-4449–1828
E-mail: sklyar.sesh@ukr.net

ВПЛИВ КІБЕРАТАК НА ЕФЕКТИВНІСТЬ ФУНКЦІОНУВАННЯ СИСТЕМИ УПРАВЛІННЯ ПРОТИПОВІТРЯНОЮ ОБОРОНОЮ

У сучасних умовах роль і значення управління для організації і ведення бойових дій незмірно збільшується. За оцінками військових фахівців [1],

ефективна система управління здатна підвищити ефективність застосування підпорядкованих підрозділів більше ніж у 2 рази.

Тому на цей час актуальним і пріоритетним напрямком розвитку збройних сил більшості провідних країн стає реалізація концепції мережецентричних війн. Основна ідея якої полягає в інтеграції всіх сил і засобів у єдиний інформаційний простір, що дає змогу багатократно збільшити ефективність їх бойового застосування за рахунок синергетичного ефекту [2].

Водночас впровадження сучасних інформаційних технологій в систему управління поряд з підвищенням її можливостей також збільшує можливості противника по здійсненню зовнішнього впливу на неї. Одним з яких є здійснення впливу на кіберпростір так як він є невід'ємною складовою інформаційного простору.

Як відомо [3] кібератака – спрямовані дії в кіберпросторі з утручанням у роботу інформаційно-телекомунікаційних систем з метою порушення конфіденційності, цілісності, доступності, авторства інформації або контролю, зміни в роботі, вимкнення, знищення обчислювальних механізмів чи інфраструктури.

Розрізняють три основні типи кібератак за метою впливу на об'єкти [4]:

порушення конфіденційності – завданням атаки є отримання несанкціонованого доступу до інформації;

порушення цілісності – передбачає несанкціоновану зміну в інформації чи програмних і технічних засобах системи;

порушення доступності – метою атаки є дестабілізація роботи системи внаслідок створення перешкод для легітимних користувачів щодо доступу їх до системи або даних, необхідних для вирішення функціональних задач.

До найпоширеніших видів кібератак належать [4]: denial of service (DoS attack); phishing; malware; ransomware; man-in-the-middle; zero-day exploit; cross-site scripting (XSS); logic bombs.

Характерною особливістю кібератак є миттєвість здійснення (протягом секунд, хвилин).

Аналіз джерел [5-6] показав, що для підтримки бойових дій і розвідувально-підривної діяльності збройні сили рф активно проводили кібератаки на систему управління Сил оборони України. А враховуючи те, що система управління протиповітряною оборони є її складовою то у випадку успішного проведення кібератак противником можлива часткова відмова каналів зв'язку та припинення обміну інформації про повітряну обстановку в автоматичній системі збору, обробки та відображення інформації "Віраж-Планшет".

Тому враховуючи досвід російсько-української війни є очевидним, що в умовах мережецентричних воєнних (бойових) дій існує необхідність врахування

впливу кібератак на ефективність функціонування системи управління протиповітряною оборони.

Список використаних джерел:

1. Теоретичні основи управління угрупованням військ (сил) у сучасних умовах збройної боротьби : монографія / О. М. Загорка, А. К. Павліковський, А. А. Корецький, С. О. Кириченко, І. О. Загорка; / за заг. ред. І. С. Руснака. – К.: НУОУ, 2020 – 248 с.
2. Тарасов В. М. Розвідувально-ударні, розвідувально-вогневі комплекси (принципи побудови в умовах реалізації концепції мережецентричних війн, оцінка ефективності бойового застосування) : монографія / за заг. ред. В. М. Телелима / В. М. Тарасов, Р. І. Тимошенко, О. М. Загорка. – К.: НУОУ. 2015 – 184 с.
3. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 5 жовтня 2017 р. // Відомості Верховної Ради. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
4. Cybersecurity: Selected Cyberattacks, 2012–2021. Washington : Congressional Research Service, 2021. 24 p. [Електронний ресурс]. – Режим доступу:https://crsreports.congress.gov/product/pdf/R/R46974.
5. Як маскуються російські кібервійська. [Електронний ресурс]. – Режим доступу: https://armyinform.com.ua/2022/05/25/yak-maskuyutsya-rosijski-kibervijska-2/.
6. Кібервійна рф проти України: як працюють російські хакери та воюють українські кібервійська. [Електронний ресурс]. – Режим доступу:https://thepage.ua/ua/politics/kibervijna-rf-proti-ukrayini-yak-voyuyut-ukrayinski-kibervijska.

Руслан СТЕПАНИШИН
ВІКНУ ім. Тараса Шевченка
ORCID: 0009-0004-7587-7234
E-mail: man_fan@ukr.net

РОЗВИТОК ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ТА ЙОГО ВПЛИВ НА МІЖНАРОДНУ ІНФОРМАЦІЙНУ БЕЗПЕКУ

На сьогодні технології штучного інтелекту (ШІ) впевнено завойовують популярність у різних сферах життя, в тому числі в області воєнного будівництва. На сьогодні багато дослідників намагаються визначити можливий вплив цього процесу на характер ведення бойових дій та ризики для міжнародної і державної

безпеки. Аналіз наявних підходів до технологій ШІ і можливих ефектів їх поширення показує, що на сьогодні спостерігається дві гіперболізовані тенденції до оцінки ШІ як явища. З однієї сторони, ШІ розглядається у вигляді "розумний робот з власною волею", який розглядає людство як перешкоду і можливу загрозу собі і планеті (концепція навіяна кінематографом у фільмах "Термінатор" і "Матриця"). З іншої – ШІ розглядається виключно як функція, здатна виконувати завдання в рамках певної професії, яку можна обмежити або заборонити і тим самим нівелювати можливі ризики.

Слабкість таких підходів заключається в тому, що ШІ не розглядається як науковий феномен, який потребує дослідження його природи. Без такого розуміння, технології ШІ можуть розвинутись неконтрольовано, що призведе до виникнення нового типу конфліктів і глобальної конкуренції. Характерною рисою таких конфліктів буде тотальна автоматизація, яка призведе до фактично руйнування класичного циклу аналізу інформації і в кінцевому результаті зведе до мінімуму контроль людини над більшістю приймаємих рішень, у тому числі у сфері оборони і безпеки.

Вже зараз системи ШІ завдяки швидкості отримання, обробки і аналізу інформації суттєво переважають аналогічні автоматизовані системи за участі людини. В окремих напрямках – візуальне розпізнавання, мовний аналіз, управління системами прогнозування на основі моделювання і розширених форм пошуку – людина не може конкурувати зі ШІ. Виходячи з цього, додаткової уваги потребує проблема інтеграції технологій ШІ з існуючими технологіями і воєнними платформами, що саме по собі являє безпековий виклик. Така інтеграція ШІ і високоавтономних воєнних систем може призвести до практично блискавичного конфлікту, в якому буде досягнута масштабна одночасна координація сил і засобів, а також їх оптимальне застосування. В результаті невеликі високотехнологічні і високомобільні сили (наприклад БПЛА) під управлінням ШІ завжди матимуть перевагу над переважаючими звичайними бойовими засобами і збройними формуваннями завдяки впливу на них в критичних точках, які ШІ визначатиме набагато швидше і точніше.

З іншої сторони, інтеграція технологій ШІ та існуючих, але застарілих воєнних платформ, здатна багатократно збільшити їх бойову ефективність і ефект від застосування. Як приклад можна навести програму переобладнання Китайською Народною Республікою власних застарілих літаків J-6 і J-7 на безпілотні літальні апарати, що дало можливість зберегти потужний бойовий потенціал ВПС з низькими експлуатаційними затратами. Крім того, така програма суттєво ускладнює оцінку бойових можливостей і планування необхідних сил і засобів для потенційного протистояння повітряним засобам НОАК.

Зазначений вище приклад свідчить, що в сучасних умовах технології ШІ суттєво розширюють спроможності як невеликих країн, так і недержавних суб'єктів щодо нарощування власного безпекового потенціалу. Інтеграція наявних

бойових платформ в сукупності з можливостями в області кібероперацій під загальним управлінням ШІ за умови застосування правильних організаційних підходів дають можливість фактично будь-якому учаснику міжнародної політики успішно протистояти більш потужним в економічному і воєнному плані акторам. Використання недорогих цифрових рішень на основі відкритого коду, електронних засобів комерційного класу, власного програмного забезпечення поряд з готовністю експериментувати і гнучко реагувати на наявні безпекові загрози вирівнює потенціали різних суб'єктів системи міжнародної безпеки. Здавалось би, що такі тенденції в подальшому призведуть до значного зниження рівня воєнно-політичної напруженості в світі. Разом з тим, в ситуації коли кінетичні і кібернетичні засоби можуть застосовуватись на великих відстанях з високою точністю і без участі людини, ймовірність їх безпосереднього використання країнами і недержавними групами і організаціями суттєво зростає. Фактично світ сходить в нову турбулентну зону створену технологічним проривом сучасності, ефекти від якого до кінця не зрозумілі. Ми з однаковою долею вірогідності можемо стикнутись як з укріпленням системи міжнародної безпеки на основі нових технологій, та і з її фактичним демонтажем.

Список використаних джерел:

1. Какое отношение ИИ и пилоты-истребители имеют к электронной коммерции? Объяснения Антуана Блондо из Sentient https://www.ge.com/news/reports/ai-fighter-pilots-e-commerce-sentients-antoine-blondeau-explains.
2. How Great Engineering Managers Identify and Respond to Challenges – the OODA Loop Model - https://waydev.co/ooda-agile-data-driven/.
3. AI vs. Humans: AI Solution Beats Stanford Radiologists in Chest X-ray Diagnostics Competition

   https://hitconsultant.net/2019/08/22/ai-tech-beats-radiologists-in-stanford-chest-x-ray-diagnostic-competition/.
4. AI Reads Handwriting Better Than Us https://www.labroots.com/trending/technology/8347/ai-reads-handwriting.
5. https://news.sky.com/story/ai-algorithm-identifies-50-new-planets-from-old-nasa-data-12057528.
6. China's Autoflight puts a canard twist on its latest long-range eVTOL (newatlas.com).
7. Air Forces Monthly, January 2021.

Олександр ТЕРНОВИЙ
НУОУ
ORCID: 0000-0003-2790-7262
E-mail: zizimota@tutanota.com

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Актуальність дослідження. Поява в суспільстві засобів інформаційної комунікації породила поняття “інформаційна безпека”. У нашому сучасному світі не дивно, що інформаційні технології стрімко розвиваються. Це призвело до збільшення кількості інформаційних систем і програмного забезпечення, призначеного для допомоги персоналу підприємства в управлінні потоком інформації. В результаті збільшився і обсяг цінної інформації. Отже, питання про те, як захистити цю інформацію, є надзвичайно важливим.

Метою роботи є розгляд основних питань по управлінню інформаційною безпекою.

Основний матеріал. Важливо визнати, що в науковій літературі не існує єдиного, узгодженого визначення терміну “інформаційна безпека”. Цю концепцію найкраще можна зрозуміти як стан безпеки для систем, які обробляють і зберігають дані, у якому захищено цілісність, доступність і конфіденційність інформації. Крім того, його можна розглядати як набір заходів, призначених для захисту інформації від доступу, розкриття, зміни, знищення, перевірки, запису або надання неавторизованим особам [1].

Мета захисту інформаційної безпеки полягає в підтримці справжності, цілісності та правильності даних, одночасно пом’якшуючи потенціал будь-яких несанкціонованих змін в інформаційних системах. Захист інформації є надзвичайно важливою відповідальністю для підприємств, оскільки це може суттєво вплинути на їхні фінансові та операційні функції, а згодом і на позиції на ринку. Для забезпечення зростання компанії та її актуальності в галузі життєво важливо створити комплексну систему управління інформаційною безпекою.

Із зростанням обсягу і важливості інформації з'явилися також і загрози для її безпеки. Управління інформаційною безпекою стає вельми актуальною та необхідною складовою сучасного світу [2].

Однією з найбільших загроз для інформаційної безпеки є кіберзлочинці, які використовують різні технології та методи для отримання несанкціонованого доступу до конфіденційної інформації. Віруси, шкідливі програми, фішинг та соціальна інженерія – це лише деякі з їхніх інструментів. Завдяки поширенню Інтернету і збільшенню кількості підключених пристроїв, ризики зростають щодня.

Управління інформаційною безпекою передбачає вжиття різноманітних заходів для захисту інформації від подібних загроз. Важливим компонентом є встановлення сильних паролів та використання двофакторної аутентифікації для ускладнення доступу до систем та даних. Постійне оновлення програмного забезпечення та використання антивірусних програм допомагає запобігти атакам через вразливості. Шифрування важливої інформації забезпечує її захист у випадку несанкціонованого доступу.

Законодавчі аспекти також відіграють важливу роль у сфері інформаційної безпеки. Закони про захист персональних даних, такі як Загальний регламент про захист даних (GDPR) в Європі, зобов'язують компанії дотримуватися строгих стандартів збереження інформації та сповіщати про порушення безпеки даних. Стягнення за порушення інформаційної безпеки може включати значні штрафи та юридичні наслідки.

Культура інформаційної безпеки також важлива. Інформаційна безпека не може обмежуватися лише IT-відділом. Всі співробітники повинні бути свідомі загроз інформаційної безпеки та знати, як правильно діяти в разі підозрілих ситуацій. Навчання персоналу стандартам і правилам інформаційної безпеки є важливим етапом у забезпеченні безпеки даних [3].

У майбутньому інформаційна безпека буде продовжувати еволюціонувати. Зараз ми спостерігаємо застосування штучного інтелекту для виявлення та протидії кіберзагрозам, а також зростання використання блокчейн-технологій для захисту інформації. Глобальний характер інформаційної безпеки вимагає співпраці між країнами та міжнародними організаціями для боротьби з кіберзагрозами.

У заключенні, управління інформаційною безпекою – це критична задача для підприємств і держав. Вона вимагає комплексного підходу, поєднаного з технічними, організаційними та культурними заходами.

Список використаних джерел:

1. Верескун М. В. Методичне забезпечення системи інформаційної безпеки промислових підприємств. Економіка і організація управління. 2014. № 1 (17). С. 54–60.

2. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Humanitarian vision. 2016. Vol. 2, Num. 1. С. 27–32. URL: http:// nbuv.gov.ua/UJRN/hv_2016_2_1_7 (дата звернення: 02.10.2023).

3. Маркіна І. А., Дячков Д. Н. Основи формування системи менеджменту інформаційної безпеки підприємства. Проблеми і перспективи розвитку підприємництва. 2016. № 3(1). С. 80–88.

Марія ХАРДЕЛЬ
ORCID: 0000-0003-4577-781X
E-mail: marishakhardel@gmail.com
Роман ХАРДЕЛЬ, д.ф.
НАСВ ім. гетьмана Петра Сагайдачного
ORCID: 0000-0002-2243-9722
E-mail: spantamano2@gmail.com

ВІКІПЕДІЯ: ЕФЕКТИВНИЙ ІНСТРУМЕНТ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ ВІЙНИ У СФЕРІ ІСТОРИЧНОЇ СВІДОМОСТІ

Російська федерація веде безжальну війну, метою якої є тотальне знищення України, як народу, який осмілився кинути виклик імперським амбіціям росії.

Важливою складовою цієї війни, згідно Доктрини сучасної війни, розробленої начальником російського генерального штабу валерієм герасимовим є інформаційна агресія [1].

Головним завданням інформаційної агресії рф, спрямованим проти України, є дискредитація та подальша ліквідація у суспільній свідомості самого поняття української нації, її культури, а також історичних цінностей українського народу, як одного з головних чинників національної свідомості.

Для реалізації стратегії застосування цієї інформаційної агресії росіяни намагаються отримати контроль над усіма сучасними складовими інформаційного простору.

Одним з найбільш впливових явищ сучасного інформаційного простору виступає доступна всім онлайн-енциклопедія Вікіпедія. Даний ресурс характеризується надзвичайно високими вебометричними характеристиками, а головне – величезним рівнем довіри аудиторії до розміщеної в ній інформації.

Одночасно, склалася розгалужена й складна внутрішня інформаційна інфраструктура, завдяки якій реалізується створення та модерація статей. Хоча у Вікіпедії декларується принцип об'єктивності, нейтральності та неупередженості, насправді функціонує злагоджена та керована з єдиного центру структура агентів впливу, які здатні провадити у Вікіпедії інформаційну політику, що цілком відповідає цілям та завданням інформаційної складової агресивної доктрини росії.

Хоча з початком повномасштабної агресії проти України в російськомовному кластері Вікіпедії відбувалися певні процеси, котрі спрямовані проти інформаційної політики кремля, які знаходили зовнішнє вираження у появі статей. Вони в цілому суперечать офіційній позиції російської влади, в цілому російськомовний сегмент Вікіпедії залишається під контролем відповідних російських владних структур[2]. Характерним прикладом може бути російськомовна стаття "Вторгнення Росії в Україну", що призвела до погроз з

боку роскомнагляду заблокувати російськомовну Вікіпедію[3]. В подальшому ця ситуація трансформувалася до компромісного варіанту, що зрештою так чи інакше влаштувала кремлівських кураторів інформаційного простору[4]. Крім цього, ведеться активна робота зі створення абсолютно підконтрольного кремлю клона Вікіпедії під назвою Руніверсаліс, сторінки якого "редагуються відповідно до вимог законодавства Російської Федерації та з повагою до традиційних цінностей" [5].

Також інформаційний вплив кремля прослідковується й в Українському сегменті Вікіпедії. Більшість інформаційних акцій щодо перейменування, видалення або внесення змін у певні проросійські статті україномовної Вікіпедії, очевидно, є наслідком нескоординованої діяльності патріотів України, які є активними дописувачами та модераторами Вікіпедії [6].

Отже, з метою забезпечення розуміння і формування у світової спільноти правдивого поняття української нації, її культури, історичних цінностей, як одного з головних чинників національної свідомості українського народу, а також безпеки України та протидії російській інформаційній агресії, варто сформувати та забезпечити скоординовану діяльність інформаційної системи, що має складатися з кваліфікованих фахівців, які одночасно є експертами у різноманітних галузях, та достатньо обізнані із внутрішніми правилами, принципами та політикою, що діє у середовищі Вікіпедії.

Список використаних джерел:

1. Герасимов В. Ценность науки в предвидении. Новые вызовы требуют переосмыслить формы и способы ведения боевых действий. *Военно-промышленный курьер.* URL: https://web.archive.org/web/20211220001911/https://vpk-news.ru/articles/14632 (дата звернення 16.09.2022).
2. Википедия в России и в БРИКС. Проблемы и решения (часть 2). *Российский совет по международным делам.* URL: https://russiancouncil.ru/blogs/mihail-lavrov/wikipedia-in-russia-and-brics-part-2/ (дата звернення 16.09.2022).
3. Liffe K. Moscow threatens to block Russian-language Wikipedia over invasion article. *Reuters.* URL: https://web.archive.org/web/20220307170432/https://www.reuters.com/world/europe/moscow-threatens-block-russian-language-wikipedia-over-invasion-article-2022-03-02 (дата звернення 16.09.2022).
3. Обсуждение:Российско-украинская война. *Википедия.* URL: https://ru.wikipedia.org/wiki/Обсуждение:Российско-украинская_война#Однобокость_статьи (дата звернення 24.10.2022).

4. Базовые принципы и планы. *Руниверсалис.* URL: https://руни.рф/Руниверсалис#Базовые_принципы_и_планы (дата звернення 16.09.2022).

5. Ropek L. Researchers Say 'Suspicious' Edits on Wikipedia Reek of Pro-Russian Propaganda. *Gizmodo*. URL: https://gizmodo.com/wikipedia-russia-ukraine-propaganda-suspicious-edits-1849673060 (дата звернення 16.09.2022).

Максим ЧЕПЕЛЬ, д.ф.
ORCID: 0000-0003-1395-7920
E-mail: maxch79@ukr.net
Олександр ЗАГРЕБЕЛЬНИЙ, д.ф.
НАНГУ
ORCID: 0000-0003-1449-6257
E-mail: zagrebus@ukr.net

ДО ПИТАННЯ РОЗРОБЛЕННЯ МЕТОДИКИ МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ШУМУ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ В ІНТЕРЕСАХ СИЛ БЕЗПЕКИ І ОБОРОНИ

Сьогоднішні події, які відбуваються в нашій державі стосуються всіх сфер життєдіяльності суспільства в цілому та кожного громадянина України окремо. Інформаційний простір країни став місцем ведення інформаційної війни, а інформаційно-психологічні операції – звичним явищем, ворог використовує засоби масової комунікації як-то канали та засоби передачі інформаційних повідомлень на великі території та маси [1] в своїх пропагандистських цілях. У великому об’ємі матеріалу ми не завжди можемо відрізнити насправді важливу інформацію від інформаційного шуму – неважливої, вторинної інформації, якою супроводжується або заміщується основне повідомлення [2] і цей ефект активно використовується противником. Інформаційний шум може призводити до спотворення інформації, зниження її якості, штучного перевантаження споживача з метою відведення уваги від важливого контенту. Той факт, що інформаційний шум завдає шкоди не тільки пересічним громадянам, але і безпосередньо впливає на ефективність виконання завдань складовими сектору безпеки і оборони є доведеним і потребує негайного реагування. Задля елімінації наслідків інформаційного шуму потрібно розробити методику моніторингу інформаційного шуму в інформаційному просторі.

На нашу думку, основними етапами цієї методики могли би бути:

ідентифікація сил і засобів, якими насаджується інформаційний шум;

визначення форм, в яких реалізовується інформаційний шум та його спрямованість;

визначення об’єму неважливої (вторинної) інформації за певний проміжок часу, її інтенсивність, середня тривалість та об’єкти, на який направлений інформаційний шум;

визначення ступеня напруженості інформаційної обстановки, яку утворює інформаційний шум;

визначення тенденції (тренду) до збільшення (або зменшення) об’ємів інформаційного шуму;

оцінювання рівня впливу інформаційного шуму та його наслідків.

Наразі розроблення дієвої методики моніторингу інформаційного шуму в інформаційному просторі країни є актуальним завданням відповідних органів і структур.

Список використаних джерел:

1. Різун В. В. Теорія масової комунікації : підручник. Київ : Просвіта, 2008. 260 с.

2. Як працює “інформаційний шум” в дезінформації. URL: https://cpd.gov.ua/category/glossary/principles (дата звернення 18.09.2023).

Олександр ЧЕРВЯКОВ
НУОУ
ORCID: 0009-0008-9482-1593
E-mail: o.chervijkov@i.ua

АНАЛІЗ ІСНУЮЧИХ ЗАСОБІВ АГРЕГУВАННЯ ІНФОРМАЦІЙНИХ ПОВІДОМЛЕНЬ В ІНТЕРЕСАХ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Сьогодні одним із найбільш актуальних завдань в інформаційно-аналітичній роботі стало забезпечення швидкості та якості обробки й аналізу великих обсягів структурованих і неструктурованих даних в інтересах інформаційної безпеки Збройних Сил України. Очевидно, що зростання обсягу інформації актуалізує проблему оптимальних методів роботи з нею. Все більше користувачів глобальної мережі мають потребу у отриманні оперативної й актуальної інформації. Реалізація цього завдання сприяє розвитку нових інструментів, серед яких спеціальні сервіси – агрегатори, які акумулюють інформацію з різних джерел.

Агрегатор новин (іноді RSS-агрегатор) – клієнтська програма або веб-застосунок для автоматичного збору повідомлень із джерел, що експортуються у формати RSS або Atom [1]. Агрегатори бувають двох типів – веб-агрегатори і

програмні, але завдання у них однакові – робота з контентом та отримання оновлень.

Основними перевагами агрегаторів у пошуках онлайн-новин користувачі називають швидкість оновлення і зручність розташування багатьох джерел інформації в одному місці. Зважаючи на кількість, швидкість поширення та зростання популярності агрегаторів новин, на сьогодні можна говорити про два напрямки їх використання: як користувацький інструмент (направлений на задоволення особистих інформаційних потреб) і як професійний (направлений на автоматизацію, покращення та полегшення збору інформації).

Розглянемо сучасні засоби агрегування новинного контенту.

Сервіс Google News – це безкоштовний агрегатор новин забезпечується і управляється Google. Бета-версія була запущена у вересні 2002 року і офіційно випущена в січні 2006 року. Першопочатково ідея була розроблена Крішна Бхарат. 3 червня 2009 року запрацювала українська версія сервісу.

Основними можливостями даного сервісу є:

користувацьке налаштування новин;

тематична класифікація новин за рубриками: країна, світ, місцеві новини, бізнес, наука й технології, розваги, спорт;

новинна стрічка повідомлень, яка включає в себе заголовок, дата публікації, джерело публікації, повний перегляд повідомлення;

поле запиту, для пошуку новин;

місцевий прогноз погоди;

перегляд новин за найбільш актуальними темами.

Ukr.net – один з найбільш відвідуваних сайтів в Україні. Згідно з даними SimilarWeb, у нього 78 млн переглядів на місяць. На головній сторінці сервісу є блок топ-новин і поділ за розділами. Агрегатор самостійно не публікує жодних новин чи статей, стрічка новин створюється автоматично та є підбіркою гіпертекстових посилань на інтернет-сторінки статей, опублікованих на різних інтернет-сайтах України та світу [2]. Посилання, що збираються програмними засобами та розміщуються в релевантній рубриці, представлені у стрічці новин.

Таким чином, до основних переваг агрегаторів можна віднести:

оперативність подачі інформації;

велику джерельну базу;

можливість фільтрування запропонованих інформаційних джерел та додавання нових;

можливість здійснення тематичного пошуку;

тематична підписка;

отримання push-повідомлень;

відображення різних точок зору на інформаційну подію, що відбулася.

Часткова автоматизація процесу відбору інформації під час забезпечення інформаційної безпеки Збройних Сил України за допомогою агрегаторів новин

дає можливість аналітику зосередити увагу на смисловому аналізі інформації, перевірці її на достовірність, повноту та відповідність до запиту.

Отже, аналіз існуючих засобів агрегування інформаційних повідомлень в інтересах забезпечення інформаційної безпеки Збройних Сил України показує, що формування постійне використання росією в офіційній (мзс рф) та політичній площині спеціальних наративів та інформаційних ярликів з метою делегітимізації української влади (“партія війни”, “київська хунта”, “бандерівці”, “фашисти”, “нацисти”), а також кодування суспільної свідомості українців комплексом “молодшого брата”.

Список використаних джерел

1. Агрегатор новин [Електронний ресурс] // Вікіпедія : веб-сайт. – Режим доступу: https://uk.wikipedia.org/wiki/Агрегатор_новин.

2. Геотегування [Електронний ресурс] // Вікіпедія – вільна енциклопедія. – 2017. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Геотегування Про стрічку новин [Електронний ресурс] // Ukr.net : веб-сайт. – Режим доступу: https://www.ukr.net/news/terms.html.

Олег ЧЕРТОК, к.т.н.
ORCID:0000-0003-2178-7909
E-mail: olehchertok@gmail.com
Олег ЛАВРОВ, к.т.н.
ORCID:0000-0003-1292-5986
E-mail: lavrov1107@gmail.com
Юрій КУЧЕРЕНКО, к.т.н, с.н.с.
ХНУПС ім. Івана Кожедуба
ORCID: 0000-0001-9937-371X
E-mail: kucherenkoyf@gmail.com

АКТУАЛЬНЕ ЗАВДАННЯ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СФЕРИ УКРАЇНИ В УМОВАХ ПРОТИСТОЯННЯ РОСІЙСЬКІЙ АГРЕСІЇ

В умовах ведення повномасштабної збройної агресії з боку Російської федерації (РФ), коли відбувається жорстка боротьба міжвидових угруповань військ та їх компонентів не тільки в повітряному просторі, на землі, в морі, а також і в інформаційному просторі з метою отримання інформаційної переваги над противником, здійснюється активне застосування засобів ведення інформаційної боротьби в інформаційній сфері. Зараз РФ веде жорстку інформаційну боротьбу в інформаційній сфері (ІС) України та її складових (медіа простір, державні

електронні ресурси та різні системи державного і військового управління (СДВУ), соціальні мережі та інші інформаційні об'єкти) своїми інформаційними засобами (методами), з метою здійснення впливу на них, за рахунок проведення інформаційних та психологічних операцій. Можна вважати, що сучасні війни за своїми ознаками (застосування високоточних засобів ураження, широкомасштабне інтегроване використання інформаційних, розвідувальних, навігаційних та вогневих засобів у різних сферах ведення бойових дій (БД), масоване впровадження новітніх інформаційних технологій та елементів штучного інтелекту у СДВУ, застосування інтегрованих систем управління військами і засобами, що формують єдиний командно-інформаційний простір (ЄКІП) в зоні ведення БД) стають більш інформаційними, в яких здійснюється проведення певних інформаційних дій та операцій, направлених проти соціальних та інформаційно-технічних систем держави і в першу чергу на СДВУ з метою одержання інформаційної переваги над супротивником.

Тому, на сьогодні, одним з першочергових і актуальних завдань є забезпечення надійного захисту ІС України і її основних елементів, в тому числі СДВУ від комплексної дії інформаційних засобів впливу противника на їх функціонування в умовах ведення інтенсивного інформаційного протиборства. До сучасних засобів інформаційного (психологічного) впливу відноситься сукупність спеціально організованої інформації (методів) та інформаційних технологій (засобів), що дозволяє цілеспрямовано змінювати, знешкоджувати, копіювати, блокувати інформацію, а також долати системи захисту, здійснювати дезінформацію, пошкоджувати функціонування носіїв інформації й інформаційних мереж та впливати на свідомість як окремої особи, так і суспільства, державу (в тому числі політичне (військове керівництво) в цілому.

Стосовно захисту ІС України необхідно вдосконалювати теорію щодо побудови комплексної системи захисту ІС, як інформаційної складової національної безпеки країни та її адаптованості до сучасних викликів і загроз, що динамічна змінюються як зараз, так і у подальшому. Також треба пам'ятати, що інформаційна боротьба ведеться не тільки під час ведення БД але і у мирний час, а засоби її ведення постійно вдосконалюються. В перспективі слід очікувати, що багато країн будуть прагнуть до домінування у світовому інформаційному просторі і витиснення України із зовнішнього та внутрішнього інформаційного ринку, а тому вони будуть вдосконалювати концепції ведення інформаційних війн, в основу яких будуть закладені положення щодо створення засобів небезпечного впливу на ІС інших країн, в тому числі і нашої держави, порушення функціонування ДВСУ та одержання доступу до електронних ресурсів, і в першу чергу до інформації, що містить державну таємницю.

З метою протидії цим інформаційним засобам та заходам впливу на ІС необхідно мати комплексну систему захисту ІС (КСЗІС) держави, яка повинна бути адаптованою до характеру та динаміці зміни методів ведення інформаційної

боротьби у ІС. КСЗІС повинна складатися з основних функціональних підсистем: організаційної підсистеми – повинна проводити аналіз застосування різних інформаційних та психологічних засобів, методів, програм в ІС країни, прогноз їх впливу на всі складові ІС (медіа простір, сегменти мережі інтернет, соціальні мережі, СДВУ, електронні ресурси та суб'єкти інформаційної діяльності) та управління застосуванням відповідних сил і засобів (організаційних елементів і програмно-технічних засобів (методів), програм), спрямованих на захист інформації та свідомості громадян своєї країни та здійснення планування і організації виконання заходів щодо протидії цим загрозам; підсистеми захисту від інформаційного впливу різних інформаційних (психологічних) засобів – забезпечує виконання ряду заходів щодо захисту елементів ІС держави, її елементів і в першу чергу СДВУ від негативної дії технічних та програмних засобів інформаційного впливу, з метою блокування їх дії; підсистеми інформаційного впливу – забезпечує адекватний вплив на дії, які спричинили виникненню певних загроз в ІС держави за рахунок адаптивного застосування необхідних методів (програм та засобів) психологічного впливу на організаційні елементи та технічного впливу на функціонування різних інформаційних засобів (комплексів, систем) та інших елементів ІС недружелюбних країн, що визивають дані загрози.

Функціонування даних підсистем повинно бути тісно взаємопов'язаним та синхронізованим за часом між собою і направлене на здійснення надійного захисту ІС та її елементів (електронні ресурси, СДВУ, інформаційні об'єкти, медіапростір, суспільство, особистість).

Стосовно інформаційного захисту СДВУ, як головних елементів ІС, порушення функціонування яких стає одним з головних завдань при веденні сучасних війн, необхідно, на основі визначених вимог і впровадження КСЗІС, здійснити вдосконалення теорії щодо розробки системи захисту інформації (СЗІ) СДВУ з метою підвищення їх можливостей щодо надійного функціонування і в тому числі, в умовах ведення жорсткого інформаційного впливу на них різними інформаційно-технічними засобами.

СЗІ повинна уявляти собою взаємопов'язану сукупність засобів, методів та заходів, які направлені на запобігання знищення, зміни змісту, несанкціонованого отримання та використання інформації, що циркулює в СДВУ.

Для визначення основних вимог до СЗІ при розробці СДВУ необхідно: проаналізувати методи, засоби і програми, що може використовувати ворог (недружня країна) для порушення функціонування даної системи управління; провести класифікацію загроз за видами, можливим джерелам їх виявлення, характером прояву та визначити їх вагу у відповідності до ступеня їх впливу на функціонування СДВУ, що розроблюється; визначити напрямки вдосконалення існуючих методів, механізмів та засобів з забезпечення інформаційно-технічної безпеки функціонування даних системи управління.

Після чого визначити які основні функціональні завдання повинна вирішувати СІЗ і розробити її організаційно-технічну структуру для конкретної СДВУ, що розроблюється. Система захисту інформації СДВУ повинна представляти собою взаємопов'язану сукупність взаємодіючих між собою для реалізації головної мети – захисту інформації та функціонування даної системи управління всіх засобів, методів та заходів, необхідних для реалізації визначених задач щодо захисту інформації, що визначена і циркулює в неї та буди адаптованою до зміни відповідних загроз як зовнішніх, так і внутрішніх, що впливають на її функціонування.

Вдосконалення СЗІ в СДВУ підвищить надійність функціонування СДВУ в різних умовах обстановки. Впровадження КСЗІС країни є одним з основних завдань держави на сучасному етапі її боротьби за незалежність, свободу та територіальну цілісність, що дозволить забезпечити дотримання відповідного рівня національної безпеки України.

Список використаних джерел:

1. Сектор безпеки і оборони: стратегічне керівництво та військове управління: монографія / Саганок Ф.В., Фролов В.С., Павленко В.І. та ін.; за ред. д.військ.н., проф. І.С. Руснака. Київ: ЦЗ МО та ГШ ЗС України, 2018. 230 с.

2. Странніков А.М. Інформаційна боротьба у воєнних конфліктах другої половини XX століття: монографія. Київ: Альтерпрес, 2006. 191 с.

3. Кучеренко Ю.Ф., Власік С.М., Сальников О.В., Воробйов О.Г. Методологічні аспекти щодо розробки системи захисту інформації в системах управління військового призначення. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2022. № 2(72). С. 65–70. DOI: 10.30748/zhups.2022.72.10.

Інга ШЕРЕШКОВА
НУОУ
ORCID: 0000-0002-8358-9871
E-mail: ingashereshkova@gmail.com

РОЗВИТОК ПСИХОЛОГІЧНОГО САМОЗАХИСТУ ВІЙСЬКОВОСЛУЖБОВЦІВ ЗБРОЙНИХ СИЛ УКРАЇНИ ВІД НЕГАТИВНОГО ВПЛИВУ МЕДІАПЕРЦЕПТИВНОЇ КОМУНІКАЦІЇ

За умов постійного та бурхливого перенаповнення інформаційного простору, застосування технологій маніпулятивного впливу, використання інформаційного середовища у російсько-українській війні та як наслідок спрямування негативного

медіаперцептивного впливу саме на особовий склад військ (сил), військовослужбовцям Збройних Сил України необхідно набувати нових особистісних якостей та властивостей, навичок та компетентностей аби бути спроможними протидіяти таким патогенним впливам.

Підготувати військовослужбовців Збройних Сил України до конструктивного подолання наслідків негативного медіаперцептивного впливу та психологічного дискомфорту за рахунок свідомої спрямованості психологічного самозахисту на виявлені джерела негативного впливу медіаперцептивної комунікації нами було вирішено за допомогою авторської програми розвитку психологічного самозахисту від негативного впливу медіаперцептивної комунікації "Слово – теж зброя!".

Завдання цієї програми полягають у розвитку когнітивно-рефлексивного, емоційно-перцептивного та поведінково-регулятивного компонентів психологічного самозахисту від негативного впливу медіаперцептивної комунікації, зокрема: а) формування знань щодо глосарію ключових понять, зокрема дефінцій "психологічний самозахист", "негативний інформаційно-психологічний вплив комунікації" та "медіаперцептивна комунікація"; б) підвищення рівня обізнаності про показники високого рівня психологічного самозахисту від негативного впливу медіаперцептивної комунікації; в) оволодіння механізмами психологічного самозахисту від негативного впливу медіаперцептивної комунікації; г) формування позитивного ставлення до необхідності психологічного самозахисту від негативного впливу медіаперцептивної комунікації; д) формування здатності розпізнавати психологічні загрози медіаперцептивної комунікації, наявності атрибутів медіаперцептивної комунікації та закономірностей психологічного впливу інформаційних продуктів, що потрапляють до сфери свідомості військовослужбовців Збройних Сил України; здійснювати аналіз та оцінку психологічної маніпулятивності (перцептивності) медіаперцептивної комунікації.

Оскільки, інформація лише тоді стає внутрішнім надбанням особистості, коли вона випробувана, відпрацьована в реальних ситуаціях, хоча і навчальних, тому нашою програмою передбачається використання активних та інтерактивних методів навчання, при цьому їх вибір мотивується метою і завданнями програми, специфікою й потребами нашої аудиторії (криголами, міні-лекції, групові дискусії з означеної проблеми, мозкові штурми, метод незакінчених речень, ігрові вправи, домашні завдання, мультимедійні презентації, аналітична робота в групах тощо).

Основу інформаційно-методичних матеріалів Програми "Слово – теж зброя!" складають авторські розробки (результати теоретико-емпіричних досліджень особливостей психологічного самозахисту від негативного впливу медіаперцептивної комунікації) [1,2,3].

При створенні Програми "Слово – теж зброя!" враховувались результати комплексної психодіагностики індивідуально-психологічних особливостей

психологічного самозахисту від негативного впливу медіаперцептивної комунікації та результати анкетування щодо наявного рівня сформованості психологічного самозахисту військовослужбовця Збройних Сил України від негативного впливу медіаперцептивної комунікації. Ключовим та основоположним моментом у процесі розвитку психологічного самозахисту від негативного впливу медіаперцептивної комунікації є усвідомлення та подолання, виявленої під час психодіагностики проблематики та специфічних особливостей психологічного самозахисту від негативного впливу комунікації саме військовослужбовців Збройних Сил України.

Запропонована програма є комплексним інструментом розвитку психологічного самозахисту від негативного впливу медіаперцептивної комунікації, її можна використовувати як в повному обсязі, так і частково для розвитку окремих його компонентів.

Розробка та впровадження програми розвитку у військовослужбовців Збройних Сил України психологічного самозахисту від негативного впливу медіаперцептивної комунікації здійснювалась у рамках реалізації формувальної частини дисертаційного дослідження, до якої увійшло 62 військовослужбовці військової частини А0139, з яких були сформовані дві незалежні групи: експериментальна група (ЕГ) (31 особа) та контрольна група (КГ) (31 особа). Ці групи були сформовані з однаковим розподілом осіб за п’ятьма рівнями розвитку психологічного самозахисту від негативного впливу медіаперцептивної комунікації, що попередньо було встановлено на констатувальному етапі експерименту.

На початку та в кінці формувального етапу психологічного експерименту з контрольною та експериментальною групами було проведено діагностику психологічного самозахисту від негативного впливу медіаперцептивної комунікації за допомогою авторської анкети “Рівень сформованості психологічного самозахисту військовослужбовця Збройних Сил України від негативного впливу медіаперцептивної комунікації”.

З учасниками експериментальної групи було здійснено впровадження програми розвитку у військовослужбовців Збройних Сил України психологічного самозахисту від негативного впливу медіаперцептивної комунікації “Слово – теж зброя!”.

Розроблена та апробована програма розвитку психологічного самозахисту військовослужбовців Збройних Сил України від негативного впливу медіаперцептивної комунікації “Слово – теж зброя!” підтвердила свою ефективність, оскільки отримані статистично значущі зміни, які продемонстрували військовослужбовці ЕГ порівняно із відсутністю значного прогресу у військовослужбовців зі складу КГ.

Аналіз емпіричних даних вказує на статистично значущі позитивні зміни U-критерію Манна-Уітні за показниками психологічного самозахисту

військовослужбовців Збройних Сил України від негативного впливу медіаперцептивної комунікації та додаткових показників в ЕГ: аналітичного мислення (Uемп = 324, $p \leq 0,05$), навіюваності (сугестії) (Uемп = 290, $p \leq 0,05$), емоційної запальності (Uемп = 200, $p \leq 0,01$), емоційної збудливості (врівноваженості) (Uемп = 101, $p \leq 0,01$), сприйняття інформації (Uемп = 195, $p \leq 0,01$), саморегуляції поведінки (Uемп = 241, $p \leq 0,01$), знань (Uемп = 100, $p \leq 0,01$), умінь (Uемп = 236, $p \leq 0,01$), навичок (Uемп = 341, $p \leq 0,05$), інформаційних загроз військового середовища (Uемп = 155, $p \leq 0,01$).

Загальний показник розвитку психологічного самозахисту військовослужбовців від негативного впливу медіаперцептивної комунікації в ЕГ підвищився на 32%, відповідно до непараметричного U-критерію Манна-Уітні такі зміни можемо вважати статистично значущими на рівні достовірності $p \leq 0,05$ (Uемп=321,5, $p \leq 0,05$), що є позитивним результатом реалізації нашої програми розвитку та виконання завдань експериментального дослідження.

Перспективним напрямом подальшого дослідження проблематики розвитку у військовослужбовців Збройних Сил України психологічного самозахисту від негативного впливу медіаперцептивної комунікації вважаємо опрацювання інструментарію для відомчого моніторингу ризиків та загроз негативного впливу медіаперцептивної комунікації.

Список використаних джерел:

1. Шерешкова І.І. (2022) Атрибути тексту та закономірності його психологічного впливу на людину. *Вісник Національного університету оборони України. Збірник наукових праць,* 1 (65), 132-141.
2. Шерешкова І.І. (2020) Поняття “психологічний самозахист” в системі загально-наукової універсалії “захист”. *Вісник Національного університету оборони України. Збірник наукових праць*, 5 (58), 201-207.
3. Шерешкова І.І. (2021) Психолінгвістичне маніпулювання текстових повідомлень. *Baltic Journal of Legal and Social Sciences, Number 3. Riga, Latvia : “Baltija Publishing”,* 183-192.

СЕКЦІЯ 5: ВНУТРІШНІ (КРИЗОВІ) КОМУНІКАЦІЇ

Олександр БІНЬКОВСЬКИЙ, к.в.н., доц.
НАДПСУ ім. Богдана Хмельнитцького
ORCID: ID 0000-0002-3581-3963
E-mail: Oleksandrbaa1003@gmail.com

АКТУАЛЬНІ ПИТАННЯ СТРАТЕГІЧНОЇ КОМУНІКАЦІЇ В ІНТЕРЕСАХ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДЕРЖАВНОГО КОРДОНУ УКРАЇНИ

Агресія Російської Федерації проти України, особливо в частині інформаційної війни, обумовила пошук адекватних рішень на національному рівні, зокрема в контексті вироблення інтегрованих підходів ефективного застосування механізмів стратегічних комунікацій.

При цьому особливості пошуку таких підходів повинні відповідати основним критеріям демократичного устрою України, дотримання концепцій свободи слова, відсутності обов'язкової ідеології та інших здобутків демократичного суспільства і не ставати на рейки зухвалої пропаганди на кшталт країни-агресора.

Сектор безпеки і оборони України, як об'єднуюча інституція правоохоронних органів та військових формувань є основним локомотивом розвитку системи забезпечення національної безпеки у цілому та системи стратегічних комунікацій, зокрема.

Закон України "Про державний кордон України" (далі Закон) чітко визначає об'єктову сутність державного кордону в загальнодержавній системі забезпечення національної безпеки, акцентуючи увагу на тому, що державний кордон України є відображенням територіальної цілісності, політичної та економічної незалежності, суверенітету та єдності України. Державний кордон України є недоторканним. Наразі, стає відразу зрозумілою глибинна сутність державної стратегії у воєнному протистоянні України з Російською Федерацією щодо виходу сил оборони держави на кордони 1991 року.

Захист державного кордону є невід'ємною частиною загальнодержавної системи забезпечення національної безпеки яка полягає у скоординованій діяльності військових формувань та правоохоронних органів держави, організація і порядок діяльності яких визначаються законом. Ця діяльність провадиться в межах наданих їм повноважень шляхом вжиття комплексу політичних, організаційно-правових, дипломатичних, економічних, військових, прикордонних, імміграційних, розвідувальних, контррозвідувальних, оперативно-розшукових, природоохоронних, санітарно-карантинних, екологічних, технічних та інших заходів.

Координація діяльності із захисту державного кордону України утворених відповідно до законів України військових формувань та правоохоронних органів здійснюється у мирний час Державною прикордонною службою України, у межах ділянок державного кордону України в районах ведення воєнних (бойових) дій, визначених Головнокомандувачем Збройних Сил України, - відповідним військовим командуванням, а у межах у межах ділянок державного кордону України, на яких здійснюється прикриття державного кордону України, - органом військового управління Збройних Сил України.

Аспекти стратегічної комунікації в інтересах захисту державного кордону пропонується розглянути не тільки з точки зору удосконалення її окремих комунікативних компонент та реалізації координаційних функцій прикордонного відомства чи Збройних Сил України, а з точки зору дослідження більш перспективних її моделей.

Динаміка життя державного кордону супроводжувалась і буде супроводжуватись надалі постійним тиском політичного, економічного та воєнного характеру з боку Росії та її сателіта Республіки Білорусь, якщо воєнно-політичний курс цих держав залишиться без кардинальних змін.

Їх інформаційно-ідеологічні парадигми прогнозовано будуть базуватись на стратегічних та малих наративах щодо:

історичних аспектів приналежності прикордонних територій;

порядку встановлення та проходження державного кордону, його делімітації та демаркації;

національних особливостей, культурної та релігійної спадщини;

аспектів добросусідства, міждержавного та регіонального співробітництва;

функціонування органів державної влади та місцевого самоврядування, правоохоронних органів та військових формувань на державному рівні та в прикордонні України;

законності прикордонних та митних процедур;

своєчасності та доцільності запровадження прикордонних, імміграційних, природоохоронних, санітарно-карантинних та екологічних обмежень, тощо.

І це тільки загальний їх перелік. Питання більш широкого спектру лежить у площині варіативності завершення війни, реформаторських змін у середині держави, питаннях розвитку прикордонних регіонів України. Безумовно, що будь-які позитивні зрушення в Україні будуть супроводжуватись активізацією пропаганди, формуванню негативних наративів серед міжнародної спільноти та населення нашої держави.

Їх стратегічна мета зрозуміла – створення та підтримання політичної, економічної, воєнної та соціальної напруги на національному та міжнародному рівнях, зокрема і щодо ймовірності реалізації чергового сценарного варіанту перегляду кордонів, залякуючи усіх відновленням воєнного протистояння.

Беручи за основу характер визначених загроз, можна сформулювати мету створення, подальшого дослідження та перспективного застосування інтегрованої моделі стратегічних комунікацій сектору безпеки і оборони в інтересах захисту державного кордону України.

Отже, її метою слід вважати – інтегроване, скоординоване і належне використання комунікативних можливостей правоохоронних органів та військових формувань сектору безпеки і оборони для просування і захисту національних інтересів держави на державному кордоні України в рамках: публічної дипломатії, зв'язків із громадськістю, правоохоронних та військових зв'язків, інформаційних і психологічних операцій, інших заходів.

Основними принципами, що визначають порядок функціонування моделі стратегічних комунікацій у сфері захисту державного кордону України, є її інтегрованість, законність і демократизм, цілеспрямованість, інформативність, гнучкість, взаємодія та координаційна спроможність. Розглянемо визначені принципи більш детально.

Інтегрованість моделі передбачає здійснення паралельних процесів комунікативної активності складових сектору безпеки і оборони, а також в системі стратегічної комунікації Міністерства внутрішніх справ України.

Її законність та демократизм полягає у пошуку таких підходів до контенту стратегічної комунікації, який відповідатиме законно визначеним та проголошеним національним цінностям, основним критеріям демократичного устрою України, дотримання концепцій свободи слова, прав людини і громадянина.

Цілеспрямованість моделі це чіткість і зрозумілість мети стратегічної комунікації, визначеність цільової аудиторії в національному та міжнародному суспільному середовищі, а при проведенні інформаційних та психологічних операцій конкретність у визначенні їх об’єктів та прогнозованих кінцевих результатів.

Інформативність моделі передбачає сконцентровану та актуалізовану сукупність інформаційного контенту у форматі стратегічних та малих наративів, що об’єктивно та у повній мірі характеризують та розкривають основні аспекти державної політики у сфері безпеки державного кордону, діяльність державних та правоохоронних органів, військових формувань на державному кордоні в мирний час та при введенні різних правових режимів.

Гнучкість моделі вказує на швидку варіативність змін інформаційного контенту, переорієнтації зусиль та напрямків роботи, тощо.

Взаємодія і координаційна спроможність моделі базується на засадах взаємоузгодженої діяльності, уникнення ситуацій, коли інформаційна діяльність одних структур призводить до ускладнення (чи неможливості) інформаційної діяльності інших структур. Запропонована для розгляду ідея потребує принципового дослідження фахівцями сектору безпеки і оборони України.

Список використаних джерел:

1. Закон України “Про державний кордон України” (Відомості Верховної ради України (ВВР), 1992, № 2, ст.5).
2. Бринцев В. В. Державне управління: питання теорії і практики у воєнній сфері в Україні : навч. посіб. НУОУ ім. Івана Черняховського. Київ, 2017. 176 с.
3. Пунда Ю. В., Грищенко В. П., Грицай П. М. Основи воєнної безпеки держави : підруч. НУОУ ім. Івана Черняховського. Київ, 2017. 204 с.

Михайло БОЧАРОВ, к.в.н.
НУОУ
ORCID: 0000-0001-9198-3855
E-mail: mboch75@gmail.com
Ілля ЧАЙКОВСЬКИЙ, к.мед.н., доц.
Інституту кібернетики імені В.М. Глушкова НАН України
ORCID: 0000-0002-4152-0331
E-mail: illya.chaikovsky@gmail.com
Антон ШАРИПАНОВ, к.т.н.
Інститут проблем математичних машин і систем НАН України
ORCID: 0000-0001-6804-0533
E-mail: anton.sha.ua@gmail.com
Софія ПАРОВСЬКА
в/ч 3027 НГУ
E-mail: siciliya14@gmail.com

ОЦІНЮВАННЯ ПСИХОЛОГІЧНОЇ ГОТОВНОСТІ ВОЇНІВ СИЛ ОБОРОНИ УКРАЇНИ ЯК ІНСТРУМЕНТ УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЙНОЇ СТРУКТУРИ ПІДРОЗДІЛІВ ВІЙСЬК (СИЛ)

Актуальність. Результати аналізу воєнних конфліктів останніх десятиріч вказують на стійку тенденцію до збільшення частки інформаційно-психологічних операцій. “Гібридні” умови бойових дій посилюють невпевненість, страх в особового складу та значно збільшують ймовірність його психічного травмування. При цьому головним інструментом протидії такому впливу і мотиваційним чинником, який впливає на досягнення успіху в бойовій обстановці, визначено заходи внутрішньокомунікаційної роботи в системі стратегічних комунікацій ЗС України, метою яких є забезпечення ефективного обміну цільовою інформацією між окремими підрозділами, командирами та підлеглими.

Стійке збільшення інформаційної складової в ході російсько-української війни потребує одночасного удосконалення системи стратегічних комунікацій ЗС України, реструктуризації органів військового управління та організаційної структури підрозділів військ (сил). Однак в умовах війни кожне таке рішення має бути максимально виваженим, тому в експерименті з удосконалення організаційної структури військ (сил) доцільно передбачити об'єктивне оцінювання ефективності вищезазначеного процесу.

Одним з небагатьох важливих показників бойової готовності військових частин (підрозділів) військ (сил), який безпосередньо пов'язаний із заходами внутрішньокомунікаційної роботи та може бути оцінений об'єктивно, є психологічна готовність захисників України до бойових дій.

Отже, адекватні методи експрес-оцінювання психологічної готовності особового складу військ (сил) у бойових умовах можуть забезпечити якість проведення низки експериментів удосконалення системи стратегічних комунікацій ЗС України, реструктуризації органів військового управління та організаційної структури підрозділів військ (сил).

Водночас, зниження адекватності підходів до моніторингу психологічної готовності ускладнює підтримання командирами, їх заступниками головної умови реалізації бойового потенціалу військ – "пориву до знищення ворога" (за визначенням К. Клаузевіца).

Так, у 2014–2015 роках, в умовах інтенсивних бойових дій в ході антитерористичній операції на Сході України, психічних травм різної тяжкості зазнали близько 80% вояків, що на 50% більше сталих 50–55%.

Саме тому визначення можливості експрес-оцінювання психологічної готовності особового складу військ (сил) у ході експериментів з удосконалення системи стратегічних комунікацій ЗС України, органів військового управління та організаційної структури підрозділів військ (сил) є важливим науково-практичним завданням і метою нашого дослідження.

Сукупність маркерів вимірювання психологічної готовності військовослужбовців до бойових дій не є повною та потребує вивчення сутності і складових функціонального стану (ФС) людини.

У цілому ФС потребує інтегрального оцінювання функцій, які прямо або опосередковано зумовлюють ефективну діяльність військовослужбовців в різних умовах діяльності видів та родів військ (сил).

Загальними складовими функціонального стану визнано когнітивну, психоемоційну та ресурсно-енергетичну.

Когнітивна складова характеризує здатність до опрацювання інформації, її оцінюють за допомогою бланкових і комп'ютерних об'єктивних тестів.

Психоемоційна складова характеризує емоційний стан, значною мірою дотична до підсвідомості, її оцінюють здебільшого за допомогою суб'єктивних анкетних опитувальників, а також у ході діагностичної співбесіди з психологом.

Іншим сучасним інструментом для об’єктивного аналізу психоемоційної складової є досить нові апаратні методики, наприклад оцінювання деяких особливостей спектральних параметрів варіабельності ритму серця.

Ресурсно-енергетична складова характеризує здатність організму забезпечити метаболічними ресурсами виконання певної діяльності її оцінюють за допомогою об’єктивних фізіологічних та психофізіологічних методів.

Визначено, що серцево-судинна система відображає функціональний стан вегетативної та нейроендокринної регуляції.

За допомогою створених в Інституті кібернетики імені Віктора Глушкова НАН України інноваційних програмно-апаратних електрокардіографічних комплексів (керівник розробки – І.А. Чайковський) у стаціонарних і польових умовах проведено численні дослідження спрямовані на визначення функціонального стану та фізіологічної ціни діяльності воїнів Сил оборони України за різними сценаріями бойових умов.

Так, для реалізації угоди про наукове і науково-технічне співробітництво від 01 квітня 2020 року в ході спільних досліджень з Національним університетом оборони України вивчено функціональний стан достатньої кількості різних категорій військовослужбовців за варіантами експрес-діагностики та довготривалого моніторингу в умовах навчальної, службової і бойової діяльності та доведено:

експрес-діагностика функціонального стану військовослужбовців за фізіологічними та психоемоційними показниками дає змогу об’єктивно визначати індивідуальну оперативну готовність кожного військовослужбовця до виконання завдань і швидко ухвалювати рішення про поліпшення зазначених важливих компонентів боєздатності особового складу;

довготривалий моніторинг функціонального стану військовослужбовців за вказаними показниками дає змогу запобігати критичному перевищенню його фізіологічних та психоемоційних можливостей, прогнозувати готовність підрозділу до тривалих бойових дій.

Наприклад, у ході визначені функціонального стану воїнів кількох стрілецьких підрозділів під час бойового злагодження за допомогою мініатюрних приладів з пальцевими електродами українського виробництва виявлено статистично достовірну різницю у показниках вегетативного резерву та психоемоційного стану між групами військовослужбовців старших та молодших 40 років.

Протягом 2023-2024 років у бойових підрозділах Національної гвардії України під час ротації, на початку заходів з відновлення боєздатності та після прибуття з відпустки, перед поверненням у зону бойових дій за допомогою зазначеного програмно-апаратного комплексу обстежено понад 1000 військовослужбовців. Виявлено, що у більшості військовослужбовців, виведених на ротацію, спостерігається зниження показника психоемоційного

стану, яке у багатьох поєднується з тонкими змінами, що вказує на погіршення стану серцевого м'яза. Найменшою мірою змінювався показник загального функціонального резерву військовослужбовця. Виявлено значні відмінності у профілі зниження зазначених показників у військовослужбовців віком до 30 років і старшого віку. У молодших військовослужбовців показники психоемоційного стану знижувалися більшою мірою і менше відновлювалися після відпустки, на відміну від показника стану серцевого м'яза. Очевидно, ці факти вказують на меншу цілісність особистості молодих бійців. Також зауважимо що у багаторазово контужених бійців збільшується частота аритмій.

Таким чином, проведені дослідження підтверджують можливість експрес-оцінювання психологічної готовності воїнів Сил оборони України в ході анонсованих керівництвом ЗС України експериментів з удосконалення системи стратегічних комунікацій, органів військового управління та організаційної структури підрозділів військ (сил).

Анатолій ГОЛОТА
ХНУПС ім. Івана Кожедуба
ORCID: 0000-0002-1574-4163
E-meil: kozak1955g@meta.ua

ВНУТРІШНІ КОМУНІКАЦІЇ ЯК СКЛАДОВІ СИСТЕМИ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ТА СИСТЕМИ МОРАЛЬНО-ПСИХОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ

У Стратегії воєнної безпеки України від 25 березня 2021 року, визначено, що одним із заходів всеохоплюючої оборони України є нав'язування своєї волі в інформаційному просторі. Також там вказано, що формування та реалізація ефективної воєнної політики ґрунтується, зокрема, на стратегічних комунікаціях та інформаційній політиці у воєнній сфері. У свою чергу в Стратегії інформаційної безпеки від 28 грудня 2021 року, була поставлена стратегічна ціль – створення ефективної системи стратегічних комунікацій.

Сьогодні в умовах воєнної агресії та інформаційної війни з боку РФ постановка цього питання набула особливої актуальності, адже після другої світової війни йде найбільше за масштабом військове протистояння, яке сформувало небувалу коаліцію прихильників України, прицьому визначило певну нерішучисть держав загального півдня та неоднорідність бачень певних держав світу щодо ведення війни до повного звільнення України від окупанта, окремі відмінності у висвітленні ходу бойових дій та стану внутрішньополітичних відносин. Все це потребує термінової і повної реалізації системи стратегічних комунікацій в інтересах підтримки іміджу України та високого морального духу

захисників нашої держави, недопущення різнобічного висвітлення ходу бойових дій, формування та реалізації стратегічних наративів серед наших прихільників, противників та хитких для їх схиляння в бік України, недопущення внутришньо-політичних напружень через факти корупції, окремі випадки неналежного забезпечення бойових підрозділів, соціальний захист ветеранів тощо.

В цьому контексті треба звернути увагу на те, що Енциклопедія сучасної України пропонує таке розуміння інформаційної війни: "Інформаційна війна" – вплив на населення іншої *країни у мирний або військовий час* через розповсюдження певної інформації та захист громадян власної країни від такого впливу [1]. Проти України активно проводяться інформаційно-психологічні операції та інформаційно-психологічні впливи, що складають *єдину систему операцій* з взаємопов'язаними цілями, спрямованими на зниження рівня *морально-психологічного стану особового складу* Збройних Сил та інших структур сектору безпеки і оборони [2]. Повністю погоджуємось з думкою Почепцова Г., який розглядає інформаційну війну як "…комунікативну технологію впливу на масову свідомість з *короткочасними та довгостроковими цілями*" [3]. Тобто інформаційні війни йдуть безперервно.

На нашу думку система МПЗ виконала свою важливу роль у збереженні вертикалі керування процесами у сфері самоідентифікації та впровадження національно-державницької ідеології і стала перехідним етапом до державного рівня впливу на формування належного морально-психологічного потенціалу (морального духу) військовослужбовців Збройних Сил України. Реалізація духовного потенціалу держави повністю відноситься до інформаційної сфери та сфери комунікацій і співпадає із завданнями державних стратегічних комунікацій щодо нав'язування своєї волі в інформаційному просторі, в які вже включені заступники командирів з МПЗ із своїми підлеглими через сферу внутрішніх комунікацій. Так склалося у часі, що назрілий перехід від відомчої системи морально-психологічного забезпечення до державної концепції використання духовного потенціалу (забезпечення морального духу) військ об'єктивно співпадає з розвитком нового військово-політичного функціоналу – Стратегічних комунікацій. І хто як не заступники командирів з МПЗ на даний час володіють знаннями і здібностями, щоб прийняти на себе завдання системи СК, які мають здійснюватись на всіх рівнях військового управління. Вбачається, що настав час відбутись об'єднанню систем МПЗ та СК в єдиній інформаційній сфері.

При цьому є дуже важливим не зробити поспішних організаційних рішень в умовах ведення війни. На час ведення бойових дій існуючі структури МПЗ треба зберегти як актуальні. Але при цьому треба визначити, що їх реальні повноваження не відповідають назві їх відомчої структури. Доцільно здійснити трансформацію посад заступників командирів з МПЗ у посади заступників командирів *з питань* МПЗ, або заступників з морально психологічної підготовки, а краще ще б заступників командирів із стратегічних комунікацій. Це є сфери

діяльності, де реалізуються конкретні практичні завдання, форми і методи роботи посадових осіб цих структур.

При цьому термін “морально-психологічне забезпечення” в силу чисельних факторів, які формують МПС особового складу, має бути “своїм” для всіх без виключення структур управління, кожного командира і начальника. Це сфера суспільної свідомості, яка є складовою діяльності всіх посадових осіб. Назва структур МПЗ не повинна дезорієнтувати всі інші структури щодо їх ролі у питаннях МПЗ. Завдання щодо МПЗ мають були включені у обов’язки всіх посадових осіб без очікування ними відповідних рекомендацій з боку будь-яких керівних структур в мирний і особливий період. Заступники ж командирів із стратегічних комунікацій мають вирішувати спеціальні завдання щодо аналізу СПО, оцінки МПС, недопущення негативного інформаційно-психологічного впливу, ідеологічної роботи, військово-іпатріотичного виховання тощо.

Потребує уточнення словосполучення “вплив на свідомість і психіку” особового складу, адже відповідно до Академічного тлумачного словника психіка є продуктом діяльності кори великих півкуль головного мозку. Ця діяльність називається вищою нервовою діяльністю. Свідомість – вищий етап розвитку психіки, її виникнення обумовлене трудовою діяльністю в умовах колективного спілкування. Свідомість це процес відображення дійсності мозком людини, який охоплює всі форми психічної діяльності й зумовлює цілеспрямовану діяльність людини. Тобто вплив на свідомість людини, як вищої форми психіки, є достатнім.

Треба всім зрозуміти, що заходи Стратегічних комунікацій реалізуються на всіх рівніх військового управління: стратегічному, оперативному і тактичному.

Психологічна підготовка особового складу – це завдання безпосередніх командирів, сержантів. Тобто навчання за принципом “Роби як я”. Це немає відношення до структур МПЗ, крім занять загального характеру з основ психології. Товма І.М. вважає, що здійснювати психодіагностику психоемоційного стану військовослужбовців-учасників бойових дій повинен психолог. На відміну від цивільних психологів, які розглядаються як фахівці вузького профілю, діяльність військового психолога включає в себе психодіагностику, психопрофілактику, психологічну підготовку, соціально-психологічну адаптацію та психологічне консультування військовослужбовців. Має бути окрема самостійна психологічна служба з відповідними дипломованими фахівцями та з додержанням положень Етичного кодексу психолога.

Особливого значення в умовах гібридних війн набуває світоглядно-інформаційна стійкість військовослужбовців, оскільки саме від їх психологічного стану, рівня патріотизму, фахової підготовки, ціннісних переконань залежить обороноздатність держави. Світоглядно-інформаційна стійкість військовослужбовців являє собою синтез переконань, цінностей, принципів та ідеалів національно-патріотичного спрямування з всебічною поінформованістю

щодо процесів та явищ, які відбуваються в середині країни та за її межами. Зміцнення світоглядно-інформаційної стійкості військовослужбовців не можливе без глибоких знань щодо різних сфер суспільного життя та навичок критичного мислення задля якісного сприйняття, оброблення та інтерпретації інформаційних потоків. Розуміння сутнісних характеристик світоглядно-інформаційної стійкості військовослужбовців безпосередньо корелюється з такими феноменами як духовна безпека, інформаційна безпека, культурно-історична самоідентифікація, національно-патріотичне виховання тощо [4]. І в цьому є головна роль внутрішніх комунікацій.

Список використаних джерел:

1. Інформаційна війна. – (Енциклопедія сучасної України). URL: https://esu.com.ua/sear ch_articles.php?id=12460 (звернення: 23.09.2023).
2. Інформаційно-психологічна боротьба у воєнній сфері: монографія / Г.В. Півцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. – Х.: Вид. Рожко С.Г., 2017. – 276 с.
3. Почепцов Г.Г. Информационные войны. Основы военно-коммуникативных исследований. Москва: “Рефл-бук”, Киев: “Ваклер”, 2000. 576 с.
4. Калиновський Ю.Ю. Світоглядно-інформаційна стійкість військовослужбовців в умовах гибридної війни / Ю.Ю. Каліновський // XVIII міжнародна наукова конференція Харківського національного університету Повітряних Сил імені Івана Кожедуба*“Новітні технології – для захисту повітряного простору”: тези доповідей*, 27 – 28 липня 2022 року. – Х.: ХНУПС ім. І. Кожедуба, 2022. – 660 с.

Людмила ГОНТАРЕНКО, к. псих. н., доц.
НУЦЗУ
ORCID: 000-0001-69935494
E-mail: Lgontarenko910@gmail.com

НЕОБХІДНІСТЬ ЗМІН СОЦІАЛЬНО-СТРАТЕГІЧНИХ КОМУНІКАЦІЙ

Російська Федерація широко використовуючи дезінформацію, відверті маніпуляції, пропаганду та інші підходи до управління інформаційними потоками з деструктивними цілями. Наявність на території нашої держави значної кількості об'єктів підвищеної небезпеки з вичерпаними технічними та технологічними ресурсами, створює реальні загрози життєдіяльності населення, подальшому соціально-економічному розвитку та національній безпеці України. Крім того тероризм сусідньої держави несе все більше значних економічних, соціальних,

політичних, демографічних та екологічних втрат не тільки Україні, але і світовій спільноті вцілому. Нав'язуючи нову комунікативну стратегію міжнародним організаціям, державам [2], органам місцевого самоврядування у вирішенні зовнішніх і внутрішніх проблем, вони змушені нагальні питання перевести в площину обговореннння, не вирішуючи питання по суті.

Тероризм Росії вже призвів до цілої низки негативних наслідків: соціальні - масові захворювання людей з важким перебігом хвороби та високим ступенем летальних випадків, паніка, страх, нервово-психічні розлади, інвалідність, параліч волі, виснаження медичних ресурсів, висока смертність серед медичного персоналу, порушення роботи лікувальних установ, падіння життєвого рівня громадян; економічні - колапс економіки країни, захворювання і падіж продуктивних сільськогосподарських тварин, знищення врожаю культурних рослин, які є основним джерелом харчування населення, зростання числа біженців, розруха, дискредитація країни на світовому ринку як торгового партнера, надмірні матеріальні і фінансові витрати на проведення протиепідемічних, карантинних та інших заходів, самопараліч транспортної системи; політичні – усунення або шантаж небажаних політичних лідерів, створення обстановки недовіри до керівництва країни, активізація діяльності політичної опозиції; демографічні – істотне скорочення чисельності населення; військові – приховане виведення з лав збройних сил військовослужбовців евентуального або реального супротивника без вступу в контакт з його збройними силами.

Інформаційне протистояння військовим загрозам про дійсні наслідки агресивних дій Росії та поширення правдивої інформації допоможе вибудовувати нові стратегічні комунікації в світових організаціях [1]. Світ як система повинен реагувати на зміни своєї цілісності уявлень, захистити від руйнації всю його цілісність.

Заходи в межах стратегічних комунікацій повинні стати зрозумілими і чіткими, без можливосте й відхилення [3], що досягти цілей не тільки в національних інтересах, а й світу в цілому. А інформаційна діяльність не призводила до протиріч та взаємознищення.

Список використаних джерел:

1. Akcinaroglu, S., Tokdemir, E. (2018). To Instill Fear or Love: Terrorist Groups and the Strategy of Building Reputation. Conflict Management and Peace Science, 35(4), 355-377.

2. Antipova, O. (2023). Strategic communications as a component of state information security. Law Journal of the National Academy of Internal Affairs, 13(1), 44-52. doi: 10.56215/naia-chasopis/1.2023.44.

3. Требін, М. П. (2019). Феномен тероризму: розуміння сутності. “Вісник НЮУ імені Ярослава Мудрого”. Серія: Філософія, філософія права, політологія, соціологія, 2(41), 88–102. https://doi.org/10.21564/2075-7190.41.168239.

Кіра ГОРЯЧЕВА, к.екон.н, доц.
ВІКНУ ім. Тараса Шевченка
ORCID: 0000-0003-1503-4425
E-mail: horyachevakira@gmail.com

ПРОФІЛІ ЛІДЕРСЬКИХ КОМПЕТЕНЦІЙ ДЛЯ ІННОВАЦІЙНИХ ДІЯЧІВ У НАУКОВО ОРІЄНТОВАНІЙ ДОСЛІДНИЦЬКІЙ ТА ІННОВАЦІЙНІЙ ІНСТИТУЦІЇ

Інновації стали критично важливими для країн, організацій, інституцій та окремих людей у світі, який стає дедалі складнішим. Лідери, відповідальні за інновації, повинні бути компетентними у впровадженні інновацій. Проте багато хто визнає, що вони не впевнені щодо успішності їхньої практики. Компетенції для інноваційного лідерства можуть відрізнятися від тих, що використовувалися раніше для розробки та досягнення оперативних та стратегічних цілей [1]. Дослідження компетенцій інноваційного лідерства видаються обмеженими і фрагментарними. На сьогодні майже немає свідчень того, що з’являється сукупний і узгоджений масив знань на цю тему. Хоча внесок у цю галузь знань зростає, основна увага приділяється окремим дисциплінам чи елементам, а не комплексному чи системному огляду основних компетенцій, необхідних для досягнення успіху. Автором актуалізується питання створення профілю компетенцій для інноваційних лідерів. Може бути розроблений на основі досліджень, проведених у науково-дослідницькій та інноваційній інституціях. Цей профіль має включає компетенції, виявлені в основній вибірці лідерів, чиє лідерство призвело до створення нових знань або винаходів, а також до впровадження їх цільовими реципієнтами в комерційних і некомерційних або суспільно корисних доданих вартостях. За основу варто брати перелік лідерських компетенцій з різних джерел, включаючи авторів високорейтингових наукових статей, комерційні програми розвитку лідерських якостей, спостереження дослідників та відповіді респондентів. Респонденти можуть пройти анкетування, щоб вказати, наскільки важливими, на їхню думку, є ті чи інші компетенції для успішних інноваційних лідерів. Отриманий в результаті профіль пропонує структуру, яка може стати підтвердженою моделлю в ході подальших досліджень. Зацікавлені сторони, які можуть отримати користь від цієї інформації, включають самих інноваційних лідерів, тих, хто призначає таких лідерів для

управління інноваціями, а також тих, хто забезпечує навчання та розвиток лідерів.

Пропонується створити набір лідерських компетенцій, які можуть бути інтегровані в профіль. Такий профіль покликаний принести користь нинішнім і майбутнім лідерам, їхнім організаціям, постачальникам послуг та інноваційній професії, що тільки формується, запропонувавши деякі результати дослідження, засновані на практиці успішних інноваційних лідерів у науково орієнтованій дослідницькій та інноваційній інституції.

Важливою необхідністю для розкриття теми є відображення сучасного розуміння понять інновацій, лідерства, інноваційного лідерства, компетентності та профілю, що слугуватиме основою для розробки профілю компетентності інноваційного лідерства. Отриманий профіль може слугувати основою для розробки та перегляду програми розвитку інноваційних лідерів.

Велика кількість внесків у базу створених профілів є специфічними для окремих дисциплін і фрагментарними за своєю природою. Наслідком фрагментарних внесків є відсутність інтегрованих відповідей на реальні проблеми. Такий внесок залишає важливого бенефіціара управлінських досліджень – керівника – із завданням інтегрувати елементи в більш системну, узгоджену структуру, придатну для практичних дій. В результаті можливе створення профілів компетенцій, які не належать до певної галузі знань і не замасковані під статистичні дані, але які можна використовувати для покращення лідерських компетенцій і результатів за короткий проміжок часу.

Список використаних джерел:

1. Сергеєва Л. М., Кондратьєва В. П., Хромей М. Я. Лідерство: навч. посібн. /за наук. ред. Л. М. Сергеєвої. – Івано-Франківськ. “Лілея НВ”. 2015. – 296 с.

2. Horiacheva K. (2023). Formation of Military Leadership Through the Lens of History. Revista Cuestions Politicas. (Web of Science).

3. Ryzhykov V., Horiacheva K. (2023). Substantiation of the content and structure of organizational and pedagogical conditions for the professional growth of researchers of educational and scientific institutions of the Ministry of Defense of Ukraine in the structure of scientific knowledge. Scientific innovations and advanced technologie. Vol.7.

Елеонора ГУСЬКОВА
НУОУ
ORCID: 0000-0002-2884-2889
Роман БАКУМЕНКО, к.пед.н.
НУОУ
ORCID: 0000-0003-3381-2075
E-mail: e.guskova@edu.nuou.org.ua
Тетяна ВОЙТКО
НУОУ
ORCID: 0000-0002-4326-0633

СТРАТЕГІЧНІ КОМУНІКАЦІЇ ЯК МЕХАНІЗМ ФОРМУВАННЯ ДОВІРИ ДО СИЛ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ ПІД ЧАС РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Україна зіткнулася з однією з найбільших викликів своєї сучасної історії – російсько-українською війною, що триває з 2014 року. Ця конфліктна ситуація вимагає від сил безпеки та оборони країни не тільки фізичної міцності, але й підтримки та довіри з боку населення. Один із ключових інструментів для досягнення цього є стратегічні комунікації (StratCom).

Об'єднана доктрина союзників AJP-10 визначає стратегічні комунікації як функцію командної групи, яка відповідальна за розуміння інформаційного середовища для всіх відповідальних аудиторій і, на основі цього розуміння, використовуючи всі засоби комунікації – включаючи дії, зображення, слова – для належного інформування та впливу на ставлення та поведінку аудиторії через наративний підхід у пошуках бажаного кінцевого стану.

Іншими словами, стратегічні комунікації – це системний підхід до управління інформаційними потоками, спрямованими на формування позитивного сприйняття та довіри до конкретної організації або держави. У випадку України, стратегічні комунікації мають за мету не лише інформувати громадян про події на фронті, але й побудовувати їхнє розуміння, сприяти об'єднанню суспільства навколо цілей національної безпеки та оборони.

Зазначимо, що під час російсько-української війни Україна стикалася з численними викликами у сфері стратегічних комунікацій. Зокрема:

Дезінформація: як свідчать результати опитування, проведеного соціологічною службою Центру Разумкова з 22 лютого по 1 березня 2023 року, найвищим рівнем довіри в українців серед державних і суспільних інститутів користуються Збройні сили. Втім російська пропаганда активно використовує інформаційні ресурси для поширення неправдивих повідомлень і спотворення фактів, зокрема і щодо ЗСУ та сил безпеки та оборони в цілому. Тому перед українськими фахівцями зі стратегічних комунікацій постало завдання оперативно

спростовувати дезінформацію та надавати якомога оперативніше, а почасти й на випередження, достовірну інформацію громадянам.

Підтримка військових операцій: Українські війська та їх дії під час контрнаступу вимагають підтримки і розуміння з боку населення, яке проживає як на вільній, так і на окупованій (та щойно деокупованій) територіях. Стратегічні комунікації повинні підкреслити важливість цих дій для національної безпеки та свободи.

Залучення громадян: Важливо включити громадян в процес прийняття рішень і підтримки сил безпеки та оборони. Це може відбуватися через роз'яснення стратегій та прозору інформаційну взаємодію.

Для ефективних стратегічних комунікацій в умовах війни необхідно дотримуватися наступних принципів:

Достовірність і об'єктивність: Інформація, що надається громадянам, повинна бути перевіреною та об'єктивною та враховувати правила висвітлення інформації відповідно до Наказу Головнокомандувача ЗС України №73, де наведено перелік інформації, розголошення якої може призвести до обізнаності противника про дії Збройних Сил України, інших складових сил оборони, негативно вплинути на хід виконання завдання за призначення під час дії правового режиму воєнного стану.

Співпраця із медіа: медіа відіграють важливу роль у поширенні інформації. Співпраця з ними може підвищити якість інформаційних повідомлень за умови дотримання ними нового Закону України "Про медіа", зокрема пункту IX, у якому зазначено особливості правового регулювання діяльності медіа в умовах збройної агресії.

Емоційний зв'язок: Спілкування повинно бути емоційно зв'язаним з аудиторією. Спільні цінності, історія та ідентифікація громадян з оборонними силами можуть підвищити підтримку.

Прозорість і відкритість: Громадяни повинні мати можливість отримати доступ до інформації про військові операції та прийняття важливих рішень.

Українські військові та інші зацікавлені сторони вже досягли певних успіхів у сфері стратегічних комунікацій під час збройної агресії з боку російської федерації. Наведемо кілька прикладів успішних кейсів.

Проект "Кіборги". Під час облоги аеропорту Донецьк волонтери та активісти створили проект "Кіборги". Вони розповідали історії та надавали інформацію про героїчну оборону аеропорту та захисників, яких часто називали "кіборгами". Цей проект не лише підвищив моральний дух військових, але й став символом сили та відданості українського народу.

Громадські обговорення на форумах і соціальних мережах. Громадські форуми та соціальні мережі стали платформами, де військові та громадяни можуть обговорювати актуальні питання, розповідати свої історії та ділитися досвідом. Це сприяє підтримці і підвищує рівень обізнаності.

Створення інформаційних ресурсів та медіа-проєктів. Українські військові та волонтери активно створюють та підтримують інформаційні ресурси та медіа-проєкти, які пояснюють стратегію та потреби армії. Наприклад, “Миротворець” збирає інформацію про воєнні злочини, а “InformNapalm” проводить дослідженні відкритих джерел, розкриває російську агресію та допомагає вивести інформацію на міжнародний рівень.

Публічні релації та медіа. Військові розробили власну стратегію публічних релацій та активно співпрацюють з медіа для надання об’єктивної інформації про події на фронті. Один із прикладів - регулярні брифінги для медіа та громадськості, які щоденно відбуваються в Military Media Center, що працює у Міністерстві оборони України, Media Center Ukraine 9 – громадська ініціатива, та інші.

Підтримка відомих осіб та мистецьких ініціатив. Велика кількість українських відомих осіб, таких як спортсмени, музиканти та актори, публічно виражають підтримку військових і ветеранів. Також було створено численні мистецькі ініціативи, які підтримують військових через мистецтво та культуру.

Ці приклади свідчать про важливість інформаційної складової в конфліктах і відображають різноманітні підходи, які використовувалися українськими військовими та громадянами для підвищення обізнаності та підтримки сил безпеки та оборони України. Завдяки цим зусиллям, вдалося створити позитивне сприйняття сил безпеки та оборони серед значної частини населення. Громадяни більше розуміють необхідність захисту країни та підтримують військових.

Ми переконані, що не варто забувати про важливий аспект використання стратегічних комунікацій для формування довіри до українських сил безпеки та оборони й на міжнародному рівні. Це допомагає підтримувати партнерства з іншими країнами, спонукати міжнародну спільноту виступати на стороні України та демонструвати її бажання співпрацювати у боротьбі з агресором.

Наведемо кілька ключових підходів до використання стратегічних комунікацій на міжнародному рівні.

Формування інформаційних повідомлень для міжнародної аудиторії:

Створення чітких і добре підготовлених інформаційних повідомлень, які пояснюють ситуацію в Україні, агресію Росії та дії українських сил, є важливим завданням. Ці повідомлення доступні на різних мовах і розповсюджуються через різні міжнародні канали зв’язку.

Лобіювання та дипломатична діяльність:

Важливим компонентом стратегічних комунікацій є лобіювання та дипломатична діяльність. Українська дипломатія може співпрацювати з міжнародними партнерами для підтримки позиції України та висвітлення агресії Росії на міжнародному рівні.

Залучення громадських організацій та активістів:

Громадські організації, активісти та лідери громадської думки можуть бути потужними агентами стратегічних комунікацій. Співпраця з ними може допомогти впливати на міжнародну аудиторію та мобілізувати підтримку.

Медіа та інформаційні кампанії:

Розробка та запуск інформаційних кампаній у світових медіа може допомогти витіснити російську пропаганду та поширювати достовірну інформацію про ситуацію в Україні.

Залучення міжнародних спостерігачів:

Регулювання через акредитування і запрошення міжнародних спостерігачів і журналістів на територію України сприяє об'єктивному висвітленню подій та забезпечує прозорість. Це також сприяє формуванню довіри до дій українських сил безпеки.

Доступ інтернаціональним слідчим органам до доказів злочинів російської агресії:

Забезпечення доступу міжнародним слідчим органам до доказів військових злочинів і порушень прав людини може підсилити підтримку міжнародного співтовариства та сприяти притягненню винних до відповідальності.

Таким чином, усі ці підходи допомагають створити позитивне сприйняття та довіру до українських сил безпеки та оборони на міжнародному рівні. Тобто стратегічні комунікації грають ключову роль у формуванні міжнародної підтримки та мобілізації зусиль у боротьбі з агресією та збереженні миру в Україні.

Список використаних джерел:

1. Ministry of defence. Allied Joint Doctrine for Strategic Communications (AJP-10), Edition A, version 1, 13 March 2023 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1175697/AJP_10_with_UK_elements_web.pdf.

2. Результати соціологічного опитування, що проводилося соціологічною службою Центру Разумкова "Оцінка громадянами ситуації в країні, довіра до соціальних інститутів, політиків, посадовців та громадських діячів, ставлення до окремих ініціатив органів влади" (липень 2023р.) https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/otsinka-gromadianamy-sytuatsii-v-kraini-dovira-do-sotsialnykh-instytutiv-politykiv-posadovtsiv-ta-gromadskykh-diiachiv-stavlennia-do-okremykh-initsiatyv-organiv-vlady-lypen-2023r.

3. Наказ Головнокомандувача Збройних Сил України від 03.03.2022 №73 "Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану" https://ips.ligazakon.net/document/MUS36785

4. Закон України “Про медіа” №2849-IX. від 13.12.2022 року. https://zakon.rada.gov.ua/laws/show/2849-20#Text.

5. Указ Президента України №555/2015 Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України" https://www.president.gov.ua/documents/5552015-19443.

Андрій ЗАХАРЖЕВСЬКИЙ, к.т.н., доц.
Любов БЕРКМАН, д.т.н., проф.
ДУІКТ
ORCID: 0000-0002-6772-1596
E-mail: berkmanlubov@gmail.com

МОДЕЛЬ ПОБУДОВИ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ

Захист конфіденційності інформації є важливою складовою інформаційно-комунікаційних мереж (ІКМ) зв’язку. Це забезпечується за допомогою різних технічних засобів, таких як шифрування, контроль доступу, автентифікація тощо. Забезпечення конфіденційності інформації за рахунок мережевих ресурсів інфокомунікаційних мереж зв'язку є критично важливим завданням з багатьма аспектами і важливими наслідками.

Першим кроком організації забезпечення конфіденційності інформації є розроблення політики безпеки в ІКМ, як набір документованих правил, процедур, стандартів і рекомендацій, які розробляються і впроваджуються в організації з метою забезпечення захисту інформації та інфраструктури мережі від різних загроз і загроз для безпеки [1]. Політика безпеки (ПБ) в ІКМ визначає рамки та стратегії, які допомагають забезпечити конфіденційність, цілісність та доступність інформації.

Одним із підходів побудови ПБ ІКМ є її формалізація та застосування моделі Белла-ЛаПадула для порушника [2,3].

Рис. 1. Схема моделі Белла–ЛаПадула

У запропонованому підході ПБ ґрунтується на побудові та обробці двох матриць: сеансової та транспортної (поштової). Сеансова матриця призначена для управління доступом користувачів до документів (файлів). Вона визначає тип доступу користувача до документів. Поштова матриця регламентує можливість пересилання файлів (об'єктів) між користувачами різного рівня безпеки електронною поштою.

При використанні матричної моделі доступу, умови доступу кожного суб'єкта S до кожного об'єкта O та суб'єкта S_1 до іншого суб'єкта S_2 визначаються вмістом матриць доступу: сеансової матриці M та транспортної матриці MT.

Кожен елемент M_{ij} сеансової матриці доступу M визначає права доступу i-го суб'єкта до j-му об'єкту (читати, редагувати, немає доступу). Приклад матриці доступу зображено в вигляді таблиці 1.

Таблиця 1

Матриця доступу

	O_1	O_2	...	O_n
S_1	*r*	-	...	*rw*
S_2	*rw*	*rw*	...	-
...	...	...	...	...
S_m	*r*	*rw*	...	*r*

Елементи у сеансовій матриці доступу мають такі значення: *r* – читання, *rw* – редагування, "-" – немає доступу. Кожен елемент MT_{ij} транспортної матриці доступу MT визначає права доступу i-го суб'єкта до j-му суб'єкту. Приклад транспортної матриці доступу наведено у таблиці 2.

Таблиця 2

Транспортна матриця

	S_1	S_2	...	S_m
S_1	1	0	...	1
S_2	0	1	...	0
...	...	...	...	...
S_m	1	0		1

Елементи у транспортній матриці доступу мають такі значення: 1 – *i*-й суб'єкт може надсилати дані *j*-му суб'єкту, 0 – *i*-й суб'єкт не може надсилати дані *j*-му суб'єкту.

У процесі функціонування системи множини суб'єктів та об'єктів можуть динамічно змінюватися. Такі зміни можуть відбуватися внаслідок появи нових суб'єктів та об'єктів, знищення суб'єктів та об'єктів, а також зміни прав доступу суб'єктів до об'єктів. Відповідно [4], у процесі функціонування системи повинні змінюватись і матриці доступу.

Використання двох матриць (сеансової та транспортної) дозволяє, по-перше, перевіряти кожну з них на несуперечність (правильність завдання політики безпеки), а по-друге, ввести в модель поняття порушника.

У кожному з цих варіантів за допомогою сеансової та транспортної матриць можна визначити список об'єктів, до яких він отримує доступ. Очевидно, що цей список залежить від повноважень S_i користувача.

Основною перевагою даного підходу є математична формалізація аналізу дотримання чинної політики безпеки, що дозволяє передати контроль за станом системи керуючій програмі.

Розглянута модель значно підвищує рівень захищеності операційних систем, СУБД та додатків, а також дозволяє контролювати витікання конфіденційної інформації в ІКМ та буде відповідати вимогам Міжнародної організації зі стандартизації [1].

Список використаних джерел:

1. ISO/IEC 27002:2013, Information technology – Security Techniques – Code of practice for information security controls. URL: https://cdn.standards.iteh.ai/samples/54533/63552c0d2b4244a7b3e583a9a30d37d6/ISO-IEC-27002-2013.pdf.

2. Жора В. В. Підхід до моделювання рольової політики безпеки / В. В. Жора // Правове нормативне та метрологічне забезпечення систем захисту інформації в Україні : інтернет журн. – 2003. – № 7. – С. 45 – 49.

3. Jason Andress. The Basics of Information Security (Second Edition) // Syngress - 2014, Pages 39-56, https://doi.org/10.1016/B978-0-12-800744-0.00003-8.

4. Elisa Bertino, Sajal K. Das, Krishna Kant, Nan Zhang. Access Control, and Formal Methods. // Handbook on Securing Cyber-Physical Critical Infrastructure. Morgan Kaufmann – 2012, Pages 573-594, https://doi.org/10.1016/B978-0-12-415815-3.00023-6.

Наталя ІВАНОВА, д.психол.н., проф.
ORCID: 0000-0002-6108-4725
E-mail: ivanova2112@ukr.net
Ольга ПАЛИВОДА, к.психол.н.
НАСБУ
ORCID: 0000-0003-2027-3316
E-mail: olsorvanec@gmail.com

ВНУТРІШНІ КОМУНІКАЦІЇ У БЕЗПЕКОВИХ ІНСТИТУЦІЯХ В УМОВАХ ВІЙНИ: ФОКУСУВАННЯ НА ОСОБИСТІСТЬ

У складних умовах повномасштабної збройної агресії рф проти України пріоритетності набувають питання успішної діяльності фахівців сектору безпеки і оборони, від роботи яких залежить, насамперед, і забезпечення національної безпеки, і наближення нашої перемоги. В організації роботи безпекових інституцій з-поміж інших пріоритетів слід акцентувати увагу й на налагодженні взаємодії та діалогу з колективами фахівців, оскільки саме внутрішні комунікації – це ключовий елемент функціонування будь-якого органу чи підрозділу.

У межах зазначеного до основних завдань внутрішніх комунікацій слід віднести такі: упроваджувати інноваційні управлінсько-організаційні технології (зокрема, зорієнтовані на формування готовності до дій в екстремальних умовах); наслідувати пріоритетні цінності; підвищити рівень довіри до керівників, корпоративної культури; запроваджувати корпоративні стандарти і традиції (взаємодопомога, взаємодовіра); оптимізувати інформаційні потоки та налагодити зворотній зв'язок; формувати інститут ефективного лідерства; розвивати систему мотивування та реалізовувати іміджеві технології успішного фахівця-патріота.

Тож цілями внутрішніх комунікацій в умовах війни є:

- взаємодопомога та взаємна довіра;
- формування відчуття захищеності (соціальної, фізичної);
- забезпечення успішної діяльності та взаємодопомоги;
- підтримання належного іміджу інституції та довіри до неї;
- високий рівень розвитку професійної мотивації та цінностей фахівців;
- підтримання корпоративної культури та відчуття приналежності до певної професійно-патріотичної спільноти;
- задоволеність роботою в певній інституції.

Указані цілі будуть успішно реалізовані за умови їх упровадження до циклу внутрішніх комунікацій, що має враховувати екстремальність воєнного стану та поєднує такі складові, як: *інформування* (донесення необхідної інформації), *залучення до діалогу* (обговорення отриманої інформації та визначення шляхів і варіантів її реалізації) та *зворотній зв'язок* (дані про стан та наслідки реалізації певної інформації в межах вирішення конкретної проблеми, визначення переваг /

недоліків та наступних інформаційних блоків, які мають бути впроваджені в роботу / комунікативний процес).

Указаний цикл буде ефективним, якщо фахівці враховуватимуть пріоритетні аспекти внутрішніх комунікацій, а саме: мету, завдання, функції, цінності фахівця/інституції, особливості корпоративної культури та системи мотивування, канали зв'язку, імідж інституції та шляхи оптимізації її діяльності.

Також у межах розбудови внутрішніх комунікацій визначаються та усвідомлюються співробітниками такі організаційні феномени, як: місія (навіщо ми працюємо), візія (якими ми маємо бути), цінності (як ми маємо поводитись) та стратегія (що, як і коли ми маємо робити).

Разом з цим, слід враховувати і певні фактори, що можуть спричинити проблеми у внутрішніх комунікаціях, а саме:

1. недосконале формулювання обов'язків (особливо під час впливу стрес-факторів війни та часових меж терміновості ухвалення об'єктивних рішень, адекватних дій);
2. нераціональне розподілення завдань (не здійснюється розподіл залежно від потенційних можливостей фахівців, рівня їх підготовленості та особистісних характеристик);
3. імітація професійної взаємодії (створюється враження про взаємодію, але відсутні її конкретні результати);
4. невідлагоджений процес прийняття рішень (наприклад, відбуваються певні порушення в алгоритмі збору та об'єктивного аналізу інформації, її реалізації);
5. деструктивна конкуренція (не заради важливого результату, а задля самоствердження чи задоволення власних амбіцій);
6. неефективне управління (нечіткість постановки мети та завдань щодо конкретних дій, неефективний розподіл завдань між підлеглими, відсутність у керівника авторитету серед підлеглих та здатності їх консультувати щодо виконання певних завдань тощо).

Зокрема, щоб уникнути негативного впливу зазначених факторів, доцільно налагодити у процесі внутрішніх комунікацій дієвий зворотній зв'язок, який має бути зорієнтований на: діалог, конструктивну співпрацю за будь-яких обставин, підвищення рівня професійної мотивації фахівців, злагодженість дій, розвиток корпоративної культури.

Основними принципами дієвості такого зворотного зв'язку мають бути: конструктивність, своєчасність, гнучкість, конкретність, відкритість, взаємоповага, об'єктивність. Але слід ураховувати й найпоширеніші помилки фідбеку, зокрема такі: неконструктивна критика, перехід на особистості, відсутність конкретики, недотримання домовленостей.

До того ж, важливо визначити вектори вдосконалення корпоративної культури, насамперед: зосереджуватись на основних цінностях фахівців (родина, життя, безпека, взаємодопомога тощо); заохочувати командну роботу (разом до перемоги)

та культуру спілкування (взаємоповага, взаєморозуміння), мотивувати фахівців, пропагувати дотримання доброчесності та морально-етичних норм, дбати про імідж та лояльність, запобігати проявам деструктивної взаємодії та девіантної поведінки.

Таким чином, із вищевикладеного випливає, що оптимізації внутрішніх комунікацій в умовах війни сприятиме низка дієвих психологічних технологій, зокрема таких:

“маркери внутрішніх комунікацій” – виявлення та фіксація маркерів внутрішніх комунікацій; слід ураховувати, що зовнішніми проявами внутрішніх комунікацій є такі: комунікативна культура, толерантність, безконфліктна поведінка, відсутність агресивних реакцій та дій, щирість, порядність, кореляція слова з ділом, вчасне доведення інформації;

“передумови ефективності внутрішніх комунікацій” – виокремлення низки передумов внутрішніх комунікацій; керівники мають розглядати комунікацію як важливу частину своїх посадових обов’язків; дії та поведінка всіх співробітників повинні узгоджуватися з місією та візією, цінностями та ключовими меседжами інституції; прозора комунікація повинна бути частиною корпоративної культури;

“розвиток внутрішніх комунікацій” – насичувати комунікацію та події цінностями; зорієнтовувати комунікацію на активний фідбек; розробити та впровадити стандарти комунікації; установлювати правила ефективної комунікації та дотримуватись їх; голос має “звучати” однаково як для зовнішньої аудиторії, так і для співробітників інституції; підвищувати рівень мотивації фахівців та їх лояльності; навчати співробітників і керівників навчатись разом; розвивати та підтримувати корпоративну культуру; удосконалювати арсенал каналів внутрішніх комунікацій.

Розглянуті психологічні аспекти внутрішніх комунікацій у безпекових інституціях в умовах війни сприятимуть формуванню їх оптимізаційної системи.

Дар'я КАШПЕРСЬКА, д.ф.
ORCID: 0000-0001-8554-9235
E-mail: dkashperska@gmail.com
Олексій ПИСЬМЕННИЙ, к.політ.н., ст.дос.
ВА ім. Євгенія Березняка
ORCID: 0000-0002-0814-0492
E-mail: armor.ua75@gmail.com

КОМУНІКАТИВНІ ТАКТИКИ І СТРАТЕГІЇ ВОЄННОГО ОРАТОРА В ЦИФРОВУ ЕПОХУ

Широкомасштабна агресія РФ стала каталізатором суттєвих трансформацій комунікативних тактик та стратегій *Офісу Президента України* та самого глави

держави. Так, суто ритуальні колись звернення Президента до українського народу перетворилися на щоденну онлайн комунікацію у час гострої екзистенційної загрози, яка могла призвести до глобального зламу геополітичного характеру. Саме такий злам і був би переможним результатом консцієнтальної війни ворога. Одначе феномен консцієнтальності був взятий до уваги, особливо в стратегічних комунікаціях Володимира Зеленського. Стилістика та зміст його наративів, візуальна складова створеного образу Президента під час війни, способи та засоби донесення головних меседжив до внутрішньої та зовнішньої цільової аудиторії (ЦА) – це приклад успішної реалізації консцієнтальних СК.

Серед головних специфічних якісних характеристик промов Зеленського М. Кармазіна виокремлює такі [1]: фіксацію появи нової лінії розлому між Росією та цивілізованим світом; викриття в Європі "розуміючих Путіна". Президент України намагався донести до представників вільного світу важливість посилення санкцій проти Росії, збільшення оборонної та фінансової підтримки України; стимулювання утворення антипутінської коаліції; унаочнення присутності в європейському просторі самодостатньої української нації, здатної до самоорганізації та безпрецедентного опору ворогу тощо.

У вибудовуванні СК Президента було взято до уваги бренд-стратегію "Tone of Voice" (тон голосу) – це стиль комунікацій, звучання бренду, який простежується у всіх точках взаємодії з користувачем і пояснюється таким твердженням: "Tone of voice is not what you say, it's how you say it" ("Тон голосу – це не те, що ти сказав, а те, як ти це сказав"). Voice – голос, індивідуальність, яка відрізняє компанію від інших. Tone – тональність, яка залежить від контексту. У комунікації Володимира Зеленського як з українською, так і закордонною аудиторією важливу роль відіграє чинник ідентифікації та самоідентифікації. Його наратив ґрунтується на чіткій опозиції українського народу до ворога, на емпатії до кожного з українців та союзників; він не розділяє у своїх промовах власне "я" від "я" суспільного, більше того ця тотожність ґрунтується на мовленнєвій сугестії, яка формує розуміння, що Володимир Зеленський – це не суто керівник держави, а один з таких же громадян, що чинить спротив окупанту. Сучасні технології дали можливість створити максимально переконливу ілюзію зближення Президента з народом завдяки зверненням-селфі, записаним на телефон, переважно на фоні звичайного офісного кабінету, а не офіційного кабінету Президента. Так, 25 лютого 2022 року Володимир Зеленський зробив відео у стилі селфі, яке протягом години було переглянуто 3 мільйони разів – це частина комунікативних зусиль задля мобілізації міжнародної громадськості проти російського вторгнення в Україну.

Експерт з цифрових соціальних мереж, професор інформаційних систем Університету штату Мічиган Анджана Сусарла зауважила, що Володимир Зеленський переміг Росію у PR-війні, його відео, зроблені за допомогою iPhone і опубліковані у соціальних мережах, таких як Facebook, Telegram і Twitter,

переконливо згуртували світову громадську думку за Україну та проти Росії [2]. Можна виокремити чотири основні причини, чому відео Зеленського миттєво зробили війну в Україні глибоко особистою та резонансною для багатьох та стали лід-магнітом.

1) *Беззаперечна достовірність повідомлення*. Насамперед йдеться про запис від 25 лютого 2022 року, знятого в Києві без телесуфлерів чи офіційної атрибутики. У якийсь момент прем'єр-міністр України Денис Шмигаль, стоячи за спиною Зеленського, показав позначку часу на своєму телефоні, щоб підкреслити момент її зйомки. Передача очевидної автентичності – це одна з тактик, яку використали Барак Обама та Дональд Трамп, щоб стати президентами та надихнути своїх послідовників. Зеленський, який зараз має 13,5 мільйонів підписників в Instagram, зміг використати цю тактику, щоб заохотити більшість світу підтримувати Україну.

2) *Взаємодія з аудиторією*. Соціальні медіа підсилюють видимість повідомлення, коли користувачі відчувають особистий зв'язок із вмістом, перетворюючи їх, по суті, на людей, які формують думку, коли вони діляться ним із однодумцями. Послання Зеленського, яке наголошує на єдності свого народу та почутті солідарності, створило зв'язок із багатьма людьми, які переглядали його відео. Спираючись на переконливі й прямі повідомлення, дописи спрямовувалися широкій міжнародній аудиторії в соціальних мережах та гуманізували конфлікт.

3) *Максимальна простота контенту*. Підхід Зеленського до формування ключових наративів спрямований на надання простим громадянам контенту, який вони можуть легко використовувати в соціальних мережах для тиску на своїх політичних представників. Тобто це інструмент, який використовується переважно для оптимізації копірайтингу для створення текстів, які легко продати.

4) *Негайність повідомлення*. Дослідження показують, що повідомлення, які здаються терміновими, швидше викликають емоційну реакцію, що збільшує кількість людей, які публікують і діляться дописом. Цей каскад розмов спричиняє утворення трендів у мережі, що, переважно, стимулює більше дискусій між користувачами та робить повідомлення більш віральними. Звернення Зеленського про допомогу від імені свого народу у час, коли по всій його країні падали ракети та бомби, було максимально терміновим. Це перетворило мільйони користувачів на добровільних рекрутів для його справи – посилення міжнародного тиску, щоб допомогти Україні відбити російське вторгнення. Саме так цифрові активісти, які збирають гроші на допомогу жертвам стихійних лих, прагнуть залучити користувачів соціальних мереж до швидкої допомоги постраждалим. Лише за кілька днів хештег #standwithukraine став вірусним, і фінансова допомога почала надходити. Термінові повідомлення, опубліковані Зеленським, зіграли важливу роль у створенні армії онлайн-користувачів, які транслювали свою відданість, поділяючи подробиці збору коштів або благодійних організацій на підтримку українського народу.

Так, завдяки соціальним платформам та PR-концепції “Tone of Voice” стратегічні комунікації Президента особливо в перші місяці війни допомогли формувати те, як адресатам необхідно розуміти світ та його структурувати, як вони реагують на новини у час максимальної хаотизації дійсності. Водночас такі СК створили новий тип політичного лідера – військового оратора у цифрову епоху завдяки його прямим включенням під час засідань головних міжнародних політичних організацій, на знакових самітах та великих культурних заходах. Саме тому жива комунікація Володимира Зеленського з міжнародною спільнотою також заслуговує ґрунтовного наукового аналізу.

Список використаних джерел:

1 Кармазіна М.С. Переосмислити сьогодення: Президент України Володимир Зеленський про новітні “розломи” в Україні та світі (24 лютого – 28 червня 2022 р.). Вісник воєнної розвідки. № 69. 2022.ст. 3–9. Інв.9143.

2. Анджана Сусарла. Why Zelenskyy’s ‘selfie videos’ are helping Ukraine win the PR war against Russia. URL: https://theconversation.com/why-zelenskyys-selfie-videos-are-helping-ukraine-win-the-pr-war-against-russia-178117 (дата звернення: 15.09.2023).

Олександр КОВАЛЕНКО, ад’юнкт
НУОУ
ORCID:0000-0001-8612-3674
E-mail: kovalenko79@gmail.com

ПСИХОЛОГІЧНІ ЧИННИКИ ОРГАНІЗАЦІЇ ВНУТРІШНІХ КОМУНІКАЦІЙ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ В СИСТЕМІ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ

Комунікація визнається важливим фактором для функціонування суспільства, а його існування без неї неможливе. Зростання ролі сучасних інформаційних технологій, засобів масової інформації та соціальних мереж значно ускладнило структуру комунікацій в сучасному суспільстві. З точки зору масштабу, можна виділити дві головні категорії: стратегічні комунікації, які використовуються для залучення широкої громадськості та переходять на міждержавний рівень через засоби масової інформації, і внутрішні комунікації, які функціонують в конкретних групах, колективах, підприємствах або військових підрозділах, частинах.

Ще в 2015 році за досвідом Антитерористичної операції для покращення стану справ у внутрішніх комунікаціях військових частин Збройних Сил України наказом Генерального штабу Збройних Сил України від 03.12.2015 №472 "Про організацію діяльності високомобільних груп внутрішніх комунікацій у військових частинах (підрозділах) Збройних Сил України" була затверджена Програма налагодження внутрішніх комунікацій Збройних Сил України [1]. Створені високомобільні групи внутрішніх комунікацій з числа військовослужбовців і працівників Збройних Сил України, які пройшли навчання і тренінги. Група, на яку було покладене завдання надавати допомогу службовим особам щодо підтримання та відновлення необхідного для виконання завдань бойового духу (морально-психологічного стану), здійснювати інформаційно-психологічну підтримку, отримала найменування "Альфа". Високомобільна група внутрішніх комунікацій "Альфа" складалась з інспектора, ідеолога, військового капелана і військового психолога.

В подальшому в ході розвитку системи стратегічних комунікацій, які стають важливим завданням для забезпечення ефективності та дієвості військових операцій, було виділено внутрішні комунікації, як одну зі складових стратегічних комунікацій Збройних Сил України.

Наказом Міністерства оборони України від 22.11.2017 № 612 затверджена Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України. Згідно нього внутрішня комунікація реалізується Головним управлінням морально-психологічного забезпечення Генерального штабу Збройних Сил України та "діяльність щодо підготовки та здійснення стратегічних комунікацій, проведення інших інформаційних заходів є складовою діяльності командувачів (командирів), керівників органів військового управління всіх рівнів. В організації дій в інформаційному просторі в мирний час та в особливий період, під час підготовки та проведення операцій (бойових дій) беруть безпосередню участь командувачі (командири) та штаби всіх рівнів. Кожен з органів військового управління в залежності від своїх повноважень розробляє та планує заходи і дії підпорядкованих військ (сил), які об'єднані єдиним замислом дій в інформаційному просторі"[2].

Безпосередніми виконавцями внутрішньо-комунікаційної роботи у військових частинах є командири, штаби, заступники командирів з морально-психологічного забезпечення всіх рівнів.

Відповідно до Настанови з морально-психологічного забезпечення підготовки та застосування Збройних Сил України, затвердженої наказом Генерального штабу Збройних Сил України 27.04.2018 №173, внутрішньо-комунікаційна робота є напрямком інформаційно-пропагандистського забезпечення. Згідно Настанови "внутрішньо-комунікаційна робота реалізується шляхом: налагодження комунікаційного процесу, системного та цільового проведення пропагандистської (контрпропагандистської),

ідеологічної, інформаційно-роз'яснювальної, національно-історичної, військово-соціальної роботи з особовим складом; координації душпастирської опіки військовослужбовців; поширення здорового способу життя; участь у заходах щодо захисту від негативного інформаційно-психологічного впливу противника; систематичного аналізу проведених дій; забезпечення командирів військових частин (підрозділів) та їх заступників з морально-психологічного забезпечення прикладними методичними матеріалами, необхідними для інформаційної роботи з особовим складом в умовах підготовки і ведення операцій (бойових дій); забезпечення військ (сил) матеріалами періодичного друку, тощо"[3].

Психологічні чинники грають важливу роль у внутрішніх комунікаціях і включають в себе наступні аспекти:

Мотивація військових: Психологічний стан військових може значно впливати на їх мотивацію та військову діяльність. Внутрішні комунікації повинні сприяти створенню позитивного психологічного клімату, підтримувати духовний стан військовослужбовців та підвищувати їхню віру у місію ЗСУ.

Тренінг і психологічна підготовка: Забезпечення психологічної підготовки військових, включаючи управлінський і лідерський тренінг, може поліпшити якість внутрішніх комунікацій та збільшити довіру між різними рівнями командування.

Конфлікти і їх розв'язання: Ефективна система внутрішніх комунікацій також повинна включати в себе механізми врегулювання конфліктів. Психологічна підготовка може допомогти військовим вчитися вирішувати конфлікти конструктивно, що сприяє збереженню єдності військового колективу.

Психологічна підтримка в умовах стресу: Військовослужбовці можуть стикатися зі стресом під час бойових операцій та інших важливих завдань. Важливо мати систему психологічної підтримки, яка надає військовим можливість обговорювати свої емоції та досвід з фахівцями з психології.

Ефективність комунікації з командуванням: Внутрішні комунікації повинні бути чіткими і відкритими, щоб військовослужбовці зрозуміли мету та стратегію операцій. Це допомагає зберігати довіру між командуванням і військовослужбовцями.

Культура військової служби: Психологічні чинники можуть також впливати на культуру військової служби. Збройні Сили повинні створювати середовище, в якому військовослужбовці відчувають себе підтриманими та важливими для команди.

Зв'язок з родинами і громадськістю: Окрім внутрішніх комунікацій, важливо також підтримувати зв'язок військовослужбовців з їхніми родинами та громадськістю. Це може впливати на психологічний стан військових і їх мотивацію.

Загальна мета психологічних чинників у системі внутрішніх комунікацій в Збройних Силах України - підтримати дух військового колективу, збільшити їхню ефективність та віру у місію, а також забезпечити психологічну стійкість в умовах стресу та ведення бойових дій.

З початком широкомасштабної агресії російської федерації проти України у 2022 році постало питання покращення внутрішніх комунікацій у військових частинах Збройних Сил України. Ведення ворогом пропаганди та поширення неправдивої інформації через засоби масової інформації та соціальні мережі на початковому етапі мали значний вплив як на військовослужбовців так і на громадян України.

Існуюча на початок 2022 року система морально-психологічного забезпечення в цілому виконує покладені завдання, але має низку проблемних питань, які перешкоджають реалізації її основної мети - підтримання особового складу у психологічній готовності до успішного виконання завдань за призначенням.

Аналіз іноземного досвіду виявив, що у збройних силах держав - членів НАТО приділяється значна увага питанням морально-психологічного впливу на особовий склад, однак структури, подібної до структури морально-психологічного забезпечення Збройних Сил України, вони не мають. Також в арміях країн Альянсу не передбачені посади заступників командирів з морально-психологічного забезпечення та їм подібні, водночас:

формування необхідних психічних якостей у особового складу здійснюється, головним чином, у ході проведення занять з бойової підготовки, максимально наближених до бойових умов;

виконання окремих завдань, подібних до завдань морально-психологічного забезпечення, покладається на розрізнені структурні підрозділи: персонал, стратегічні комунікації, цивільно-військове співробітництво, соціальні відносини та інформації, військові капелани, медичні тощо.

Аналіз завдань, які виконуються структурою морально-психологічного забезпечення виявив, що деякі з них є спорідненими. Це вказує на можливість їх перерозподілу і приведення до стандартів НАТО за рахунок трансформації системи морально-психологічного забезпечення.

Одним з можливих шляхів покращення стану внутрішніх комунікацій у військових частинах Збройних Сил України є передавання функцій внутрішньокомунікаційної роботи та інформаційного супроводу особового складу - Управлінню стратегічних комунікацій Апарату Головнокомандувача ЗС України, а також Центральному управлінню цивільно- військового співробітництва ГШ ЗС України в частині, що стосується оцінювання цивільного середовища (суспільно-політичної обстановки).

Існуючу систему морально-психологічного забезпечення трансформувати у систему підтримки психологічної готовності ЗС України шляхом:

створення підрозділів соціально-психологічної підтримки у складі структур персоналу усіх рівнів і передавання функцій психологічної та соціальної підтримки підрозділам персоналу;

функцій національно-патріотичної роботи та культурологічної підтримки - Департаменту гуманітарного забезпечення МО України;

ліквідацію вертикалі заступників командирів (командувачів) з морально-психологічного забезпечення;

покладання завдань з організації (координації) діяльності за напрямом підтримки психологічної готовності ЗС України на заступників командирів усіх рівнів;

перегляд обов'язків заступників командирів з морально-психологічного забезпечення усіх рівнів та їх перерозподіл, у разі необхідності, між заступниками командирів (командувачів) та головними сержантами.

Важливість внутрішніх комунікацій в військовій частині для досягнення високої боєздатності неможливо недооцінити. Наприклад, кожен військовий у підрозділі може мати високу майстерність у власному фаху, такому як стрільба, операції зі спецтехнікою, кулінарія та інше, проте без командної співпраці і ефективної комунікації, військовий підрозділ залишається неефективним, і його боєздатність ставиться під сумнів.

Окремі взводи або роти можуть бути добре підготовленими і мати високу боєздатність, але відсутність налагодженої внутрішньої комунікації на рівні батальйону чи бригади може призвести до порушень взаємодії між підрозділами та зниження ефективності в бойових діях.

Історія війн та військових конфліктів часто підтверджує, що перемогу завжди здобували ті, хто краще координував і забезпечував командну співпрацю сотень і тисяч воїнів, навіть при чисельній перевазі супротивника.

Без ефективної внутрішньо-комунікаційної роботи з особовим складом у військовій частині неможливо досягнути високої боєздатності підрозділу. Кожен в підрозділі може бути відмінним стрільцем, оператором, водієм, кухаром і таке інше, але без бойової злагодженості, без командної роботи, без налагодженої внутрішньої комунікації військовий підрозділ буде неефективним і підрозділ не вважатиметься сповна боєздатним. Кожен взвод чи рота окремо можуть бути цілком боєздатними, але без дієвої внутрішньої комунікації в полку чи бригаді, порушень комунікації між взводами і ротами ефективність бойового застосування батальйону чи бригади різко падає.

.

Список використаних джерел

1. Наказ ГШ ЗС України від 03.12.2015 року №472 "Про організацію діяльності високомобільних груп внутрішніх комунікацій у військових частинах (підрозділах) Збройних Сил України". – К.: ГШ ЗС України, 2015 р.

2. Наказ Міністерства оборони України від 22.11.2017 № 612 “Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України”. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0612322-17#Text.

3. Наказ ГШ ЗС України від 27.04.2018 року №173 “Про затвердження Настанови з морально-психологічного забезпечення підготовки та застосування Збройних Сил України”. – К.: ГШ ЗС України, 2018 р.

Людмила КОЗЛОВСЬКА, к.політ.н., проф.
ІВМС НУ “Одеська морська академія”
ORCID: 0000-0003-2635-7916
E-mail: 7000494@gmail.com

ОДНА ІЗ ПЕРСПЕКТИВ ВНУТРІШНІХ (КРИЗОВИХ) КОМУНІКАЦІЙ НА ЕТАПІ МІГРАЦІЙНОЇ КРИЗИ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ 2022-2023 РОКІВ

Постановка проблеми. Війна росії проти України 2022-2023 рр.ставить перед нашою країною щоденні виклики.Питання міграції стояли перед Україною і до 2022 року. Сьогодні вони набули особливо гострої постановки, що визначило ***актуальність*** дослідження. Зв’язок між органами влади і громадянами країни в таких умовах передбачає посилення та удосконалення кризових комунікацій. Кризове комунікування політико-владних інститутів України з вимушеними мігрантами-біженцями в умовах війни 2022-2023 рр. стало ***об’єктом*** дослідження.

Предмет наукового пошуку – закономірності взаємодії українських мігрантів-біженців та органів влади України в кризових комунікаціях в умовах війни 2022-2023 років.

Мета дослідження – простежити взаємодію українських мігрантів-біженців з представниками державних структур України в кризових комунікаціях в умовах воєнного стану 2022-2023 років.

Завдання наукового пошуку:1) Виділити головну складову взаємодії мігрантів-біженців та органів державної влади України в кризових комунікаціях 2022-2023 років.2) Визначити один із шляхів кризового комунікування, який допоможе зупинити міграційну кризу в нашій країні та повернути мігрантів додому на Україну.

Аналіз досліджень та невирішені аспекти проблеми викладені в теоретичних положеннях щодо кризови комунікацій українських мігрантів-біженців з органами державної влади та управління України в умовах війни 2022-

2023 років в роботах Ковальської Л., Костенко В., Малиновської О. та ін., які склали ***джерелознавчу*** базу наукового пошуку.

***Виклад основного матеріалу*.** З початку повномасштабного вторгнення рф на Україну гостро постало питання вибудови внутрішніх (кризових) комунікацій органів державної влади та управління України щодо вимушеної міграції українців в умовах війни, відтоку трудового ресурсу, що є загрозою підриву національної єдності та безпеки нашої держави. Особливо це стосується втрат людського потенціалу, викликаних міграційною кризою в Україні в умовах воєнного стану 2022-2023 років. [1,с.175]

За даними Інституту демографії та соціальних досліджень імені М.В. Птахи з 24.02.2022 р. станом на травень 2023 року з нашої країни емігрувало 8,6 мільйонів громадян України. [2] Не втративши українського громадянства, вони отримали статус біженця(S), що дало можливість спрощеної інтеграції до країн перебування. Але з інтеграцією у суспільства держав Європи одночасно почався процес деінтеграції з України [3, с.59].

Перемогти ворога і відбудувати країну після війни ми зможемо тільки разом. Для цього необхідні рішучі кроки і кризові комунікації можуть допомогти їх здійснити. Національна безпека і оборона України має триматись на міцному фундаменті єдності українського народу. А вимушена міграція українських жінок-біженок молодого та середнього віку з дітьми в умовах війни з метою зберегти життя повинна зупинитися [5, с.94]. Цьому має сприяти не тільки закінчення війни, а й приближення ПЕРЕМОГИ над рашистським агресором спільними зусиллями. Соціологічні дослідження Українського центру економічних та політичних досліджень ім. О. Разумкова та Інституту демографії та соціальних досліджень імені М.В. Птахи на протязі 2022-2023 років у сфері утвердження української національної та громадянської ідентичності часто стосувалися питань українських мігрантів в умовах війни та перспектив повернення їх додому [2].

В цьому ж напрямку проводилися дослідження і в ІВМС НУ “ОМА” на кафедрі СГіФД (спеціальність 254, спеціалізація МПЗ). Були опитані курсанти 1-4 курсів ІВМС НУ “ОМА”, близькі та рідні яких мігрували за кордон як біженці в умовах війни. В результаті аналізу проведеного опитування підтвердились висновки попередніх дослідників: головним завданням уряду України мають стати кроки щодо мотивування українців повертатися додому. [8, с.67] Одним із кроків внутрішніх (кризових) комунікацій в цьому напрямку може стати посилення військово-промислового комплексу України шляхом створення заводів з виробництва боєприпасів до наданої для нашої перемоги ЄС та НАТО зброї на території України. Трудові ресурси таких заводів мають фінансуватися на рівні військовослужбовців – учасників бойових дій на лінії фронту. Така оплата праці буде значно вищою, ніж оплата праці різноробочих українців-мігрантів за кордоном, які погано знають мову приймаючої сторони. Це буде

один із стимулів повернутись на Україну. Тим більше – це приблизить Перемогу. Після розгрому ворога такі заводи можуть бути переструктуровані в машинобудівні виробництва для відбудови зруйнованої України.

Як **висновок** зазначимо,що головною складовою взаємодії мігрантів-біженців та органів державної влади України в кризових комунікаціях 2022-2023 років є подолання паніки та спрямованість на співпрацю, орієнтовану на повернення мігрантів-біженців додому на Україну. Одним із шляхів такого кризового комунікування може стати посилення військово-промислового комплексу України шляхом створення заводів з виробництва боєприпасів для нашої перемоги над ворогом на території України. Висока оплата праці на таких підприємствах може стати стимулом до повернення мігрантів-біженців на Україну, що допоможе зупинити міграційну кризу в нашій країні та восстановити найголовнішу стратегічну цінність для України – людські ресурси. Так як в дослідженні розглядалась одна із перспектив внутрішніх(кризових) комунікацій на етапі вимушеної міграції українців в умовах воєнного стану 2022-2023 років – посилення військово-промислового комплексу України – науковий пошук в цьому напрямку має бути продовженим.

Список використаних джерел:

1. Глобалізаційні процеси у світовій економіці: виклики та можливості для України : колективна монографія / за заг. ред. д.е.н., проф. О.О. Борзенко ; НАН України, ДУ “Ін-т екон. та прогнозув. НАН України”. – Електрон. дані. – К., 2022. – 264 с.
2. Ідентичність громадян України: тенденції змін / Соціологічне опитування в рамках проекту Програми MATRA при підтримці Посольства Королівства Нідерландів в Україні. К:Центр Разумкова , травень 2023.
3. Ковальська, Л., Гук, Р. (2018). Міграційні процеси в Україні в період агресії Російської федерації. (№1(29). с. 78-82). Warsaw : World science.
4. Костенко В. О. Міжнародні політико-правові інструменти міграційної політики як передумова політичної стабільності в демократичному суспільстві - Держава і право: Збірник наукових праць. Юридичні і політичні науки. Випуск 93 / Ін-т держави і права імені В. М. Корецького НАН України. Київ: Вид-во “Юридична думка”, 2023.- с.191-202
5. Малиновська, О. А. (2018). Міграційна політика: глобальний контекст та українські реалії. Київ : НІСД – 472 с.
6. Парламентські слухання на тему: ”Захист прав і свобод громадян України, які перебувають на території держав-членів ЄС та інших держав як тимчасово переміщені особи, внаслідок збройної агресії Російської Федерації”-
7. https://komspip.rada.gov.ua/documents/sluhannja/

8. Пирожков, С. І., Лібанова, Е. М., Новікова, О.Ф. (2018). Українське суспільство: міграційний вимір. Київ : Інститут демографії та соціальних досліджень ім. М. В. Птухи НАН України – 396 с.

9. Українське суспільство в умовах війни. 2022: Колективна монографія / С. Дембіцький, О. Злобіна, Н. Костенко та ін.; за ред. член.-кор. НАН України, д. філос. н. Є. Головахи, д. соц. н. С. Макеєва. Київ: Інститут соціології НАН України, 2022. 410 с.

Валентина КУПЧИШИНА, к.п.н., доц.
НАДПСУ ім. Богдана Хмельницького
ORCID: 0000-0003-0937-8029
E-mail: valentino68_68@ukr.net

ВПЛИВ ВНУТРІШНІХ (КРИЗОВИХ) КОМУНІКАЦІЙ В ОРГАНІЗАЦІЇ НА ЕМОЦІЙНИЙ СТАН ЇЇ ПРАЦІВНИКІВ

Питання комунікації були актуальні в різні часи. Вчені констатували, що поняття “комунікація”, – це не просто обмін думками/словами, – це процес, який забезпечує спадкоємність та єдність усієї життєдіяльності людини. Науковцями визначено, що комунікація виступає складовою фундаментальних основ, без яких не може існувати людина і суспільство. Ними було запропоновано декілька класифікацій комунікації за різними ознаками. Так, за однією з ознак, в межах організації вона може бути внутрішньою й зовнішньою. Метою нашого розгляду є саме характеристика та зміст внутрішніх комунікацій, які характеризують всю її діяльність.

Проблемні питання щодо змісту, організації та характеристики комунікацій розкривали у своїх наукових працях М.Бондарева, І.Зарецька, Л.Карамушка, А.Лизанець, М.Мартиненко, Є.Тихомирова, О.Феєр, Р.Черновол-Ткаченко та ін.

Так, наприклад, Р.Черновол-Ткаченко [6, с. 212-220] у своєму дослідженні визначила місце та значення внутрішніх комунікацій в діяльності організації. Автор дослідження не тільки описує особливості класифікування, але й подає аналіз й характеристику специфічних різновидів неформальних комунікацій (чутки, плітки тощо) та визначає зміст психологічного феномену “трансакція”.

Група науковців (М.Бондаренко, А.Лизанець та О.Феєр) розкривають особливості внутрішніх комунікацій в системі управління персоналом організації через їх класифікацію, значення. Ми погоджуємось з їх думкою, що між налагодженим комунікаційним процесом та якістю роботи кожної структурної ланки організації є пряма залежність. Вчені зазначають, що сам процес внутрішньої комунікації в організації сприяє виконанню трьох основних завдань – це інформування, залученість, отримання зворотнього зв’язку [3, с. 127-132].

У науковій літературі зазначено, що до внутрішних комунікації відносять будь-які комунікації всередині організації. Вони можуть бути усними й письмовими, безпосередніми й віртуальними, особистими й груповими, формальними й неформальними, горизонтальними й вертикальними. Однією з цілей будь-якої організації є ефективні внутрішні комунікації, мета яких встановлення ефективних і лояльних відносин між працівниками та керівництвом; створення комфортної робочої атмосфери для досягнення мети організації. Дослідниками відмічено, що для їх ефективності слід налагодити співпрацю у всіх напрямках, але це можливо лише за наявності зворотнього зв'язку та сприятливого морально-психологічного клімату [1].

Враховуючи умови в яких перебуває все українське суспільство, збільшилась кількість наукових досліджень, предметом яких є кризові комунікації. Це питання також неодноразово було обрано предметом дослідження. Так, І.Козубенко зауважує, що "криза (з лат. "скрута", "небезпека") – такий збіг обставин, за яких наявні засоби досягнення цілей стають неадекватними, у результаті чого виникають непередбачувані ситуації та проблеми [2, с. 175-179]. О.Скоруком [5] подано визначення феномену "криза" з погляду кризового управління: "криза – це і припинення нормального процесу, і непередбачена подія, що ставить під загрозу стабільність підприємства, і раптова серйозна подія, що має потенціал, здатний зашкодити репутації кампанії або навіть зруйнувати її". Л.Мудрак констатує, що основною вимогою кризової комунікації є вимога щодо повідомлення тільки підтвердженої й перевіреної інформації та роз'яснення щодо неможливості отримання повної інформації на цей момент [4].

Вивчення змісту наукової літератури засвідчило, що вчені спільні в поглядах, що найважливішими факторами ефективної кризової комунікації виступають такі її характеристики як: відкритість, доступність, чесність і правдивість. В той же час існує ціла низка проблемних моментів – це недостовірна і неуточнена інформація, брак інформації або недостатня її кількість, надання неправильної картини подій чи ситуації тощо. Наслідком цього є негативні емоційні стани членів організації, які спричинюють різні емоційні прояви. Не вчасно надана психологічна допомога може спричинити виникнення різноманітних захворювань членів колективу (психози, істерики, панічні атаки, мігрені, апатія тощо) та стати причиною виникнення конфліктних ситуацій, що в цілому вплине на діяльність усіх членів організації та на якість виконаних робіт.

На думку І.Козубенко, дієвим способом протистояти різноманітним стрес-факторам є розробка стратегій внутрішніх (кризових) комунікацій. Детальний аналіз психологічного стану людей, які є учасниками внутрішніх (кризових) комунікацій, дав змогу дослідниці виокремити та описати зазначені вище

стратегії та показати їх наслідки, значення для вирішення складних ситуацій [2, с. 175-179].

В результаті аналізу змісту наукових праць зарубіжних дослідників, О.Скорук у своєму дослідженні розкриває не тільки зміст "золотого правила" концепції кризової комунікації (яке було сформульовано французькими фахівцями), але й посилається на типові помилки при зіткненні з кризою (які було визначено американськими вченими). Автор дослідження підсумовує, що при впровадженні цілої низки рекомендацій щодо подолання кризових ситуацій слід враховувати особливості управління, побудови, тип кризи і ситуацію, яка існує ззовні. Автор дослідження пропонує програму, в якій розкрито зміст кожного з етапів здійснення комунікації в кризовій ситуації [5, с. 118-123].

Отже, як свідчить аналіз наукових праць, питання комунікації є актуальним у всі часи. Науковці не одностайні в поглядах стосовно її класифікації. Щодо внутрішньої комунікації, то її особливість напряму пов'язана з управлінням організації, її будовою, змістом діяльності та зовнішньою ситуацією.

Одним з різновидів внутрішньої комунікації є кризова комунікація, яка свідчить про проблемні моменти в управлінні, організації самої діяльності, у взаєминах в колективі. Все разом може стати причиною різноманітних труднощів та проблем у досягненні мети організації.

Науковцями запропоновану цілу низку рекомендацій та стратегій виходу з кризових станів, і лише детальне їх вивчення та грамотне використання сприятиме ефективному виходу з кризової ситуації.

Список використаних джерел:

1. Грицак Н. Внутрішні комунікації: вчимось розмовляти. *Агробіснес сьогодні : журнал та мультимедійна платформа успішного аграрія.* 2013. URL : http://agro-business.com.ua (дата звернення: 19.09.2023).
2. Козубенко І. В. Кризова комунікація в умовах воєнного стану. С. 175-179. URL : http://elar.naiau.kiev.ua/bitstream/123456789/23842/176-180.pdf (дата звернення: 19.09.2023).
3. Лизавець А. Г., Феєр О. В., Бондарева М. С. Внутрішні комунікації в системі управління персоналом організації. *Економічний вісник НТУУ "Київського політехнічного інституту"*. № 23, 2022. С. 127-132.
4. Мудрак Л. Комунікація і криза. Як громадам протистояти викликам і успішно діяти в період кризи: посіб. Київ: Без видавництва, 2020. 108 с.
5. Скорук О. П. Кризові комунікації під час пандемії COVID-19. *Збірник наукових праць ЧДТУ.* Випуск 59. Серія: Економічні науки. 2020. С. 118-123.
6. Черновол-Ткаченко Р. Л. Роль комунікаційних процесів у забезпеченні ефективного управління навчальним закладом. *Наукові записки кафедри педагогіки*. Випуск XXIV. Харків, 2010. С. 212-220.

Дмитро ЛИСЕНКО, д.ф.
ORCID: 0000-0003-4468-681X
E-mail: d.lysenko@edu.nuou.org.ua
Станіслав ПАВЛУШЕНКО
НУОУ
ORCID: 0000-0001-6222-0656

ОСОБЛИВОСТІ ВНУТРІШНЬО-КОМУНІКАЦІЙНОЇ РОБОТИ У ВІЙСЬКОВОМУ ПІДРОЗДІЛІ У БОЙОВИХ УМОВАХ

В ході російсько-української війни екстремальність бойових дій набуває нового змісту: змінюються умови виконання бойових завдань, збільшується кількість стресорів обстановки, що негативно впливають на психіку і поведінку військовослужбовців. Висока інтенсивність бойових дій призводить до фізичного і психічного виснаження особового складу. В таких умовах актуальною та значущою є організація належної внутрішньо-комунікаційної роботи у військових підрозділах, що, на нашу думку, сприятиме підвищенню морально-психологічного стану військовослужбовців і ефективності виконання завдань за призначенням.

У наказі Генерального штабу Збройних Сил України від 04.01.2017 № 4 "Про затвердження Інструкції з організації інформаційно-пропагандистського забезпечення у Збройних Силах України" під внутрішньо-комунікаційною роботою розуміють напрям інформаційно-пропагандистського забезпечення військових частин (підрозділів), що здійснюється в системі інформаційної роботи посадових осіб командирів (начальників) через сукупність дій, пов'язаних з обробленням і передаванням інформації до особового складу шляхом спілкування. Головною метою внутрішньо-комунікаційної роботи є формування довіри до військово-політичного керівництва держави та військового командування, встановлення зворотного зв'язку з підпорядкованим особовим складом, його готовності до виконання завдань, підтримання і відновлення морально-психологічного стану [1].

На думку хорватських військових психологів, впевненість військовослужбовців в успішному виконанні бойових завдань є результатом поєднання попереднього бойового досвіду, відчуття спроможності, довіри до командної структури, а також від точного розроблення та детального інформування військовослужбовців щодо плану майбутніх бойових дій [2, с. 56]. Усвідомлення військовослужбовцями бойового потенціалу своїх військ, високий рівень довіри до командирів підрозділів, обізнаність у обстановці, яка склалася, та намірах командування щодо ведення бойових дій можна сформувати та розвинути за умов організації дієвої системи внутрішніх комунікацій у військовому підрозділі.

Результати проведеного опитування та безпосередня робота у складі виїзних груп дали змогу виокремити й узагальнити чинники внутрішньокомунікаційного характеру, які негативно впливають на МПС особового складу:

непоінформованість військовослужбовців про загальний перебіг бойових дій;

отримання наказів, розпоряджень, які, на думку військовослужбовців, є незрозумілими, непослідовними і непотрібними;

невиконання вищим командуванням наданих обіцянок.

Зазначимо, що низький рівень навичок командирів (начальників) ланки "рота – батальйон" з налагодження внутрішніх комунікацій у підрозділі, організації належної індивідуальної роботи з підлеглими, зокрема негативними лідерами, часто призводить до того, що для нейтралізації та припинення проявів негативних настроїв і відновлення МПС військовослужбовців доводиться залучати сили і засоби старшого начальника.

У підрозділах, де налагоджено комунікацію командирів із підлеглими, є зворотний зв'язок та оперативне реагування на запити і потреби особового складу, використовують різні форми внутрішньокомунікаційної роботи (бойове і командирське інформування, аналіз проведених дій), командири виконують завдання пліч-о-пліч з підлеглими, МПС військовослужбовців завжди значно вищий.

Безпосередня комунікація командирів та їх заступників з підлеглими на лінії взводних і ротних опорних пунктів, моральна підтримка, психологічна допомога, оперативне реагування на запити й потреби додають впевненості військовослужбовцям, виключають розмови по недовіру до командирів на кшталт "нас усіх покинули", "командири не висовують носа зі своїх КСП", дають змогу своєчасно реагувати на чинники, які негативно впливають на МПС особового складу.

Для налагодження дієвої системи внутрішніх комунікацій у військовій частині та підрозділах слід налагодити системну роботу і належну взаємодію за основними видами забезпечення між службами управління військової частини та підпорядкованими підрозділами, запровадити періодичну роботу мобільних груп за участю представників управління і штабу військової частини для вивчення проблемних питань, оперативного прийняття рішень, проведення інформаційно-роз'яснювальної та соціально-правової роботи задля зняття напруження в підрозділах, забезпечити впровадження у практику діяльності командирів підрозділів ланки "взвод – рота (батарея) – батальйон (дивізіон)" та їм рівних проведення щоденного командирського інформування.

До основних цілей внутрішніх комунікацій у військовій частині (підрозділі) у бойових умовах слід віднести такі:

формування командного духу, згуртування військовослужбовців;

підвищення мотивації та ефективності діяльності;

роз’яснення поточних цілей та завдань військової частини (підрозділу), змісту діяльності та змін, інформування особового складу;

сприяння ефективному процесу прийняття рішень;

формування образу та іміджу військового підрозділу;

сповільнення плинності кадрів.

Таким чином, ключовими завданнями для командирів (начальників) усіх рівнів, заступників з морально-психологічного забезпечення залишається налагодження дієвої системи внутрішніх комунікацій в ланці “командир (начальник) – підлеглі”. Належним чином організована внутрішньо-комунікаційна робота сприятиме постійному зворотному зв’язку з особовим складом, отриманню достовірної інформації про запити і потреби військовослужбовців та оперативному реагуванню на них, поліпшенню психологічного клімату, підвищенню згуртованості та побудові довірливих відносин у військовому підрозділі.

Список використаних джерел:

1. Про затвердження Інструкції з організації інформаційно-пропагандистського забезпечення у Збройних Силах України : наказ Генерального штабу Збройних Сил України від 04.01.2017 № 4.

2. Зоран Комар. Психологічна стійкість воїна. Київ : Посольство Великої Британії в Україні, 2017. 185 с.

Наталія НЕСТЕРЕНКО
НУОУ
ORCID: 0000-0002-4330-080X
E-mail: epin2975@ukr.net

СМИСЛИ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ, ЯК ПРОФІЛАКТИКА “ВИГОРЯННЯ”

Постановка проблеми. В умовах тривалої широкомасштабної агресії з боку Російської Федерації проти України при виконанні службово - бойових завдань відбувається загартування сержантського корпусу Збройних Сил України. Але, професійна діяльність може негативно впливати на розвиток особистості професіонала, однією з проявів якого є розвиток професійного вигоряння. Поняття “вигоряння” зазвичай використовують для позначення переживання людиною стану фізичного, емоційного та психічного виснаження, викликаного тривалою включеністю в емоційно напружені та значущі ситуації. Огляд теоретичних та

емпіричних досліджень дозволяє вважати, що ризик професійного вигоряння залежить від особистих витрат, яких потребує професійна діяльність.

Виклад основного матеріалу. Синдром вигоряння є формою психологічної дезадаптації і проявляється у фізичному, психічному виснаженні, втраті трудової мотивації чи емоційно-ціннісного ставлення до професії. Найбільшим ризиком до його появи схильні фахівці "допомагаючого характеру" праці. Теоретичний аналіз показує, що недостатньо розкритими залишаються особистісні фактори, що сприяють стійкості до професійного вигоряння. Спираючись на концептуальний підхід до єдності свідомості та діяльності (Б.Г. Ананьєв, А.Н. Леонтьєв, Л.С Рубінштейн та ін.) пошук факторів стійкості до неузгодженості між військовослужбовцем (працівником) та професією слід шукати у сенсожиттєвих орієнтаціях сержанта (працівника), його особистих сенсах професійної діяльності та інших ціннісно-смислових змінних [1].

Слід зазначити, що дослідження питання вигорання спрямовує наші наукові пошуки на проблему психічної стійкості як складного особистісного утворення, синтезованого окремими якостями та здібностями, що підтримуються внутрішніми (особистісними) та зовнішніми (міжособистісна, соціальна підтримка) ресурсами. Таким чином, виділяються дві групи чинників стійкості. Це особистісні чинники, до яких можна віднести позитивне ставлення особистості себе, оточуючих, до діяльності, до життя загалом і чинники зовнішнього соціального середовища як різних форм підтримки та допомоги у важких життєвих обставинах [2].

Висновки.

Теоретичний аналіз дозволяє констатувати, що смисли професійної діяльності можуть займати різні позиції в низці смислів життя людини. Якщо сенси праці займають центральне місце у структурі сенсожиттєвих орієнтації особистості, тоді відбувається успішна інтеграція особистості та професії. Згідно з доктриною В. Франкла (В. Франкл, 1990) смисли привносять у трудову діяльність те, що лежить за межами приписаних службових обов'язків і що дозволяє усвідомлено долати негативні явища у праці, серед яких виділяється синдром вигоряння. Отже, смисли праці можна розглядати як ресурси, які забезпечують життєдіяльність працівника.

В.А. Бодров (В.А. Бодров, 2006) розглядає "ресурс" як функціональний (психологічний, фізіологічний, професійний та ін.) потенціал, що забезпечує стійкий рівень реалізації активності людини та досягнення заданих параметрів упродовж певного відрізку часу. На думку Н.Є. Водоп'янової ресурси стійкості до стресу це – актуалізовані потенційні можливості людини у вигляді ментальних, вольових або фізичних дій, спрямованих на адаптацію до стресогенної ситуації або на її перетворення. Основними атрибутами особистісних ресурсів подолання стресових ситуацій є свідомість, усвідомленість, мотивованість, значимість (цінність), цілеспрямованість їх "накопичення" та використання для відновлення особистісного благополуччя після стресів минулого та сьогодення, та підготовки

до прогнозованих майбутніх стресових ситуацій. Ресурси це – допоміжні засоби, можливості, джерела, запаси, які використовуються в особливих чи виняткових випадках для досягнення бажаного результату (Н.Є. Водоп'янова, 2009). S.E. Hobfoll (S. Hobfoll, 1993) називає ресурсами те, що є цінним для людини і допомагає їй впоратися зі стресами [3].

Необхідно зауважити, що витрата ресурсів, впливає з їхнього накопичення як ціннісно-смислового надбання, утворює особистісний досвід, який забезпечує адекватне, оптимальне, раціональне існування. Згідно з гіпотезою Г. Сельє процес ресурсозабезпечення може відбуватися на різних рівнях: поверхневому та глибинному. Ресурси поверхневого рівня легко поповнюються, наприклад, після відпочинку. Відновлення глибинних ресурсів забезпечується з допомогою осмислення життя, переоцінки життєвих пріоритетів. Це відбувається тоді, коли людина намагається побачити всі сенси та вибрати один, який вважає справжнім змістом цієї ситуації. Визначеність у виборі сенсу праці досягається шляхом узгодження потреб та можливостей особистості з вимогами професії та умов праці. При цьому основну роль відіграють цінності особистісної переваги, сформовані відповідно до загальнолюдських постулатів життя.

Список використаних джерел:

1. Лаврова М. Г. Теоретичний аналіз сучасних поглядів на поняття "емоційне вигорання" // Вісник Одеського національного університету. Серія : Психологія. 2014. Т. 19, Вип. С. 194 – 202.

2. Макота Т. В. Емоційне вигорання як наслідок емоційної нестійкості особового складу підрозділів спеціального призначення // Вісник Національного університету оборони України. 2012. Вип. 3. С. 216 – 220.

3. Орел В.Є. Феномен “вигоряння” у закордонної психології: емпіричні дослідження // Журнал практичної психології та психоаналізу. №1. 2001. С. 90 – 91.

Сергій НЕХАЄНКО, к. пед. н
НУОУ
ORCID: 0000-0003-0112-1018
E-mail: panzersergij@ukr.net

МІСЦЕ І РОЛЬ ВНУТРІШНІХ КОМУНІКАЦІЙ В СИСТЕМІ МОРАЛЬНО-ПСИХОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ У ВІЙСЬКОВІЙ ЧАСТИНІ

В умовах ведення довготривалої війни та відбиття російської агресії, які відбуваються сьогодні в Україні, важливо налагодити взаємодію між усіма

ланками у військових частинах, особливо, на наш погляд, між військовослужбовцями, які безпосередньо виконують бойове завдання на полі бою та керівництвом підрозділу, військової частини.

Згідно наказу Генерального штабу Збройних Сил України від 04.01.2017 № 4 “Про затвердження Інструкції з організації інформаційно-пропагандистського забезпечення у Збройних Силах України” під внутрішньо-комунікаційною роботою розуміють напрям інформаційно-пропагандистського забезпечення військових частин (підрозділів), військових навчальних закладів, установ та організацій Збройних Сил України, що здійснюється в системі інформаційної роботи посадових осіб органів військового управління, командирів (начальників) через сукупність дій, пов’язаних з обробкою і передачею інформації до особового складу шляхом спілкування.

Головна мета внутрішньо-комунікаційної роботи – формування довіри до військово-політичного керівництва держави та військового командування, встановлення зворотного зв’язку з підпорядкованим особовим складом, його готовності до виконання завдань, підтримання і відновлення морально-психологічного стану.

Внутрішньо-комунікаційна робота реалізується шляхом:

налагодження комунікаційного процесу;

систематичного та цільового проведення командирського (бойового) інформування з особовим складом військової частини (підрозділу);

аналізу проведених дій;

забезпечення методичними матеріалами, необхідними для організації інформаційної роботи з особовим складом в будь-яких умовах обстановки;

душпастирської опіки військовослужбовців.

Внутрішні комунікації – один із механізмів, що забезпечують стабільність діяльності. Ефективна внутрішньо-комунікаційна робота − запорука стабільності військової частини перед зовнішніми кризами. Будь-які втручання ззовні будуть розбиватись об сформовану у військовій частині єдність. Коли військовослужбовці об’єднані загальними планами на майбутнє, стратегією по їх досягненню, коли кожному зрозуміла роль у цих процесах, то професійна діяльність відбувається набагато ефективніше. Корпоративна єдність − запобіжник, що дозволить стримати тиск будь-яких зовнішніх впливів.

Високий рівень корпоративної ідентичності, лояльності військовослужбовців, оптимальна організаційна культура − загальновизнані фактори успіху військової частини. Внутрішньо-комунікаційна робота спрямована на створення й підтримання корпоративної соціальної відповідальності усередині військової частини. Мова йде про високу репутацію військової частини серед її особового складу, формування позитивного соціально-психологічного клімату, підтримання почуття відповідальності та зацікавленості в справах. Якщо відносини з особовим складом вибудувані ефективно, то керівництву скоріше вдасться домогтися

високого рівня моралі серед військовослужбовців, сильної мотивації та продуктивності. Всі ці фактори сприяють посиленню вихідних позицій військової частини, тому що військовослужбовці допомагають встановлювати позитивні взаємини із зовнішніми зацікавленими сторонами.

Існує хибна думка, що внутрішні комунікації − це лише видання газети, організація й забезпечення Інтернету, проведення масових заходів. Тим часом управління внутрішніми комунікаціями − це повноцінний і дуже впливовий на кінцевий результат процес із цілями та методами, структурою, стратегією й іншими атрибутами. Наведемо кілька визначень поняття внутрішніх комунікацій, що подані у науковій літературі.

Насправді внутрішні комунікації − це комунікаційна діяльність, спрямована на особовий склад військової частини (підрозділу), формування корпоративної ідентичності та лояльності, впровадження і розвиток корпоративних культурних стандартів тощо. Від того, наскільки точно працівники уявляють стратегію організації, по яких каналах організоване спілкування “по вертикалі” та “горизонталі”, як використовується творчий колективний потенціал, наскільки близький персоналу корпоративний імідж, залежить його задоволення роботою в організації, її привабливість для партнерів, для яких якість корпоративної культури є одним із обов’язкових атрибутів надійності та перспективності установи.

Внутрішні комунікації – це система відносин у військовій частині (підрозділі), що базується на принципах корпоративної етики та культури. Все це є чітко продуманою і зваженою інформаційно-комунікаційною політикою, спрямованою на підтримку позитивного іміджу у свідомості військовослужбовців.

Внутрішні комунікації – це частина загального комунікаційного потоку військової частини, зміст якої становлять різні відомості раціонального або емоційного характеру. Їх мета полягає у встановленні, підтриманні та розвитку добропорядних відносин між військовослужбовцями, між підлеглими і командирами (начальниками).

До основних цілей внутрішніх комунікацій у військовій частині (підрозділі) слід віднести такі:

формування командного духу, згуртування військовослужбовців;

формування лояльності до керівного складу (сприяє як більшому ступеню керованості, так і менш болісному впровадженню змін та нових методів роботи);

роз’яснення як поточних цілей та завдань, так і тактики та стратегії розвитку військової частини (підрозділу), змісту нововведень та змін, інформування особового складу;

формування корпоративної культури, образу та іміджу військової частини (підрозділу);

сприяння ефективному процесу прийняття рішень (особовий склад із доступом до інформації здобуває знання, підвищує компетентність та краще озброєний під час прийняття рішень);

сповільнення плинності кадрів: ризик втратити персонал зменшується, якщо військовослужбовці беруть участь у конструктивному внутрішньому діалозі;

особистісний розвиток особового складу (ефективне функціонування задля досягнення цілей і надання кожному персональних завдань та сприяння в особистісному розвитку).

Види внутрішніх комунікацій. Прийнята наступна типологія внутрішніх комунікацій:

між підрозділами;

всередині підрозділів між товаришами по службі за рівнями управління;

міжособистісні;

неформальні.

Внутрішні комунікації за організаційною ознакою зазвичай поділяють на:

1. Вертикальні комунікації, до яких відносять спадні комунікації – (комунікації, спрямовані зверху вниз – від командира до підлеглих), та висхідні комунікації (комунікації, спрямовані знизу вгору – від підлеглих до командира).

Спадні комунікації у військовому колективі використовуються для:

постановки завдань підлеглим, віддання наказів і розпоряджень;

проведення командирського та бойового інформування;

проведення інструктажів;

забезпечення зворотного зв'язку із підлеглими;

забезпечення соціальної підтримки.

В зворотному напрямку під час висхідних комунікацій керівник має на меті:

отримати доповідь за результатами виконання завдання та кінцеві результати;

забезпечити зворотній зв'язок під час усвідомлення завдань;

вивчити думки підлеглих з різних питань;

отримати уявлення щодо необхідності поліпшення діяльності підлеглих.

2. Горизонтальні комунікації – це комунікації, спрямовані на координацію і інтеграцію діяльності особового складу різних підрозділів на одних і тих же рівнях ієрархії (наприклад, спілкування зі службових питань головних сержантів рот по обміну досвідом) для досягнення спільних цілей.

3. Діагональні комунікації – комунікації, які здійснюються особовим складом підрозділів різних рівнів ієрархії. Вони використовуються у випадках, коли комунікації іншими способами ускладнені.

Таким чином, основною метою внутрішніх комунікацій є формування за рахунок підвищення рівня лояльності та вмотивованості особового складу здорової корпоративної культури, яка підтримує стратегію діяльності та розвитку військової частини та допомагає досягти загальної мети.

Таким чином, на теперішній час пріоритетним завданням в діяльності Збройних Сил України є налагодження дієвої системи як внутрішніх комунікацій в ланці "командир – особовий склад", так і організація постійного зворотного зв'язку з військами (силами) та отримання достовірної інформації керівництвом Збройних Сил України з метою виявлення та оперативного вирішення всього спектру проблемних питань.

Список використаних джерел:

1. Агаєв Н.А., Дикун В.Г, Стасюк В.В. Особливості організації морально-психологічного супроводу в арміях зарубіжних країн : навч. посіб. Київ : НДЦ ГП ЗС України, 2020 134 с.
2. Морально-психологічне забезпечення у Збройних Силах України : підручник : у 2 ч. Ч. І. вид. 2-е, перероб. зі змін. та допов. / Н.А. Агаєв, В.Г. Дикун, В.С. Чорний та ін. ; за заг. ред. В.В. Стасюка. Бровари : ТОВ "7БЦ", 2020. 754 с.
3. Павлушенко С.М., Лисенко Д.П. Досвід підтримання та відновлення морально-психологічного стану військовослужбовців військових частин (підрозділів) Збройних Сил України під час російсько-української війни : інформаційно-аналітичні матеріали. Київ : НУОУ, 2023. 28 с.
4. Підопригора І.І., Хайрулін О.М. Інформаційно-пропагандистське забезпечення в збройних силах іноземних держав у кінці XX – на початку XXI століття. Київ : ЦП "Компринт", 2018. 128 с.
5. Про затвердження Інструкції з організації інформаційно-пропагандистського забезпечення у Збройних Силах України : наказ Генерального штабу Збройних Сил України від 04.01.2017 № 4. Київ : РВВ ЦЗСД МО та ГШ ЗС України, 2017.

Володимир ПАСІЧНИК, к.психол.н., доц.
ORCID: 0000-0002-4094-049X
E-mail: vladimirpasichnik4@gmail.com,
Олександр САВЧУК, к.психол.н.
ХНУПС ім. Івана Кожедуба
ORCID 0000-0002-8309-5927
E-mail: savchuk.project@gmail.com

ШЛЯХИ УДОСКОНАЛЕННЯ СИСТЕМИ НОРМАТИВНОГО СПІЛКУВАННЯ ВІЙСЬКОВОСЛУЖБОВЦІВ ЗБРОЙНИХ СИЛ УКРАЇНИ

Проведене нами вивчення проблематики нормативного спілкування військовослужбовців Збройних Сил України (ЗС України) засвідчило, що на

теперішній час існує протиріччя між необхідністю удосконалення міжособистісної та міжгрупової взаємодії особового складу при виконанні завдань за призначенням, особливо з огляду на наявний сучасний досвід ведення бойових дій та перспективи подальшого членства нашої країни в НАТО, і недостатнім теоретико-методичним підґрунтям вирішення цього завдання. Нині питання реалізації нормативного спілкування військовослужбовців ЗС України недостатньо представлені у сучасних наукових працях та не у повній мірі забезпечені обґрунтованими методичними рекомендаціями щодо їх вирішення.

Отже у зв'язку з важливістю забезпечення нормативності спілкування військовослужбовців військових підрозділів ЗС України, як значимого соціально-психологічного чинника, що сприяє підтриманню належного рівня їх морально-психологічного стану, актуально постає завдання обґрунтування шляхів удосконалення системи нормативного спілкування особового складу в сучасних умовах та з урахуванням перспектив розвитку нашого війська.

За результатами проведеного нами дослідження сутності нормативності спілкування, а також аналізу системи нормативного спілкування військовослужбовців такими шляхами встановлено наступні.

1. Підвищення рівня комунікативної компетентності військовослужбовців, як важливої умови забезпечення ефективності їх взаємодії, обміну інформацією та об’єктивного взаємосприйняття.

2. Чітке усвідомлення усіма категоріями військовослужбовців основної мети, на реалізацію якої має бути спрямоване спілкування особового складу, та конкретизація завдань, шляхів і організаційно-методичного підґрунтя щодо її ефективного досягнення.

3. Визначення сфер спілкування військовослужбовців, які потребують унормування та більш чіткої регламентації, а також вироблення, закріплення і введення у практику використання відповідних норм. У ході проведених нами теоретичних та емпіричних досліджень такими сферами були визначені:

– удосконалення нормативного забезпечення гендерної рівності та попередження гендерної дискримінації у військових підрозділах;

– унормування та правове врегулювання дій командирів щодо військовослужбовців, які у процесі спілкування в бойових умовах виявляють себе генераторами паніки, здійснюють деструктивний чи деморалізуючий вплив на оточуючих, мають девіантні вияви, що не містять ознак злочину;

– посилення регламентованості комунікації військовослужбовців, впровадження дієвих заходів обмеження передачі та розповсюдження інформації не уповноваженими посадовими особами у випадках масової загибелі людей, здачі у полон значної кількості особового складу та інших надзвичайних ситуаціях;

– удосконалення організаційно-методичного забезпечення дій посадових осіб щодо встановлення ознак дезадаптивних станів військовослужбовців у процесі

спілкування з ними і реалізації стандартизованих заходів надання їм належної психологічної допомоги.

У значній мірі вирішенню зазначених завдань могли би посприяти, на наш погляд, упровадження відпрацьованих з урахуванням сучасної проблематики функціонування військ та переходу на стандарти НАТО "Концепції інформаційного забезпечення бойової діяльності військових формувань" та "Етичного кодексу поведінки військовослужбовців щодо запобігання ставленню і діям, які можуть привести до ситуацій нерівності чи дискримінації".

4. Сприяння командирів, структур морально-психологічного забезпечення, інших посадових осіб військових частин та підрозділів Збройних Сил України якісній реалізації у практиці управлінської взаємодії інформаційно-комунікативної, інтерактивної та перцептивної функцій спілкування на основі розуміння їх сутності, особливостей здійснення, чинників та умов забезпечення ефективності.

5. Забезпечення спрямування змісту національно-патріотичної та психологічної підготовки командирів усіх рівнів на оволодіння ними різноманітними методами, прийомами, техніками, засобами спілкування щодо реалізації ефективного комунікативного впливу на підлеглий особовий склад, у тому числі в екстремальних умовах виконання завдань за призначенням.

Таким чином, обґрунтовані на основі проведених досліджень шляхи удосконалення системи нормативного спілкування особового складу військових частин та підрозділів Збройних Сил України є підґрунтям для подальшої практичної реалізації інновацій, спрямованих на підтримання належного рівня морально-психологічного стану особового складу та здорового соціально-психологічного клімату у військових підрозділах.

Сергій ПОЗДИШЕВ, к.пс.н.
НУОУ
ORCID: 0000-0001-7225-709x

СОЦІАЛЬНО-ПСИХОЛОГІЧНІ ОСОБЛИВОСТІ ФОРМУВАННЯ КОЛЕКТИВНОЇ ДУМКИ ПІД ЧАС ВНУТРІШНЬОКОМУНІКАЦІЙНОЇ РОБОТИ У ВІЙСЬКОВОМУ ПІДРОЗДІЛІ

Колективна думка становить сукупність індивідуальних суджень більшості особового складу військового підрозділу, виражає позицію, погляди, переконання, ціннісні орієнтації військовослужбовців. Відомо, що кожен військовослужбовець вільно або мимоволі порівнює власні вчинки і діяльність з думкою командира та більшістю особового складу, а також найавторитетніших товаришів по службі [1, с. 96–97]. Це закономірність, адже

колективна думка, що виражає розум, волю і почуття більшості, викликає в людини прагнення до самовдосконалення. Спонукальна сила колективної думки визначається також тим, що особистість остерігається негативних оцінок і докорів більшості, яка може знизити її авторитет у колективі.

Важливу роль у керуванні колективною думкою відіграє згуртованість особового складу військового підрозділу. Коли колектив тільки створюється, сформувати єдину думку командирові набагато важче, адже підлеглі ще не зблизилися і не розуміють один одного. У цей період спостерігається так звана піддатливість, чи, інакше кажучи, сприйнятливість новачків до думок окремих несумлінних підлеглих [2, с. 131–135]. Тоді в колективі може з'явитися індивідуально-групова думка, що відрізняється від думки командира і більшості особового складу. Як правило, негативна думка захищає недобросовісних, недисциплінованих підлеглих і суперечить загальній думці колективу.

Влада й досвід, повага та довіра роблять авторитетним і вражаючим кожне слово командира. Одне це зобов'язує командира уникати необачних суджень, необдуманих висновків. Перш ніж вимовити вголос яку-небудь думку, командир зобов'язаний ретельно продумати її, тому що вона неодмінно відображатиметься на поведінці підлеглих. Відрив від дійсності, марнослів'я, невпевненість викликають недовіру до командира, у той час як переконливість і категоричність його слів змушують не сумніватися в правильності його позиції, особливо в бойових умовах. Колективна думка в екстремальних умовах діяльності відрізняється особливою єдністю поглядів та оцінних суджень.

Колективна думка як соціально-психологічний процес має три умовних етапи розвитку.

На першому етапі підлеглі сприймають, переживають та оцінюють вчинок або подію, у кожного з них з'являється своя суб'єктивна оцінка й індивідуальна думка-судження.

На другому етапі формування колективної думки підлеглі обмінюються думками та оцінками. Цей етап може проходити або спокійно, або в суперечках залежно від того, наскільки інформація стосується інтересів кожної особистості.

На третьому етапі у формуванні колективної думки беруть участь групи підлеглих, які мають різні знання, переконання, інтереси, досвід. Чим більше зворушує вчинок або подія, загальні інтереси підлеглих, найбільш значущі питання військової служби, повсякденної або бойової діяльності, тим активніше вони дискутують і відстоюють групові інтереси й погляди.

Якщо підлеглі правильно і глибоко розуміють сутність процесів, які відбуваються, сперечаються не заради власних інтересів, а в ім'я вирішення завдань військової служби, то в колективі народжується компетентна

колективна думка. Якщо з якихось важливих причин підлеглі знають мало або їм не додають особливої уваги, то вони, безумовно, не можуть судити про них досить компетентно та кваліфіковано.

Для оптимізації керування колективною думкою командиру не можна упустити момент першого етапу, коли підлеглі ще тільки переживають події, які їх схвилювали, і ставлення до них ще не сформовано. Відомо, що тому, хто першим повідомив про подію, значно легше сформувати групові оцінні судження щодо цієї події. Це визначається так званим феноменом психічної інерції. Знаючи джерела повідомлень і їхній вплив на розвиток групової думки, командир завжди може загасити вогнище помилкового судження і спрямувати погляди в єдиний фокус позитивної спільної думки. Головне в цей момент – попередити появу незрілих поглядів, упереджених оцінок. Допомогти в цьому командиру можуть молодші командири або актив підрозділу, які, постійно перебуваючи серед товаришів по службі, швидко реагують на новину, правильно її оцінюють, формують позитивну установку на сприйняття інформації.

На другому етапі командиру важче змінити хибні судження окремих військовослужбовців, тому що індивідуально-групова думка має відому інерцію. У цьому разі потрібно переконувати підлеглих, змінювати їх погляди, повідомляти колективу конкретні факти та аргументи без згадування хибних суджень. Іноді достатньо не звертати увагу на неточну інформацію, щоб вона втратила свій зміст і значення.

Керувати груповими думками непросто, ще складніше розвивати принципову критику. Досвід роботи з формування зрілої колективної думки показує, що критикувати потрібно передусім не дрібні помилки й окремі висловлювання, а серйозні порушення моральних норм, військової дисципліни, негативну спрямованість особистості. Найрозповсюдженішою помилкою недосвідчених командирів є намагання зробити предметом обговорення підлеглого керівного складу майже кожен випадок порушення.

Формуванню колективної думки передує велика організаторська робота, важливе місце в якій приділяється груповим бесідам і зборам особового складу військового підрозділу. Командиру важливо оцінювати зрілість колективної думки, мати чіткий зворотний зв’язок через систему відвертості і справедливої критики недоліків [3, с. 491–492].

Таким чином, керування колективною думкою досягається командиром завдяки дотриманню таких умов: розвиток системи внутрішніх комунікацій у підрозділі; регулярне інформування про поточні події; умілий вибір найдоцільніших форм впливу на свідомість і почуття підлеглих (наради, збори, групові й індивідуальні бесіди та ін.); доведення до підлеглих правдивої інформації; доведення до колективу власної думки командира з найважливіших питань служби і побуту, її значимості для зміцнення

дисципліни і підвищення боєздатності підрозділу; підтримання статутних взаємин та активна боротьба з відхиленнями від норм загальнолюдської моралі.

Список використаних джерел:

1. Капосльоз Г.В., Глова Л.А., Куліда І.М. Соціальна психологія у військовій діяльності : навч. посіб. Київ : НУОУ ім. Івана Черняховського, 2018. 160 с.

2. Прикладна психологія військової діяльності: підручник / за заг. ред. В. І. Осьодла. Київ : НУОУ ім. Івана Черняховського, 2022. 292 с.

3. Морально-психологічне забезпечення у Збройних Силах України : підручник : у 2 ч. Ч. 1. Вид. 2-ге, перероб. зі змін. та допов. Н.А. Агаєв, В.Г. Дикун, В.С. Чорний та ін.; за заг. ред. В.В. Стасюка. Бровари : ТОВ "7БЦ", 2020. 754 с.

Іван ПОНОМАРЕНКО
НУЦЗУ
ORCID: 0000-0003-4780-3209
E-mail: ponomar500@gmail.com

ВНУТРІШНЯ МОТИВАЦІЯ ЯК ВАЖЛИВИЙ КОМПОНЕНТ ПСИХОЛОГІЧНОГО БЛАГОПОЛУЧЧЯ РЯТУВАЛЬНИКІВ

В процесі професійного становлення фахівців служби цивільного захисту процес професіоналізації вимагає від рятувальників бути відданими обраній справі, бути внутрішньо мотивованими та намагатися бути самоефективними у діяльності забезпечуючи психологічне благополуччя. Рятувальники, які мотивовані отримати результат від діяльності мають безліч переваг перед рятувальниками, які не зацікавлені у результаті або амотивовані. Одним із сучасних підходів до мотивації є теорія самодетермінації Е. Десі та Р. Райана. У теорії самодетермінації внутрішня мотивація розглядається як прагнення суб'єкта професійної діяльності виконувати завдання заради інтересу у самому процесі роботи, задоволення та радості від її виконання. Розглядаючи зовнішню мотивацію при виконанні завдань, то завдання виконується суб'єктом з метою досягнення інших цілей, зовнішніх відносно до самої діяльності. Внутрішня мотивація пов'язана з внеском зусиль та більш високим рівнем психологічного благополуччя, продовжується навіть при відсутності зовнішніх нагород та покарань та розвиває компетенції. Внутрішня мотивація тісно пов'язана з рівнем

ідентифікованої регуляції діяльності, тобто діяльність здійснюється рятувальниками з метою досягнення результатів, які обрані суб'єктом усвідомлено та суб'єктивно важливі, як наприклад, кар'єрне зростання рятувальників. Окрім цього, внутрішня мотивація пов'язана з інтегрованою регуляцією, тобто діяльність знаходиться у гармонії з іншими сферами життя суб'єкта і перетворюється як частина власної ідентичності, наприклад покликання бути рятувальниками, допомагати людям у екстремальних ситуаціях.

Отже, внутрішня мотивація є важливим компонентом психологічного благополуччя рятувальників як суб'єктів професійної діяльності.

Список використаних джерел:

1. Deci, E.L., Connell , J.D., Ryan, R.M. (1989). Self-determination in a work organization. Journal of Applied Psychology, 74(4), 580-590.

Ольга СЕВЕРІН
ЖВІ ім. С.П. Корольова
ORCID: 0009-0006-1376-2583
E-mail: olya013severin@gmail.com

АНАЛІЗ ВПЛИВУ ГРАФІЧНОГО ДИЗАЙНУ НА ПОВЕДІНКУ ЦІЛЬОВОЇ АУДИТОРІЇ

Від початку агресивних дій Росії проти України та подальшого початку війни на нашій території ворог активно використовує графічний дизайн для створення візуального продукту. Іншими словами, держава-агресор вже багато років веде гібридну війну[1] не лише проти України, а й проти всього світу, адже однією зі складових війни 4G є інформаційні маніпуляції. Адже саме так люди звертають увагу на інформаційні повідомлення, роблять певні висновки у своїй свідомості та змінюють поведінку у потрібний бік. Все тому, що графічний дизайн та його правильне планування з урахуванням особливостей і потреб цільової аудиторії здатні створити картинку, яка допомагає споживачам обдумати ідеї та зробити певні висновки, що, в свою чергу, призводить до бажаної зміни поведінки[3]. Знання того, як графічні продукти моделюють поведінку, також може допомогти у протидії російській пропаганді.

Графічний дизайн використовується не лише в маркетингу, а й в інших сферах, наприклад, у військовій. Він може бути використаний для створення таких продуктів, як:

книжкові матеріали та ілюстрації;
реклама та інформаційні плакати;
графічні рішення для листівок і марок;
дизайн вінілових та DVD дисків;
фірмовий стиль заходу – створення логотипу;
буклети, брошури, календарі та інша продукція психологічного впливу;
упаковка, етикетки та кришки;
сувенірна продукція;
веб-сайти та мобільні додатки.

У майбутньому готовий продукт можна використовувати як матеріал для впливу на свідомість людини, привертаючи таким чином її увагу та змінюючи її поведінку/зовнішній вигляд/поведінку у бажаному напрямку.

Наразі найпомітнішою сферою застосування графічного дизайну є маркетинг. Це на багато глибше і всеохоплююче поняття, ніж просто просування, реклама і продажі. Однією з його ключових складових є графічний дизайн, який використовується для створення візуально ефективних продуктів. Одним з най успішніших прикладів графічного дизайну в у впливі на свідомість ЦА є компанія Nike [2]. Бренд приділив багато уваги кольорам, шрифтам і формам при застосуванні основних елементів для створення привабливого іміджу. Компанія на власному прикладі показала, що невеликий, ненав'язливий логотип може привернути майже загальну увагу.

Вплив графічних продуктів на поведінку людини залишається актуальною темою і сьогодні. Адже те, як операція чи інший захід візуалізує свої ідеї, цілі та завдання, є першим враженням, яке вона справляє на цільову аудиторію. З цієї причини багато вчених піднімали це питання. Один з них, доктор Р. Джоші, у своїй книзі “Graphic Products In Event Design” [3] розкрив, як створювати продукти, що втілюють обличчя компанії або події. Як най ефективніше привернути увагу споживачів візуальної інформації та на чому зосередити увагу при розробці продукту. Bahira Dar-Ethiopia та його роботи також заслуговують на увагу. Доведено, що ігнорування умов цільової аудиторії часто створює неефективні стимулюючі умови та призводить до провалу комунікації. Автор також підкреслює, що для успішного розвитку комунікації проект повинен бути попередньо протестований разом з цільовою аудиторією, наводить приклади позитивного і негативного використання графічних продуктів і вказує нате, що при створенні початкового дизайну візуального продукту найважливіші ідеї могли бути невраховані і можуть бути виправлені в процесі попереднього оцінювання. Якщо їх не виправити, такі недогляди можуть суттєво завадити досягненню бажаної реакції. Окремо варто розглянути книгу[6] К. М. Родиганова й І. О. Єрмакова, в який вони описують яким чином під час війни використовують образи (дітей, жінок, ворогів, героїв тощо) у сприйнятті. У своїй праці [6] автори описують чотири основні види маніпуляцій з візуальним контентом в контексті інформаційно-смислової війни: фотоманіпуляції

(втручання в цілісність зображення, ретуш, монтаж); фотофейки як маніпуляції з контекстом та описом фотографій; постановочні світлини; використання засобів художньої виразності (композиція, ракурс, кадрування, невербальне повідомлення тощо).

У військовій сфері графічний дизайн з'явився з посиленням інформаційно-психологічних операцій[8]. Графічний дизайн використовувався і продовжує використовуватися у виробництві широкого спектру ефективних візуальних продуктів, від пропагандистських листівок до гуманітарних продуктів. Однією з країн, які стали засновниками цього способу впливу на свідомість людей, є США, де є багато успішних прикладів продуктів, розроблених за допомогою графічного дизайну.

Ефективність впливу на людей також залежить від того, чи правильно проаналізована цільова аудиторія[7], чи правильно підібрані головні та другорядні аргументи. Якщо аналіз не є коректним, вплив може мати протилежний бажаному ефект. Важливу роль відіграють також різні характеристики цільової аудиторії. Найпростішими прикладами є мовна та регіональна приналежність. Використання румунської символіки та мови у візуальному продукті, орієнтованому на білорусів, є небажаним, оскільки це не приведе до бажаного результату. Однак з російським вторгненням в Україну часу на вивчення деталей стало менше. Тому на перший план вийшли якість, унікальність та масштаб розповсюдження розроблених нами продуктів. Розроблені нами відео продукти спрямовані на максимально широку цільову аудиторію.

Не зважаючи на плин часу, питання використання та вивчення графічного дизайну в сфері інформаційно-психологічних операцій залишається актуальним і сьогодні, оскільки Росія постійно проводить активні заходи психологічного впливу в Україні та світі.

Список використаних джерел:

1. Тараненко М. М., “ГІБРИДНА ВІЙНА В УКРАЇНІ: ІСТОРІЯ ТА СУЧАСНІСТЬ”// ВІСНИК НТУУ “КПІ”. Політологія. Соціологія. Право. Випуск 3/4 (31-32) 2016.
2. Продавец обуви. История компании Nike, рассказанная ее основателем. Фил Найт ULR:https://books.google.com.ua (дата звернення: 16.09.2023).
3. Dr. R Joshi, “Graphic Products In Event Design”. – Видавництво “Thames & Hudson”, 2021 – 352 с.
4. ULR:https://er.knutd.edu.ua/bitstream/123456789/19147/1/Kolisnyk_mono_2020.pdf (дата звернення: 09.09.2023).

URL:https://repository.sspu.edu.ua (дата звернення: 12.09.2023).

5. URL:http://r.donnu.edu.ua/handle/123456789/1558 (дата звернення: 01.09.2023).
6. URL:https://www.proquest.com (дата звернення: 20.09.2023)

7. URL:https://www.inacademy.uz/index.php/ejsspc/article/view/3814/3385 (дата звернення: 05.09.2023).

Василь СТАСЮК, д.п.н.
ORCID: 0000-0002-7943-8456
E-mail: vvsrad@gmail.com
Володимир ДИКУН
ORCID: 0000-0001-8144-7098
E-mail: dykynvg@gmail.com
Андрій КИРИЧЕНКО, д.ф. (PhD)
НУОУ
ORCID: 0000-0002-1333-5980
E-mail: kyrychenkoav@ukr.net

ДІЯЛЬНІСТЬ ПОСАДОВИХ ОСІБ ВІДДІЛЕННЯ МОРАЛЬНО-ПСИХОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ БРИГАДИ ПІД ЧАС ОТРИМАННЯ ЗАВДАННЯ (RECEIPT OF MISSION)

Командир є найважливішим учасником MDMP. Командир використовує свій досвід, знання і судження, щоб ефективно керувати процесом MDMP.

Начальник штабу (chief of staff, COS) або виконавчий офіцер (executive officer, XO) є ключовим учасником MDMP. Він управляє і координує роботу штабу і забезпечує контроль якості в ході MDMP. Начальник штабу повинен чітко розуміти задум і вказівки командира. Він контролює весь процес: встановлює графік роботи штабу та його секцій, час і місце проведення брифінгів, надає необхідні інструкції для завершення планування.

Зусилля штабу і всіх секцій в ході MDMP спрямовуються на надання командиру допомоги щодо розуміння обстановки, прийняття рішень та їх синхронізації в план або наказ.

Загалом, командири ініціюють MDMP після отримання або в очікуванні бойового завдання, або ж неофіційною – в разі реагування на зміни обстановки.

Мета першого кроку, “Отримання завдання” – приведення в стан готовності всіх учасників майбутнього процесу прийняття воєнних рішень планування, визначення часу, який є для планування, визначення підходу до планування, у тому числі і як скоротити сам процес, якщо це потрібно/буде потрібно.

Основним продуктом цього кроку є первинна оцінка операційного середовища, вказівки щодо підпорядкування команд (сил і засобів) та документ, який містить попередні вказівки командира – WARNO.

Як тільки військова частина (полк, бригада тощо) отримує бойове завдання (або, коли наказує командир військової частини), секція інтеграції поточних

операцій (S-3) оповіщає штаб та інших ключових учасників MDMP про необхідність підготовки до процесу планування.

Зміст роботи посадових осіб структур морально-психологічного забезпечення (далі – МПЗ) під час процедури – "приведення в готовність штабу та інших ключових учасників MDMP" передбачає:

оповіщення офіцерів структурного підрозділу з МПЗ штабу військової частини;

збір відповідного особового складу (за необхідності);

розподіл (уточнення розподілу) посадових осіб структурного підрозділу з МПЗ штабу військової частини за командними пунктами (CP) (UKR national elements – пунктами управління), включення їх до оперативного складу секцій командних пунктів (груп пунктів управління);

зайняття оперативним складом місць на командних пунктах (CP) (UKR national elements – пунктах управління) (хто? де?);

уточнення оперативним складом секцій/груп командних пунктів (пунктів управління) функціональних обов'язків щодо роботи у складі секції/групи відповідного командного пункту/пункту управління;

перевірка оперативним складом секцій/груп командних пунктів (пунктів управління) та підготовка до застосування засобів зв'язку та АСУ на робочих місцях (за наявності);

організація роботи (бойового чергування) оперативним складом секції/групи МПЗ на відповідному командному пункті (пункті управління).

Після доведення до особового складу штабу про початок MDMP, штаб та всі ключові учасники MDMP готується, у частині що стосується, до аналізу бойового завдання, збираючи необхідний для цього інструментарій. Під час підготовки необхідного інструментарію особовий склад структурного підрозділу з МПЗ здійснює:

усвідомлення первинних завдань, вивчення (уточнення директивних документів) документів вищого командування (старшого начальника);

з'ясування даних щодо району операції (area of operations, AO);

в разі реагування на зміни обстановки – усвідомлення ситуації та характеру зміни обстановки;

отримання необхідних документів, підготовку інформаційно-довідкових матеріалів та інструментарію:

– документів, які стосуються отриманого (очікуваного) завдання, району операції, графічних документів, топографічних карт, макетів тощо;

– наявних розвідувальних даних, оцінок вищих штабів щодо району операції;

– оцінок, аналізів, відомостей інших військових (цивільних) організацій (відомств) тощо;

вивчення додаткових, довідкових матеріалів (каталогу об'єктів, інформаційних бюлетенів, розвідувальних донесень тощо);

підготовка формалізованих документів, варіантів донесень і т.ін.

Після того, коли зібрано весь необхідний інструментарій, наявна матеріальна база та засоби, у кожній штабній секції (від S-1 до S-9) відбувається процедура оновлення поточних оцінок – особливо, що стосується стану дружніх підрозділів, ресурсів та ключових міркувань щодо аспектів цивільного середовища. Загалом, під час процедури оновлення поточних оцінок відбувається не тільки узагальнення найважливіших факторів та припущень з точки зору окремо взятої секції, а також узагальнення інформації від інших секцій,військових і цивільних організацій.

Таким чином, основним завданням процедури оновлення поточних оцінок є – оцінка наявної бази даних та визначення прогалин в інформації. За результатами оцінки, згідно NATO STANAG, приймається рішення щодо організації додаткового збору інформації, (тієї що не вистачає), в частині що стосується морального стану особового складу (Morale).

Враховуючи національні особливості (UKR national elements), структури МПЗ безпосередньо відповідають за збір, систематизацію, аналіз, узагальнення, повноту та достовірність даних щодо морально-психологічного стану (далі – МПС) особового складу військ, а також в частині що стосується з'ясування впливу ключових міркувань цивільного середовища на МПС своїх військ.

У зв'язку з цим, з метою оновлення поточних оцінок, підлеглим посадовим особам структур МПЗ ставиться завдання щодо оцінювання МПС особового складу підрозділів військової частини, встановлення рівня морально-психологічної готовності військовослужбовців до дій у визначених умовах обстановки, усунення прогалин в інформації щодо базових критеріїв та показників МПС особового складу.

Після отримання бойового завдання, штаб проводять попереднє оцінювання часу який є для MDMP, підготовки і початку виконання бойового завдання.

Оскільки час є фактором, який враховується в усіх операціях. З метою надання підлеглим достатнього часу для планування, згідно NATO STANAG, командири дотримуються правила "однієї третини до двох третин". Вони відводять одну третину наявного часу на власне планування та виділяють дві третини своїм підлеглим для їх планування та підготовки.

Чим більше часу командири потратять на власний MDMP, тим більше часу буде у противника для підготовки і переміщення додаткових підрозділів, сил та засобів.

На основі поточного розподілу часу здійсненого командиром, штаб розробляє тайм-лінію (графічне уявлення календарного плану подій), де визначається, скільки часу можна витратити на кожний крок і в цілому MDMP.

Крім цього, тайм-лінія MDMP вказує необхідні документи та хто за них відповідає, визначає час і місце проведення нарад та брифінгів і хто до них залучається. Вона служить орієнтиром для секцій командного пункту (UKR

national elements – підрозділів пунктів управління) протягом всього процесу прийняття воєнних рішень.

На підставі цієї інформації, керівник підрозділу МПЗ (UKR national elements) складає розрахунок часу роботи службових осіб підрозділу МПЗ в ході планування бою (бойових дій) де зазначається: скільки загалом часу необхідно для планування МПЗ отриманого завдання; відпрацювання завдань з МПЗ під час відповідних кроків MDMP; хто, який документ/матеріал до якого терміну має підготувати/відпрацювати; хто, коли та де та яку доповідь здійснює; час та місце, участі у проведенні брифінгів тощо.

З урахуванням національних особливостей та вимог NATO STANAG, з дозволу командира військової частини, з метою орієнтування підлеглих про характер майбутніх дій та надання більшого часу для планування МПЗ отриманого завдання підрозділам можуть віддаватися (направлятися) початкові вказівки з МПЗ.

Після віддачі WARNO 1. штаб та його структурні підрозділи переходить до відпрацювання процедур другого кроку MDMP, з урахуванням компетенцій та особливостей виду діяльності.

Список використаних джерел:

1. Агаєв Н. А., Дикун В. Г, Стасюк В. В. Особливості організації морально-психологічного супроводу в арміях зарубіжних країн : навч. посіб. Київ : НДЦ ГП ЗС України, 2020 134 с.

2. Агаєв Н. А., Дикун В. Г., Стасюк В. В. Особливості оцінювання цивільних аспектів (міркувань) відповідно до оперативних стандартів НАТО : навч. метод. посіб. Київ : Видання університету, 2018. 44 с.

3. Процес прийняття рішень під час бойових дій. Київ : Міжнародний Комітет Червоного Хреста (МКЧХ), 2018. 68 с.

4. Морально-психологічне забезпечення у Збройних Силах України : підручник : у 2 ч. Ч. І. вид. 2-е, перероб. зі змін. та допов. / Н. А. Агаєв, В. Г Дикун, В. С. Чорний та ін. ; за заг. ред. В. В. Стасюка. Бровари : ТОВ “7БЦ”, 2020. 754 с.

5. STANAG 2014 TOP (Ed. 9) : 2000. Formats for Orders and Designation of Timings, Locations and Boundaries. 2000 (NATO STANDARDIZATION OFFICE (NSO)). URL: http://www.trngcmd.marines.mil/Portals/.pdf. (дата звернення: 06.04.2021).

6. STANAG 2437 : 2017. AJP-01(E)(1) Allied Joint Doctrine for Operations. 2017 (NATO STANDARDIZATION OFFICE (NSO)). URL: https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDE_V1_E_2437.pdf. (дата звернення: 20.03.2023).

7. STANAG 2490 : 2019. AJP-3(C) Allied Joint Doctrine for the Conduct of Operations. 2019 (NATO STANDARDIZATION OFFICE (NSO)). URL:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf. (дата звернення: 20.03.2021).

8. STANAG 2526 : 2019. AJP-5 Allied Joint Doctrine for the Planning of Operations. 2019 (NATO STANDARDIZATION OFFICE (NSO)). URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/837082/dcdc_doctrine_nato_planning_of_ops_ajp. (дата звернення: 20.03.2023).

9. STANAG 2565 : 2019. AmedP-8.10A Psychological Guide for Leaders Across the Deployment Cycle. 2019 (NATO STANDARDIZATION OFFICE (NSO)). URL: ttps://www.coemed.org/files/stanags/03_AMEDP/AMedP-8.10_EDA_V1_E_2565.pdf. (дата звернення: 20.03.2023).

10. STANAG 2631 : 2019. APP-28 Tactical Planning for Land Forces. 2019 (NATO STANDARDIZATION OFFICE (NSO)). URL: https://www.forsvarsmakten.se/siteassets/english/swedint/engelska/swedint/information-to-admitted-students-and-participants/nltpc/app-28-eda-v1-e.pdf. (дата звернення: 06.04.2023).

Олег ХАЙРУЛІН, к.психол.н.
НУОУ
ORCID: 0000-0001-7042-7948
E-mail: oleg.khairulin.ph@gmail.com

ПЕРФОРМАТИВНИЙ ПОТЕНЦІАЛ МОВНОЇ ГРИ У ПУБЛІЧНОМУ ДИСКУРСІ

Життєдіяльність сучасної людини є об’єктивним віддзеркаленням нової епохи, особливості якої втілилися в науковому та загальнокультурному акронімі VUCA. Концепт VUCA був обраний світовими лідерами і науковцями для опису хаотичного, бурхливого й такого, що стрімко змінюється, середовища, яке швидко стало “новою нормою”, та особливості якого використовуються агресивними геополітичними суб’єктами в якості засобів впливу. Прикладом цього є злочинні дії російської федерації, що призвели до анексії українського Криму та широкомасштабної російсько-української війни. Геополітична стратегія рф передбачає досягнення військово-політичних цілей у тому числі через використання особливостей сучасного інформаційного (медіа) простору. Зокрема у рф активно поширюються наукові дискурси соціального інжинірингу, геймифікації і дотичного ігровій тематиці рефлексивного управління. За наведених обставин вітчизняна наука повинна своєчасно і якісно робити свій внесок в справу унеможливлення, стримування й усунення соціальних наслідків медіа-активності зовнішніх ворожих і недружніх сил, спроб використання

інформаційного простору для дестабілізації соціального, економічного і політичного благополуччя українського суспільства.

Дослідження присвячене складному і багатоаспектному явищу, що складає теоретичний і прикладний науковий інтерес – перформативному (від англ perform – виконувати) потенціалу мовної гри у просторі публічної політики і публічного дискурсу (масової комунікації) [6]. Об'єктом дослідження виступає мовна гра, предметом – характеристики її перформативного потенціалу, що реалізується усіма учасниками (стейкхолдерами) публічного дискурсу, соціального (публічного) спілкування.

Грунтовна розробка ключових аспектів проблематики психогенного, перформативного впливу інформації на людину стала результатом комунікативного повороту у філософії, інших наукових дисциплінах та відображена в працях психологів і представників психолінгвістичного напряму Л. С. Виготського, Л. Вітгенштайна, Д. Остіна, Т. М. Титаренко, Л. А. Найдьонової, Л. В. Засєкіної, Л.О. Калмикової, Н.В. Чепелєвої, В.В. Жовтянської, С.Г. Денисюк, О.М. Кочубейник, Н.В. Чепелєвої, Л.Ф. Компанцевої, В.В. Зірки, К.О. Черемних, І.В. Александрук, О.О. Золотар, О. О. Селіванової, Д. Мак-Квейла, Д. Лакоффа, М. Джонсона та ін.

На ігрову природу комунікації і діяльності людини у ній вказує чисельна кількість наукових досліджень широкого хронологічного і змістовного діапазону. Історія досліджень гри, як соціального явища, розпочинається ще філософськими роботами Платона. Водночас дослідження гри як форми і засобу вербальної і креолізованої комунікації розпочинається лише напочатку XX століття, коли Л. Вітгенштайн обгрунтовано описав мовну (мовленнєву) гру як модель комунікації або конституції тексту, в якій відтворюється несуперечливий контекст і слова вживаються у суворо визначеному сенсі. Гра як модус діяльності атрибутивно передбачає інтеракцію (взаємодію), спілкування, комунікацію. Позбавлена циклічності, рекурсивного повторення, така, що має хоча би мізерну долю невизначеності комунікація і є грою. Тобто комунікація у більшості – гра. Аналіз актуальних розвідок щодо перформативного (сутності перформативного впливу також відповідає ознака - маніпулятивний) потенціалу мовної гри саме у публічному дискурсі, свідчить про певну обмеженість таких досліджень. На нашу думку це обумовлено певною специфікою і складністю як самого контрукту "мовна гра у публічному дискурсі", так і засобів його дослідження, особливо на рівні реальних мовленнєвих дій (публічних виступів, публікацій тощо). Також обрання наукової методології вивчення перформативного потенціалу мовної гри у публічному дискурсі залежить від конкретних наукових дисциплін, які б уможливили такий вибір. На нашу думку такими науковими дисциплінами доцільно обрати передусім психолінгвістику, лінгвістику, психологію особистості і соціальну психологію. Спеціальною методологічною і предметною платформою тут виступає синтез теорії мовних (мовленнєвих) ігор Л. Вітгенштайна, теорії

походження і розвитку вищих психічних функцій людини Л.С. Виготського, теорії комунікативної дії Ю. Габермаса, теорії дискурсу Т.А. Ван Дейка, концепції значення мови для логічної побудови науки Р. Карнапа, теорії мовних актів та перформативності тексту Дж. Сьорла та Д. Остіна, теорії репрезентації дійсності В.В. Жовтянської, підходи Л.В. Засєкіної, В.В. Зірки, Л.О.Калмикової, Н.В. Чепелевої та ін.

У дослідженні перформативного потенціалу мовної гри в публічному дискурсі явище і феномен мовної гри виступає засобом інформаційних впливів у просторі публічного дискурсу. Пропонується концептуальною основою мовної гри обрати класичне узмістовлення цієї дефініції, що визначається у роботах Л. Вітгенштайна, Дж. Сьорла, Д. Остіна та Ю. Габермаса. Зміст наукового конструкту "публічний дискурс" пропонується сприймати через оптику підходів Т.А. Ван Дейка, Л.В. Засєкіної, Л.О.Калмикової, Н.В. Чепелєвої, В.В. Жовтянської та ін.

Основою для аналізу перформативного потенціалу мовної гри у публічному дискурсі нами обрано наукові підходи відомих дослідників у галузі психолінгвістики. Зокрема Т.А. Ван Дейк акцентує на необхідності розрізнення понять дискурс і текст, оскільки дискурс має відношення до актуальної мовної дії, тоді як текст стосується системи мови або формальних лінгвістичних знань [6]. За висновками Т. А. Ван Дейка дискурс – це комунікативна подія, що відбувається між промовцями, слухачами (спостерігачами та ін.) в процесі комунікативної дії в певному хроністичному, просторовому та іншому контексті. Дискурс може відбуватися як мовна, письмова комунікативна дія, може мати вербальні і невербальні складові [6]. Таке визначення сприймається особливо важливим, оскільки не обмежує дискурс рамками конкретного мовного висловлювання, але враховує особистісні і соціальні характеристики своїх суб'єктів і безліч інших аспектів актуальної мовної ситуації. Л.В. Засєкіна розвиває дискурсивну парадигму Т. А. Ван Дейка зауважуючи, що дискурсом вважається мовленнєва діяльність суб'єктів, комунікативний процес і продукт мовленнєвої діяльності індивідів. Дискурс - це "мовлення, занурене в життя", яке включає, окрім тексту, екстралінгвістичні параметри, необхідні для його розуміння, і соціальний контекст, що містить інформацію про учасників комунікації та їхні характеристики [1; 2].

Сутність і зміст публічного дискурсу виходять із логіки Т.А. Ван Дейка щодо особливостей політичного та інших інституціональних, тобто залежних від соціальних інститутів, типів дискурсу. Тому доцільно сприймати публічний дискурс як дискурс публічної політики, деліберативний осередок усіх актуальних для певної спільноти (multi-stakeholder processes (MSP) [5]) дискурсів (політичних, наукових, освітніх, релігійних, публіцистичних, журналістських, художніх, маргинальних тощо).

Перформативні можливості мовної гри як засобу маніпулятивного впливу на свідомість людини нами розкрито у попередніх дослідженнях [3; 4]. Зокрема було обгрунтовано, що психологічні та психолінгвістичні властивості соціальної комунікації спроможні бути джерелами індоктринації у семантичне ціннісне поле адресата певних смислів, а також збурень у нього потрібних адресанту психоемоційних станів. Це відбувається завдяки психологічним законам незавершеної дії, зв'язку пам'яті з емоціями та мотивацією, закону краю, ефектів емоційного посилення уваги, феноменам натуралістичної омани та самовпевненості, ефекту Барнума. Структура відповідної авторської концепції включає психологічну та семантико-синтаксичну диференціацію п'яти класів лексем відповідно до їх перформативно-критеріальних характеристик [3; 4].

Виходячи із наведеного пропонується в контексті перформативних, маніпулятивних можливостей, сприймати мовної гру як ефективний засіб організації та здійснення публічного дискурсу. Зважаючи на те, що у публічному просторі можливі як позитивні, так і негативні наслідки використання закономірностей мовної гри, вважається за доцільне проведення дослідження передусім інформаційно-психологічних ризиків використання мовної гри як засобу публічного дискурсу.

Список використаних джерел:

1. Засєкіна Л.В., Засєкін С.В. Вступ до психолінгвістики. Навчальний посібник. - Острог: Видавництво Національного університету "Острозька академія", 2002. - 168 с.
2. Засєкіна Л. В. Мова як когнітивно-дискурсивна психомеханіка свідомості. *Психологічні перспективи.* № 23 (2014), видання Волинського національного університету ім. Л. Українки, – с. 112-126.
3. Хайрулін О.М. Психологічні аспекти мовної гри як засобу впливу на свідомість людини. *Психологічні перспективи.* №37 (2021), видання Волинського національного університету ім. Л. Українки, – с. 256-269.
4. Хайрулін О.М. Інформаційно-психологічна безпека особистості в контексті мовної гри. *Вісник Національного університету оборони України* : збірник наукових праць НУОУ. 2021. №1. С. 107–129.
5. Bettye Pruitt and Philip Thomas. Democratic Dialogue – A Handbook for Practitioners. GS/OAS. Washington, D.C. USA. International IDEA. Stockholm. Sweden. Printed by: Trydells Tryckeri AB, Sweden. - 241 p.
6. Van Dijk, T. Ideology: A Multidisciplinary Approach. – L.: Sage, 1998. -383 p.

Михайло ХАРЛАМОВ, д.іст.н, проф.
ORCID: 0000-0002-5289-0290
E-mail: mike1982kharlamov@gmail.com
Тетяна ВАЩУК
НУЦЗУ
ORCID: 0009-0007-7885-0987
E-mail: 336dnz@gmail.com

СОЦІАЛЬНО-ПСИХОЛОГІЧНА РЕАБІЛІТАЦІЯ ВНУТРІШНЬОПЕРЕМІЩЕНИХ ОСІБ (НА ПРИКЛАДІ ВІЛЬНОНАЙМАНИХ ПРАЦІВНИКІВ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ)

Проблеми соціально-психологічної підтримки та реабілітації осіб, що були переміщені в середині української держави аналізуються в окремих працях авторів – науковців розпочинаючи з 2014 року з моменту анексії Російською Федерацією Автономної Республіки Крим та окупації частини Донецької та Луганської областей. Так О. Чуйко розглядає питання соціальної реабілітації зокрема і внутрішньопереміщених осіб та зазначає що соціальна реабілітація має багатоаспектний характер та включає в себе 3 основні компоненти: доступність середовища, соціальний контекст реабілітаційного процесу (соціальне прийняття, відповідність або адаптація до світогляду та цінностей громади та доступність середовища) і підбір відповідних методів (кризове втручання, соціальний супровід, державні та місцеві програми підтримки), що в сумі дозволить зробити процес системно-структурованою технологією і сферою практики.

З науковцем Чуйко також солідарна і автор Ю. Песоцька, яка аналізує в своїй праці соціальну реабілітацію та соціальну адаптацію внутрішньо переміщених осіб. У роботі Песоцької визначено поняття першої психологічної допомоги, яка є необхідним етапом для подолання посттравматичних стресових розладів та інших розладів, а також є складовою соціально – реабілітаційного процесу. Окрім того описано рекомендації для надання соціальних послуг ВПО, які сприятимуть соціальній реабілітації та соціальній адаптації.

Автор Т. Кузьмич розглядає соціальну адаптацію внутрішньо переміщених сімей з дітьми та зазначає, що результати дослідження стану адаптації внутрішньо переміщених осіб в Україні показали, що першочерговими потребами цієї категорії є: фінансова, гуманітарна, житлова та медична допомога. Усі потреби відповідають економічним потребам уразливої групи. Важливу роль на успішність адаптації відіграє соціальне самопочуття людини в колективі можливість отримання кваліфікованої допомоги та працевлаштування.

Окрім соціальної адаптації сучасні науковці розглядають не менш важливий компонент, а саме психологічну адаптацію. Наприклад Ю. Гундертайло розглядає

питання особливостей психологічної допомоги ВПО у сучасних реаліях та зазначає що вже на етапі планування роботи з психологічної підтримки ВПО слід чітко окреслювати цілі такої діяльності, зосереджуючись на соціально-психологічній інтеграції у місцеву громаду та виявленні й реалізації людського потенціалу ВПО, адже значна частина ВПО залишиться в регіоні на значний проміжок часу або і на завжди. Серед основних напрямків роботи дослідниця виділяє: психологічне опрацювання досвіду, зосередження уваги на підтримці ініціатив жінок та дітей.

В. Соловйова в своїй науковій праці "Пошук шляхів надання спеціалізованої психологічної допомоги дітям ВПО через систему перенаправлення" каже про необхідність у ефективній міжсекторальній та міжвідомчій взаємодії із спеціалістами відповідних служб у забезпеченні повноцінного психологічного і соціального розвитку особистості, та створення алгоритму переправлення до відповідних організацій, які надають спеціалізовані психологічні та психотерапевтичні послуги.

З початку повномасштабного вторгнення Російської Федерації в Україну місто Харків одразу опинилося в епіцентрі бойових дій. Протягом лютого – березня 2022 року частина вільнонайманих працівників Національного університету цивільного захисту України (НУЦЗ України) – профільного закладу вищої освіти Державної служби України з надзвичайних ситуацій виїхали за межі міста Харків з власними родинами, з метою вберегти своє життя та життя своїх родин. Працівників НУЦЗ України можна було поділити на певні категорії: 1. співробітники, що залишалися в Харкові; 2. співробітники, що виїхали з Харкова до відносно безпечних районів Харківської області; 3. працівники, що виїхали за межі Харківської області у відносно безпечні райони інших областей України.

Найбільш складним було становище працівників НУЦЗ України, що залишилися у місті Харків на початку 2022 року. Переважним чином це були люди, які не могли виїхати через необхідність доглядати похилих родичів. Вони не отримували фінансову підтримку держави, як внутрішньо переміщені особо, хоча отримували гуманітарну (продукти харчування, засоби гігієни тощо) та соціально-психологічну допомогу від держави та різноманітних міжнародних та волонтерських організацій.

Працівники НУЦЗ України, що були переміщені у південно-західні райони Харківщини (Валківщина, Красноградщина, Мереф'янщина тощо) переважним чином зупинялися у родичів та знайомих. Вони були оформлені, як внутрішньопереміщені особи (отримували фінансову допомогу від держави), а також отримували різні види допомог (в тому числі і допомогу в соціально-психологічній реабілітації), як від міжнародних організацій, так і від волонтерських організацій, так і від місцевих громад.

Працівники НУЦЗ України, що були переміщені у західні та центральні області України (Львівщина, Тернопільщина, Хмельниччина, Черкащина тощо) також були оформлені, як внутрішньопереміщені особи (отримували фінансову

допомогу від держави), а також отримували різні види допомог (в тому числі і допомогу в соціально-психологічній реабілітації), як від міжнародних організацій, так і від волонтерських організацій, так і від місцевих громад.

Слід зазначити, що переважна більшість працівників НУЦЗ України, що виїхали за межі міста Харків не були сторонніми спостерігачами тієї жахливої ситуації, що коїлася в той час. Вони самі займалися волонтерством (допомагали іншим внутрішньопереміщеним особам, збирали кошти та речі для Збройних Сил України та інших формувань сил безпеки та оборони тощо). Працівники НУЦЗ України самі отримували соціально-психологічну підтримку та реабілітацію, а також як фахівці іноді самі надавали іншим допомогу і підтримку. Слід зазначити, що влітку – восени 2022 року переважна більшість працівників НУЦЗ України повернулися до міста Харків, окрім окремих науково-педагогічних працівників, які переїхали до міста Черкаси для ведення занять для курсантів даного навчального закладу. У Черкасах дані співробітники також отримували і отримують досі соціально-психологічну реабілітацію як внутрішньопереміщені особи.

Список використаних джерел:

1. Гундертайло Ю. Д. Особливості психологічної допомоги впо у сучасних реаліях. Всеукраїнський науково-практичний семінар, м. IX-ті Гротівські читання РАКУРСИ ПСИХОЛОГІЧНОГО БЛАГОПОЛУЧЧЯ ОСОБИСТОСТІ, 9 черв. 2017 р. С. 54–58.
2. Кравченко О.О., Чупіна К.О. Соціально-психологічна реабілітація ВПО: з досвіду Уманського державного педагогічного університету імені Павла Тичини. Соціальна психологія. Юридична психологія. Випуск 41. 2022. С. 251-254. URL: http:/habitus.od.ua/journals/2022/41-2022/44.pdf.
3. Кузьмич Т. Соціальна адаптація внутрішньо переміщених сімей з дітьми. Традиції та нові наукові стратегії у центральній та східній європі. 2020. С. 126–134. URL: https://novaosvita.com/wp-content/ uploads/2020/0.
4. Песоцька Ю. Соціальна реабілітація та соціальна адаптація внутрішньо переміщених осіб. Social Work and Education. 2022. № 9. С. 89–99.
5. Соловйова В. Пошук шляхів надання спеціалізованої психологічної допомоги дітям впо через систему перенаправлення. Головна сторінка eKMAIR. URL: http://ekmair.ukma.edu.ua/bitstream/handle/123456789/13285/Soloviova_Poshukia_shliakhiv_nadannia_spetsializovanoi_psykholohichnoi_ dopomohy.pdf.
6. Чуйко О. Соціальна реабілітація: підходи до змістових характеристик процесу. Актуальні проблеми соціології, психології, педагогіки. 2015. № 4 (29). С. 152–158. URL: http://www.apspp.soc.univ.kiev.ua/index.php/home/article/viewFile/379/292.

Віктор ШИДЛЮХ
НУОУ
ORCID: 0000-0002-3792-3592
E-mail: shydlyukh@ukr.net

РОЛЬ КУЛЬТУРИ ВНУТРІШНІХ КОМУНІКАЦІЙ У ФОРМУВАННІ КУЛЬТУРИ ЛІДЕРСТВА

Конституцією України закріплено стратегічний курс держави на набуття повноправного членства України в Організації Північноатлантичного договору.

Основоположною доктриною НАТО для спільних операцій і діяльності Альянсу є Об'єднана публікація Альянсу AJP-01, яка пояснює стратегічний контекст операцій і зосереджується на основах спільних операцій і діяльності. Вона призначена для того, щоб надати командирам та їхнім штабам спільне розуміння підходів до застосування військового інструменту сили шляхом пояснення основ і принципів, і це саме та основа, з якої випливають всі підпорядковані доктрини НАТО [2].

Згідно з цією Доктриною в НАТО вважають, що збройний конфлікт є змаганням волі людей, тому маневрений підхід до ведення війни зосереджується на подоланні моральної, а не фізичної складової бою. Перевага НАТО в моральній складовій бере витоки з професійної військової культури та моральної легітимності, отриманої завдяки поведінці їх військових сил. Професійна культура складається з культури лідерства, культури ведення війни, моралі та моральної згуртованості. [2].

В цій Доктрині розглядають культуру лідерства як "здатність надихати тих, ким вони керують. Завдяки лідерству командири отримують підтримку тих, ким вони командують. Лідерство має за мету чинити позитивний вплив на підлеглих, задля отримання переваги у складних обставинах бою. Це джерело натхнення, мета та напрям для розвитку та захисту всіх компонентів боєздатності. Під час збройного конфлікту саме лідери руйнують параліч, спричинений людськими помилками, невизначеністю, смертю та руйнуваннями. Їхнє бачення, інтелект, комунікація та безперервна мотивація торують шлях крізь хаос і плутанину. Погане (токсичне) керівництво часто маскується ієрархією командування і має далекосяжні та згубні наслідки. Воно швидко деморалізує та дестабілізує боєздатність. Військовослужбовці мають активно вивчати усі аспекти лідерства, щоб максимізувати свій лідерський потенціал" [2].

Культура – це поліпшення, ушляхетнювання тілесно-душевно-духовних сил і здібностей людини, ступінь їх розвитку, сукупність способів і прийомів організації, реалізації та розвитку людської життєдіяльності, способів людського буття, а також

сукупність матеріальних і духовних надбань на певному історичному рівні розвитку суспільства і людини, які втілені в результатах продуктивної діяльності.

Як ми бачимо, за поглядами фахівців НАТО, комунікація командирів та безперервна мотивація "тих, ким вони командують" (підлеглих) є основою культури лідерства.

Раніше ми дослідили, що категорія "комунікація" походить від латинського слова "communico" (повідомлення, зв'язок, спілкування) і в широкому сенсі означає термін, що окреслює людську взаємодію у світі. Під терміном "внутрішня комунікація" ми розуміємо внутрішню організаційну взаємодію між суб'єктами Збройних Сил України. Ми також визначили, що поняття "культура внутрішніх комунікацій" офіцерів Збройних Сил України – це поліпшення, ушляхетнювання тілесно-душевно-духовних сил, схильностей і здібностей офіцерів до внутрішньої організаційної взаємодії, ступінь їх розвитку, сукупність способів і прийомів діяльності Збройних Сил України, реалізації та поступу офіцерської життєдіяльності, способів офіцерського буття, а також сукупність матеріальних і духовних надбань на певному історичному рівні розвитку суспільства, Збройних Сил України і самих офіцерів, які втілені в результатах їхньої продуктивної діяльності [3].

Досвід ведення сучасних операцій ще раз підтвердив, що першочергова увагу має зосереджуватись на подоланні моральної, а не фізичної складової збройної боротьби.

Перевага України в моральній складовій здобувається професійною військовою культурою та моральною легітимністю, отриманою завдяки законності і справедливості поведінки її Збройних Сил.

Професійна військова культура є одним з найважливіших елементів української національної культури як результат багатовікових традицій слави українського вояцтва. Оскільки Конституцією України закріплено стратегічний курс держави на набуття повноправного членства України в Організації Північноатлантичного договору, сучасна професійна військова культура має бути заснована на ліберально-демократичних цінностях однієї з держав-членів НАТО в майбутньому.

Професійна культура складається з культури лідерства, культури ведення війни, моралі та моральної згуртованості [2].

Актуальність формування і розвитку військового лідерства обумовлена нагальною потребою у здатності військових лідерів вести за собою в бою (операції), а також лідирувати у впровадженні якісних змін на шляху розвитку професійної культури військовослужбовців та досконалості Збройних Сил України в цілому.

Саме завдяки лідерству командири отримують підтримку тих, ким вони командують. Лідерство має за мету чинити позитивний вплив на підлеглих, задля отримання переваги у складних обставинах бою (операції) та розвитку Збройних

Сил. Це джерело натхнення, мета та напрям для розвитку та захисту всіх компонентів боєздатності.

Під час збройного конфлікту саме лідери руйнують параліч, спричинений людськими помилками, невизначеністю, смертю та руйнуваннями. Їхнє бачення, інтелект, комунікація та безперервна мотивація торують шлях крізь хаос і плутанину.

Лідерство не має звань і рангів та не є просто військовим завданням. Лідерство не обмежується лише командною ланкою, особами зі званням і посадою чи військовослужбовцями. Лідерство слід розглядати як систему лідерів. Збройні Сили лише тоді виконуватимуть свою місію добре, коли лідерство на всіх рівнях досягне відповідного рівня ефективності.

Системний підхід розглядає всіх військовослужбовців потенційними лідерами і те, як вони взаємодіють вертикально і горизонтально обумовлює їх ієрархію, де вони одночасно можуть функціонувати як лідери, послідовники та однодумці. До такого ж висновку прийшли і в [2].

В Збройних Силах завжди існує ризик того, що окремі керівники, зіткнувшись зі складністю операційного середовища або токсичною (контрпродуктивною) поведінкою старших начальників або улесливою поведінкою підлеглих, можуть проявити слабкість і обрати токсичний стиль керівництва. Тому військовослужбовці мають активно вивчати усі аспекти лідерства, щоб мінімізувати такі ризики і максимізувати свій лідерський потенціал.

У міру того, як військова справа об’єднує можливості для роботи в усіх операційних сферах, застосування сил ставатиме все більш комплексним. Кожен може мотивувати оточуючих ініціативою, прикладом і сміливістю. Досвід бойових дій показав, що існує критична потреба в лідерстві усіх рівнів від найвищого до найнижчого.

Лідерство в середовищі конкуренції. В сучасних операціях (бойових діях) здатність впливати на персонал і аудиторії та отримувати перевагу над противником буде ставати все більш складним та більш змагальним завданням. Здатність лідерів пристосовуватися до мінливих операційних умов, випереджаючи противника у потужності власних команд буде основоположною для перемоги в конкурентній боротьбі.

Ми погоджуємося з [2], що лідерство як “добре” військове керівництво, загалом можна розглядати у двох значеннях: добре у сенсі ефективності у виконання місії і добре в моральному сенсі. Моральний сенс, на нашу думку, забезпечується внутрішніми комунікаціями, підтриманням командного духу та етичністю поведінки з підлеглими.

Звичним є вважати, що хорошим лідером є той, хто зараз виконав завдання. Але, на наше переконання, такі фактори як зростаюча різноманітність мобілізованого персоналу та мінливість операційного середовища, призвели до

того, що саме моральні аспекти внутрішніх комунікацій стають усе більш важливим фактором, який дозволяє лідерам отримати моральну згуртованість команди, командний дух, необхідні для виконання місії у найскладніших обставинах не лише зараз, а і в майбутньому.

За результатами емпіричних досліджень, детальніше описаних в [4-6], ми дійшли висновку, що формування та розвиток культури внутрішніх комунікацій вимагає нової системи мислення (mindset) командирів – потенційних лідерів.

Під системою мислення (mindset) (від англ. система мислення, ментальність, свідомість, менталітет, установка) ми розуміємо сукупність соціально-психологічних настанов, загальну духовну налаштованість, установку до навколишнього світу [3].

Без нової системи мислення, генерали, офіцери та сержанти швидко опиняються в полоні радянських стереотипів авторитарних методів роботи з підлеглими, які коротко можна описати принципом “я начальник – ти ніхто”. Зміна такого стану потребує комплексного і системного методичного підходу щодо формування (розвитку) системи мислення командирів, як основи культури внутрішніх комунікацій.

Велика кількість проведених занять (тренінгів) з генералами, офіцерами і сержантами за розробленими (адаптованими) нами методиками внутрішніх комунікацій: “Командирське (бойове) інформування”; “Аналіз проведених дій”; “Пріоритет заохочень (схвалення)” тощо підтвердили високу ефективність методик у формуванні (розвитку) культури внутрішніх комунікацій і, відповідно, культури лідерства командирів.

Отже, проведене нами дослідження окреслило роль культури внутрішніх комунікацій у формуванні культури лідерства. Дослідження підтвердило, що наші погляди, сформовані ще в попередні роки [3-6], щодо формування (розвитку) культури лідерства та внутрішніх комунікацій значною мірою співпали з сучасними поглядами фахівців НАТО [2], мають прикладний характер, доповнюють і розвивають теорії лідерства та внутрішніх комунікацій. Збагачують та підтверджують ці теорії реальним бойовим досвідом і потребують подальшої імплементації в освітній процес професійної підготовки генералів, офіцерів і сержантів.

Список використаних джерел:

1. Конституція України : Закон від 28.06.1996. № 254к/96-ВР // База даних “Законодавство України” / ВР України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 26.09.2023).

2. AJP-01 Allied Joint Publication-01 Allied Joint Doctrine, Edition F, Version 1, dated December 2022 (Об’єднана Союзна Публікація -01, Об’єднана Союзна Доктрина). NATO. С. 57-60.

3. Шидлюх В.В. Засади формування культури внутрішніх комунікацій. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи* : ІІ міжнар. наук.-практ. конф., 1 жовт. 2021 р. : тези доповідей / Міністерство оборони України, НУОУ. – К. : НУОУ, 2021. С. 93-94.

4. Шидлюх В.В. Internal communications lessons learned. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи* : І міжнар. наук.-практ. конф., 1 жовт. 2020 р. : тези доповідей / Міністерство оборони України, НУОУ. – К. : НУОУ, 2020. – С. 34-35.

5. Шидлюх В.В. Результати апробації методики формування культури внутрішніх комунікацій в процесі професійної підготовки офіцерів оперативно-тактичного рівня. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи* : ІІІ міжнар. наук.-практ. конф., 31 жовт. 2022 р.: тези доповідей / Міністерство оборони України, НУОУ. – К.: НУОУ, 2022. С. 162-163.

6. Семененко В. М., Іващенко А. М., Шидлюх В. В. Організація внутрішніх комунікацій у штабах і підрозділах Збройних Сил України під час виконання завдань в районі операції Об’єднаних сил. Зб. наук. праць Центру воєнно-стратегічних досліджень НУОУ. – 2020. – № 1(68). С. 6-12.

Pavlo KORCHAGIN, graduate student,
National University of Civil Defense of Ukraine
ORCID: 0009-0004-4126-1781
E-mail: feirmen3@gmail.com
Roman SHEVCHENKO, Doctor of Technical Sciences, Professor
National University of Civil Defense of Ukraine
E mail: shevchenko605@i.ua
ORCID: 0000-0001-9634-6943

INCREASING THE EFFICIENCY OF THE SYSTEM OF TRAINING SPECIALISTS IN THE OPERATION OF EMERGENCY AND RESCUE EQUIPMENT

During the hostilities, the system of training specialists of the DSNS system faced a number of challenges that significantly affected the quality of knowledge and skills that graduates of higher education institutions receive. If the problem of the issue is considered only in the part of the training of specialists in the operation of emergency and rescue equipment, then the following should be noted. A stable structural and logical scheme of the process of coordinating and increasing the efficiency of the system of training specialists in the operation of emergency and rescue equipment provides for the presence of a mandatory procedure for the coordination of operational and technical parameters of emergency and rescue equipment and the methodology of training specialists in its operation.

The latter has a number of direct and reverse relations, which are aimed at improving the quality of the capabilities of the emergency prevention and response system, primarily at the regional level, and provides a planned basis for the application of procedures for saturating the prevention system with new and modernized models of equipment, as well as a planned procedure for training specialists, which is constantly revised taking into account time and thematic limitations. Under today's conditions, the above coordination procedure is excluded from the process of distribution of emergency rescue equipment that comes in the form of humanitarian aid from partner countries. Humanitarian demining equipment and special dual-purpose equipment also remain outside its scope.

The results of the study of the problems of the process of coordinating the processes of equipping emergency and rescue equipment and training specialists in its operation made it possible to form a structural and logical scheme for the construction of the appropriate methodology [1].

The latter allows you to use it both for directly forming methods that differ by level of purpose (local, regional, state) and to take into account the territorial features of the region in terms of the organization and nomenclature of emergency rescue equipment.

On the other hand, the formed structural and logical scheme allows taking into account different forms of training of specialists in the operation of emergency and rescue equipment, both by the form of training (off-line, online, etc.) and by the level of training (bachelor's degree, master's degree, etc.).

Accordingly, the mathematical modeling procedure is based on the innovative approaches outlined in [2], regarding the consideration of the importance of the consequences of the 1st priority level in the formation of the connection equation and, accordingly, the influence of the consequences of the 2nd and 3rd priority levels in the formation of the boundary conditions of the mathematical model . The initial conditions are formed by the system of monitoring dangerous factors of emergency situations.

The forecasting procedure, which has a retrospective nature, is used to obtain a field of dangerous factors and further mathematical modeling based on them.

The application of a separate procedure for assessing the quality and completeness of the consistency of operational and technical parameters will allow placing the equipment that comes under the partnership program, taking into account not only the needs of the regions, but also the capabilities of educational institutions, regarding the training of specialists in its operation

The latter have significant limitations both in terms of time and teachers (organization of the process of continuous education and improvement of their qualifications). The existing contradiction between the constant increase in the nomenclature of fire and emergency rescue equipment and the impossibility of unifying the process of its study during the training of specialists and the limitation of time for training will be resolved at the expense of a clear methodology for the training of specialists, which will allow to build and further coordinate effective interaction of the complex process of preventing emergency situations and fires in the triangle "Emergencies of Emergency Situations - territorial units - educational institutions".

Thus, a structural and logical scheme of the methodology for increasing the effectiveness of the emergency prevention process in the conditions of uncertainty of the parameters of the training of specialists and the operation of emergency rescue equipment has been formed, which consists of 6 procedures, the application of which is limited to the field of regional conditions for the use of emergency rescue equipment and is related to with direct and feedback links, which in the end allows to further unify the process of training specialists taking into account experience and NATO standards.

References:

1. Korchagin Pavlo, Khmyrov Ihor, Shevchenko Roman Determination of the problems of the process of liquidation of emergency situations in the conditions of

uncertainty of the system of training specialists in the operation of emergency and rescue equipment // The 30th International scientific and practical conference “Trends and modern methods of improving scientific ideas”, Melbourne, Australia. International Science Group. 2023. P.110-112.

2. Дівізінюк М.М. Теоретичні засади парадигми “Цивільний захист”: монографія / Дівізінюк М.М., Єременко С.А., Лєвтєров О.А., Пруський А.В., Стрілець В.В., Стрілець В.М., Шевченко Р.І.; під заг. редакцією М.М. Дівізінюка та Р.І. Шевченка. Київ: ТОВ “АЗИМУТ-ПРІНТ”. 2022. 335 с.

Вадим БОГАЙЧУК, к. політ. н., доцент,
доцент кафедри соціальної комунікації
та публічної дипломатії інституту
стратегічних комунікації НУОУ
ORCID:0000-0003-4977-5870
E-mail: vadimb1964@gmail.com

ПОНЯТТЯ ДЕМОКРАТИЧНОГО ЦИВІЛЬНОГО КОНТРОЛУ В ЗС УКРАНИ В РЕАЛІЯХ СЬОГОДЕННЯ

Минув рік цієї війни. Зараз, як ніколи, наш курс на євроатлантичну інтеграцію – беззаперечний та безальтернативний.

Вступаючи до ЄС, до НАТО, ми беремо на себе зобов'язання дотримуватися принципів, норм і правил, які існують в цих організаціях, і існують з добрих причин, перевірених часом.

Демократичний цивільний контроль – один з підходів до сектору безпеки та оборони, який передбачає, що відповідальність за прийняття стратегічних рішень у військовій сфері лежить на демократично обраній політичній владі та громадянському суспільстві, а не на військовому командуванні.

У розвинутому демократичному суспільстві процес демократичного цивільного контролю над збройними силами здійснюється у різних формах і за допомогою розгалуженого комплексу способів, що стоять на перешкоді небезпечних для суспільства або антидержавних військових дій.

Система демократичного контролю також виступає дієвим механізмом розподілу відповідальності між політиками та військовими. У випадку, коли військові ідентифікували загрози та коректно оцінили об’єм витрат для їх стримування, а політики не мають можливості профінансувати передбачені оборонні заходи, то вони повинні нести відповідальність за невиконання своєї частини зобов’язань. З іншого боку, цей приклад демонструє підвищення рівня відповідальності військових у тому випадку, коли певні загрози не були

ідентифіковані, а тому не було вжито відповідних заходів або бюджет не містив обґрунтованих розрахунків.

Поняття демократичного цивільного контролю над збройними силами об'єднує одразу декілька процесів:

- контроль цивільного суспільства над прийняттям військових рішень
- парламентський контроль над оборонною політикою
- судовий контроль над дотриманням закону у військовій галузі
- цивільний контроль з боку недержавних організацій, незалежних змі, профспілок

У правовій державі демократичний цивільний контроль є своєрідним регулятором військово-цивільних відносин, коли основні принципи демократичного суспільства посідають провідне місце стосовно принципів військової справи. Як орган держави, армія повинна проводити і захищати політику саме держави, а не окремих політичних партій чи об'єднань.

Основними передумовами до впровадження дієвих механізмів демократичного контролю є прозорість оборонного сектору та підзвітність безпекових інститутів народу, який він захищає.

Моделі демократичного контролю можуть відрізнятись, однак їхній керівний принцип залишається незмінним у всіх країнах – політичні і військові лідери мають нести спільну відповідальність за національний сектор безпеки та оборони.

Ефективні підходи до здійснення контролю над сектором безпеки не виникли раптово. Вони являють собою досвід, накопичений за більше, ніж 150 років намагань створити і вдосконалити демократичне управління мечем та щитом держави.

Кращі практики демократичного контролю базуються на чотирьох основних принципах управління сектором безпеки загалом і у частині ролі парламенту зокрема, а саме:

- системі стримувань і противаг державних інституцій за контролюючої ролі парламенту.
- прозорості, без якої демократичні дебати не видаються можливими.
- комунікації представників сектору безпеки з суспільством через його законно обраних представників або інших представників громадянського суспільства.
- підзвітності, яка передбачає, що парламент та інші контролюючі суб'єкти здатні ефективно виконувати свою роль через своєчасне надання достатньої інформації та надання необхідних повноважень суб'єктам нагляду.

Сьогодні, на жаль, ситуація з демократичним контролем над ЗСУ вже привернула увагу наших найближчих союзників, і це не та увага, яка нам потрібна. Питання посилення демократичного контролю збройних сил знаходиться в переліку пріоритетних реформ для міністерства оборони України.

Довгостроковій перспективі демократичний цивільний контроль це не лише засіб протидії ризикам військових неправомірних дій, але й інструмент розвитку та вдосконалення Збройних сил. Посилення контролю в Україні з 2018 року, на наш погляд, є однією з причин кращої організації, підготовки і боєготовності та управління в ЗСУ, попри всі недоліки та виклики.

Беручи до уваги, що курс на ЄС і НАТО закріплений у нашій Конституції, конституційно випливає, що принципи та цінності членів НАТО в цьому питанні потрібно сприймати серйозно.

Крім того, в Кодексі поведінки ОБСЄ щодо військово-політичних аспектів безпеки, прийнятому всіма членами, зазначено, що:

- держави-учасниці вважають демократичний політичний контроль над військовими, воєнізованими та внутрішніми силами безпеки, а також розвідувальними службами та поліцією невіддільним елементом стабільності та безпеки. вони сприятимуть інтеграції своїх збройних сил із громадянським суспільством як важливого прояву демократії.

- кожна держава-учасниця завжди забезпечуватиме та підтримуватиме ефективне керівництво та контроль над своїми військовими, воєнізованими силами та силами безпеки конституційно встановленими органами влади, наділеними демократичною легітимністю. кожна держава-учасниця забезпечить контроль для забезпечення виконання такими органами своїх конституційних і правових обов'язків.

Досвід впровадження західними країнами демократичного цивільного контролю переконливо свідчить про його користь як для військових, так і для цивільних.

Для керівництва держави – це можливість забезпечити стабільний розвиток країни та гарантувати захист національних інтересів за допомогою ефективних силових структур.

Для суспільства – це запорука доцільного використання бюджетних коштів, спокій у повсякденному житті та гарантія дотримання прав людини як в армії, так і в суспільстві загалом.

Для воєнної організації – це чітке визначення стратегічного курсу, функцій і завдань, а також ефективний механізм забезпечення військових потреб та соціального захисту військовослужбовців.

Список використаних джерел

1. Конституція України (Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141) Із змінами, внесеними згідно із Законами – Режим доступу: http://web.znu.edu.ua/psychologicalservice//docs/normatyvni_dokumenty/konstitutsiya-ukrayini.pdf

2. Закон України Про національну безпеку України (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241) – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469–19

3. Демократичний цивільний контроль над сектором безпеки і оборони: теорія і практика : навчальний посібник / В. А. Ященко, В. Г. Пилипчук, П. П. Богуцький, О. Д. Довгань, І. М. Доронін, О. В. Петришин; за заг. ред. В. Г. Пилипчука; Науково-дослідний інститут інформатики і права НАПрН України. – Київ; Одеса : Фенікс, 2020. – 224 с.

4 . Кодекс поведінки стосовно військово-політичних аспектів безпеки ОБСЄ (1994 р.). – Джерело: сайт ОБСЄ – Режим доступу: https://www.osce.org/uk/node/253046?download=true}ОБСЄ

5. Коул И., Флури Ф., Ланн С. “Контроль и руководство: парламенты и управление в секторе безопасности.” – Женева, Швейцария /Редакторский коллектив Иден Коул, Филипп Флури и Саймон Ланн, Координатор проекта: Валентин Бадрак.- «Издательский дом «АДЕФ-Украина», 2015. – 132 с.

Геннадій ЄФІМОВ, к.н. з д.у., с.н.с.
Сергій ПОСТУПАЛЬСЬКИЙ
Володимир БЄЛЯКОВ
НАСВ ім. гетьмана Петра Сагайдачного
ORCID: 0000-0003 -3289-8292
E-mail: genefimov59@gmail.com

ВІЙСЬКОВО – ЦИВІЛЬНЕ СПІВРОБІТНИЦТВО В СИСТЕМІ ТЕРИТОРІАЛЬНОЇ ОБОРОНИ ДЕРЖАВИ

Визнання цивільно-військового співробітництва (ЦВС) важливим елементом підтримки та забезпечення ведення бойових дій - стало практикою провідних країн світу [1]. Разом з тим, успішний досвід українських військовослужбовців, задіяних у міжнародних миротворчих операціях (до початку агресії російської федерації проти України), не став поштовхом для створення структур ЦВС. У зв’язку з цим, необхідно звернути увагу на деякі особливості, які притаманні цьому процесу.

До початку проведення Антитерористичної операції (АТО) в окремих районах Донецької та Луганської областей це питання не було вирішено. Блокування пересування військових колон, перешкоджання виконанню завдань військовим формуванням, передача розвідувальної інформації протиборчій стороні, відволікання підрозділів військових формувань до виконання не властивих їм завдань - це лише деякі видимі наслідки відсутності ЦВС. Як наслідок, ряд службово-бойових завдань підрозділами не були виконані, що призвело до незворотних людських втрат.

Зазначене вимагало нагальну необхідність унормування відповідних відносин між військовими та цивільними гілками управління, для чого і був розроблений та прийнятий в лютому 2015 року Закон України “Про військово-цивільні адміністрації”, який визначав організацію, повноваження і порядок діяльності військово-цивільних адміністрацій, що утворювалися як тимчасовий вимушений захід з елементами військової організації управління [2].

Одночасно слід звернути увагу на той факт, що цивільно-військове співробітництво та військово-цивільна взаємодія достатньо суттєво різняться в сутності понятійного апарату. На відміну від цивільно-військового співробітництва, військово-цивільна взаємодія передбачає, як правило, одночасне спільне виконання різнопланових завдань різновідомчими військовими та цивільними структурами (формуваннями), чітко регламентованими за часом, місцем та способами дій, що в свою чергу притаманно виконанню заходів територіальної оборони.

Особливості участі підрозділів Збройних Сил (ЗС) України, Національної гвардії (НГ) України, Міністерства внутрішніх справ (МВС), Служби безпеки України, Державної прикордонної служби (ДПС) України в АТО, інших бойових і спеціальних діях на Півдні та Сході України, окреслили суттєві проблеми в організації взаємодії між командирами підрозділів військових формувань та місцевими органами самоврядування й населенням у районах виконання завдань.

З метою подолання зазначених недоліків Міністерство оборони України у травні 2014 року направило в райони виконання завдань оперативні групи взаємодії з питань ЦВС. Постало нагальне питання щодо налагодження цивільно-військової взаємодії усіх військових та правоохоронних формувань у зоні конфлікту.

Разом з цим, зазначене питання не стало чимось особливо новим. Ці питання неодноразово піднімалися при проведенні чисельних навчань та тренувань з територіальної оборони (ТрО). Але хибний, на наш погляд, в той час висновок про те, що окремі заходи ТрО не виконуються в смугах ведення бойових дій, офіційно не визначеної ролі і місця штабів ТрО, як робочого органу створених військово-цивільних адміністрацій в окремих районах Донецької та Луганської областей, призвели до зазначених вище наслідків.

Специфіка роботи груп ЦВС сьогодні – дії на території своєї держави. Це вимагає обов’язкового врахування мовного, ментального, релігійного аспекту, пошуку напрямів впливу на місцеве населення в районі проведення бойових дій.

При цьому, слід підкреслити що здійснення регламентованих заходів ЦВС [3-5] є вагомою, але лише певною частиною широкого комплексу воєнних і спеціальних заходів територіальної оборони [6], які повинні спільно виконуватися органами державної влади (місцевого самоврядування) та військового командування. В свою чергу заходи ТрО є складовою частиною організації національного спротиву, мета якого полягає у підвищенні обороноздатності держави, наданні оборони України всеохоплюючого характеру, сприянню готовності громадян до національного спротиву [6].

Вважаємо, що робота груп ЦВС значно виходить за межі задекларованої, а фактично є і повинна бути складовою частиною заходів ТрО, що здійснюються у мирний час та в особливий період з метою протидії воєнним загрозам, а також для надання допомоги у захисті територій, навколишнього природного середовища та майна від надзвичайних ситуацій.

При цьому слід враховувати що ТрО включає в себе військову, військово-цивільну та цивільну складові, діяльність яких здійснюються на всій території України, включно з районами ведення воєнних (бойових) дій [6].

З початком повномасштабного збройного вторгнення російської федерації з введенням правового режиму воєнного стану, Указом Президента України для здійснення керівництва у сфері забезпечення оборони, громадської безпеки і порядку на всій території України були утворені військові адміністрації на базі існуючих обласних (районних) державних адміністрацій [7], головами яких в особливий період – стали Головами Рад оборони областей, що здійснюють керівництво організацією та веденням ТрО на території областей через штаби зон (районів) ТрО, які разом з добровольчими формуваннями територіальних громад складають військово-цивільну складову ТрО [6]. В свою чергу, штаби зон (районів) ТрО у мирний час та особливий період призначені для підготовки до територіальної оборони та її ведення, координації здійснення заходів територіальної оборони силами та засобами СБтаСО держави [8]. Відповідно, на наш погляд, представники структур ЦВС військових частин (формувань) що розташовані в адміністративних районах повинні входити до складу штабів районів ТрО, а представники структур ЦВС вищого рівня – в штаби зон (областей) ТрО (без постійної присутності), що буде сприяти біль ефективній взаємодії.

Таким чином, заходи організації національного спротиву, територіальної оборони, цивільно-військового співробітництва взаємопов’язані та повинні бути невід’ємними складовими єдиної системи забезпечення обороноздатності держави. Саме це забезпечує ефективне здійснення заходів військово-цивільної взаємодії під час відбиття збройної агресії російської федерації.

Збройна агресія російської федерації проти нашої держави наочно продемонструвала необхідність постійного моніторингу цивільного середовища, всебічного вивчення і прогнозування впливу громадянського суспільства на дії складових СБтаСО, подальшого удосконалення законодавчої та нормативно-правової бази.

Список використаних джерел:

1. AJP-09 NATO CIVIL-MILITARY CO-OPERATION (CIMIC) DOCTRINE, червень 2003 [Електронний ресурс]. - Режим доступу: https://www.nato.int/ims/docu/aqp/-9.pdf.

2. Про військово-цивільні адміністрації: Закон України від 03.02. 2015 №141-VIII зі змінами від 18.01.2018 № 2268-VIII. [Електронний ресурс]. - Режим доступу: https://www.zakon.rada.dov.ua./lavas/shov/141-19#Text.

3. Тимчасова настанова з цивільно-військового співробітництва у ході підготовки та застосування Збройних Сил України: затв. наказом наказом Генерального штабу Збройних Сил України від 06.04.2019 №140 [Електронний ресурс]. - Режим доступу: https://www.dy.nayka.com.ua.?op=1&z=1459.

4. Доктрина "Цивільно-військове співробітництво" ВКП9-00(01).01: затв. наказом Головнокомандувача Збройних Сил України від 02.07.2020 № 15860 [Електронний ресурс]. - Режим доступу: https://www.shrotyvg7com.ua/wp-contenent/uploads/2022/03/СП-9-0001.01.

5. Методичний посібник для військ (сил) з питань цивільно-військового співробітництва: Київ, 2019. с.17. [Електронний ресурс]. - Режим доступу: https://www.dovidnykmpz.info/social/metodychnyy-posibnyk-dlia-viys-k-syl-z-pytan-tsyvil-no-viys-kovoho-spivrobitnytstva-2019-r/.

6. Про основи національного спротиву: Закон України від 16.07.2015

№ 1702-IX зі змінами. [Електронний ресурс]. - Режим доступу: https://www.zakon.rada.dov.ua./lavas/shov/1702-20#Text.

7. Про утворення військових адміністрацій: Указ Президента України від 24.02. 2022 №68/2022 [Електронний ресурс]. - Режим доступу: https://www.president.qov.ua/dokyments/682022-41405.

8. Про затвердження Типового положення про штаб зони (району) територіальної оборони: Постанова кабінету міністрів України від 29 грудня 2021 р. № 1442 Київ. [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/1442-2021-%D0%BF#Text.

Олег ІВАХІВ, к.політ.н.
Ігор РИНСЬКИЙ
Любов НІКОЛАЄВА
НАСВ ім. гетьмана Петра Сагайдачного
ORCID: 0000-0001-5932-5959
E-mail: osiva hiv@gmail.com

ЦИВІЛЬНО-ВІЙСЬКОВЕ СПІВРОБІТНИЦТВО НАТО: КОНЦЕПТУАЛЬНІ ЗАСАДИ

CIVIL-MILITARY COOPERATION – CIMIC (цивільно-військове співробітництво (ЦВС) в країнах членах Північно-атлантичного альянсу (НАТО) – це перш за все взаємовідносини між командуванням об'єднаних

збройних сил (ОЗС) та цивільними структурами задля забезпечення виконання поставлених завдань [1, 2, 3].

Ідея CIMIC реалізується лише за умов:

комплексного підходу до протидії існуючим загрозам;

координації зусиль військових та цивільних складових миротворчого процесу;

розширення контактів всіх задіяних антикризових інструментів НАТО з іншими зацікавленими структурами;

орієнтованості на використання невійськових суб'єктів для сприяння коаліційним збройним силам у вирішенні поставлених завдань;

надання (за потреби) силової підтримки цивільним учасникам врегулювання криз.

Система ЦВС НАТО включає:

органи управління;

спеціалізовані структури для виконання штатних функцій;

військові підрозділи для підтримки формувань ЦВС;

громадські організації, приватні компанії, що задіяні до забезпечення дій коаліції.

Розподіл повноважень (функцій):

координація відносин між НАТО та цивільними утвореннями – Військовий комітет НАТО та Комітет з планування на випадок надзвичайних ситуацій;

загальне управління механізмами CIMIC – Командування операціями НАТО;

безпосереднє керівництвом виконанням завдань ЦВС – оперативні органи штабів (групи планування, координації, експертна):

в міжвидовому штабі угруповання ОЗС НАТО – секція координації співпраці військових і цивільних формувань в зоні конфлікту та реалізації приватними компаніями заходів забезпечення миротворчого контингенту;

в штабах бригад і вище – відділення/секції ЦВС;

в оперативних, оперативно-тактичних командуваннях – радники/консультанти з питань культури, права, зав'язків з громадськістю;

в частинах (підрозділах) – командири здійснюють безпосередню реалізацію заходів ЦВС.

Основні принципи планування і організації спільної діяльності:

володіння оперативною обстановкою;

узгодження цілей і завдань між учасниками;

дотримання чинного законодавства;

повага і довіра між всіма учасниками;

пріоритетність цивільних повноважень;

комплексне планування;

ефективний оперативний обмін інформацією.

Основні етапи операції, на яких проводяться заходи ЦВС:

планування та підготовки (перед початком операції): збір інформації про ситуацію в районі розгортання, вибір цивільних партнерів, визначення механізмів співпраці, накопичення і поширення інформації;

проведення (безпосередньо під час операції): накопичення, обробка, надання інформації про поточну обстановку; виявлення критичних чинників, оцінка можливого впливу оперативної обстановки на місцеві настрої; створення сприятливих умов для дій ОЗС; забезпечення належного ресурсовикористання; ІПСО (інформаційно-психологічні операції); визначення об'єктів критичної інфраструктури противника та наслідків їх знищення; налагодження та підтримання відносин з міжнародними та неурядовими організаціями; гуманітарна допомога; контроль за дотриманням місцевих традицій; встановлення відносин довіри;

передачі повноважень (постконфліктний період): організація тимчасового управління; забезпечення процесу політичного врегулювання; створення умов для передачі повноважень; надання допомоги постраждалим та у відновленні об'єктів критичної інфраструктури; налагодження діяльності регіональних органів управління; реформування національної системи безпеки; реалізація соціальних програм.

Головна форма ЦВС при вирішенні завдань щодо забезпечення бойових дій ОЗС – аутсорсінг.

Основні шляхи удосконалення діяльності органів ЦВС:

впровадження багаторівневої системи диференційованого навчання (перепідготовки);

розширення практичного відпрацювання питань спільної діяльності військових і цивільних організмів (поєднання індивідуальних та колективних форм навчання з навчально-бойовими заходами).

Кваліфікаційні вимоги для співробітників органів ЦВС:

володіння англійською мовою;

фахова комунікація;

володіння інформаційними технологіями;

дипломатичність та відкритість;

висока компетенція в питаннях культури та гендеру;

взаємодія зі ЗМІ;

виклик довіри та прихильності до себе;

лідерські якості;

вміння взаємодіяти з оточуючими та командою;

гнучкість та логічність мислення;

орієнтування в складній обстановці;

високі фізичні та розумові здібності;

дотримання установлених норм поведінки;

впевненість дій в несприятливих умовах.

Загалом аналіз концептуальних документів цивільно-військового співробітництва НАТО дозволяє зробити висновок про прагнення керівництва Північно-атлантичного блоку розширити свої можливості з проведення антикризових операцій [1, 2, 3].

В умовах повномасштабного збройного конфлікту, в якому перебуває наша держава з 24 лютого 2022 року через невиправдану збройну агресію російської федерації, ЦВС повинно відігравати одну з ключових ролей щодо деокупації та реінтеграції тимчасово окупованих територій, бути тандемом територіальної оборони та невід'ємною складовою загальної системи обороноздатності держави [4].

Для побудови ефективної моделі територіальної оборони й національного спротиву має бути повна взаємодія влади всіх рівнів і розуміння зони своєї відповідальності [5].

Список використаних джерел:

1. Allied Joint Doctrine for Civil-Military Cooperation (AJP-3.4.9) 2013 [Електронний ресурс]. - Режим доступу: http://www.cimic-coe.org/wp-content/uploads/2014/06/AJP-3.4.9-EDA-V1-E1.pdf.
2. CIMIC Capabilities by CIOR [Електронний ресурс]. - Режим доступу: http://cior.net/ getattachment/Organisation/Civil-Military-Cooperation-(CIMIC)/CIMIC-Handbook-Final- July-2013.pdf.aspx.
3. NATO Civil-Military Cooperation (CIMIC) Doctrine (AJP-9) 2003 [Електронний ресурс]. - Режим доступу: http://www.nato.int/ims/docu/ajp-9.pdf.
4. Доктрина "Цивільно-військове співробітництво" ВКП9-00(01).01: затв. наказом Головнокомандувача Збройних Сил України від 02.07.2020 №15860 [Електронний ресурс]. - Режим доступу: https://www.shrotyvg7com.ua/wp-contenent/uploads/2022/03/СП-9-0001.01.
5. Володимир Зеленський: Ефективна модель тероборони – це надійний тил для армії, і разом вони становлять основу сильної України 11 лютого 2022р, Новини. Прес-служба ОДА Режим доступу: https://old.loda.gov.ua/news?id=65454).

Емілія КАЗАН, к.і.н.
ORCID: 0000-0002-0997-6945
E-mail: kazan.emilia@gmail.com
Ігор ЗАБОЛОТНЮК
ORCID: 0000-0001-6153-1110
E-mail: igor171976@ukr.net
Микола КОВБА
ORCID: 0000-0003-1816-1016
E-mail: mykola.kovba@gmail.com
Орислава ГОЛУБОВСЬКА
НАСВ ім. гетьмана Петра Сагайдачного
ORCID: 0000-0003-4635-3445
E-mail: orusyag@gmail.com

ЦИВІЛЬНО-ВІЙСЬКОВЕ СПІВРОБІТНИЦТВО В ПОЧАТКОВИЙ ПЕРІОД АТО

З початком активних бойових дій на Донбасі в червні 2014 року виникла нагальна проблема надання медичної допомоги військовослужбовцям, що брали участь безпосередньо в бойових діях та отримували поранення різного ступеню і цивільним, які теж отримували травми (поранення) під час перебування безпосередньо в місцях, де велись бої. З метою покращення медичного забезпечення для військовослужбовців, які беруть участь в АТО (ООС) на Сході України, зокрема щодо надання пораненим кваліфікованої, спеціалізованої, високоспеціалізованої медичної допомоги, та проведення медичної та фізичної реабілітації, нормативно-правового врегулювання лікування в цивільних закладах охорони здоров'я в МО України разом з фахівцями МОЗ України та НАМН України був створений резерв профільних ліжок у найбільш потужних цивільних закладах охорони здоров'я. Цей комплекс взаємопов'язаних заходів започаткував створення бази цивільно-військової взаємодії.

На територіях проведення АТО (ООС) цивільно-військова взаємодія спрямовується на: надання медичної допомоги хворим і пораненим військовослужбовцям в цивільних закладах охорони здоров'я. Так у 2015 р. тільки в Луганській області, в цивільних закладах системи МОЗ, медичну допомогу надано 1100 військовослужбовцям, а в закладах охорони здоров'я системи Міністерства оборони медичну допомогу отримали 3000 цивільних осіб; організацію ресурсного забезпечення закладів охорони здоров'я, зокрема лікарськими засобами, виробами медичного призначення, медичним обладнанням тощо; інформаційне забезпечення лікувального процесу (було встановлено потребу покращення інформаційного забезпечення військових зі сторони органів і

закладів охорони здоров'я системи МОЗ) [5, с. 100]. З метою поєднання зусиль медичних служб силових відомств з цивільною системою медичного забезпечення був створений міжвідомчий Військово-цивільний координаційний штаб медичної допомоги (ВЦКШМД). Головним завданням якого стала координація діяльності центральних і місцевих органів виконавчої влади, пов'язаної з функціонуванням державної системи надання медичної допомоги військовослужбовцям, працівникам правоохоронних органів і цивільному населенню в зоні проведення антитерористичної операції та на територіях, де введено воєнний стан [1, с. 112]. Створення ВЦКШМД відбулося на виконання Указу Президента України від 4 листопада 2014 р. Про рішення Ради національної безпеки і оборони України "Про невідкладні заходи із забезпечення державної безпеки" [4]. ВЦКШМД створено на підставі спільного наказу Міністерства оборони України, Міністерства охорони здоров'я України, Міністерства внутрішніх справ України, Служби безпеки України та Національної академії наук України від 13 травня 2015 р. [2, с. 238] Відповідно до покладених на нього функцій, ВЦКШМД веде реєстри: поранених військовослужбовців та представників інших силових відомств в районі проведення АТО (ООС); щоденний моніторинг безповоротних та санітарних втрат; з жовтня 2015 року – інформацію щодо трупів, які надходять до моргів бюро судово-медичної експертизи в Донецькій та Луганській областях (дані є інформацією з обмеженим доступом) [2, с. 238] У ВЦКШМД зосереджено інформацію та встановлено оперативний зв'язок щодо: сил та засобів медичної служби силових структур у зоні АТО (ООС): медичної служби штабу АТО (ООС), оперативно-тактичних угруповань, військових мобільних госпіталів, груп підсилення в цивільних лікарнях; мобілізаційних карт усіх лікувальних закладів у районі проведення АТО (ООС) (містять інформацію про ліжковий фонд, обладнання, можливості надання допомоги, медичний персонал, резерви медичних препаратів, здатність до автономної роботи); резервів другої та третьої черги бригад екстреної медичної допомоги та медицини катастроф (інформація про вузькопрофільних фахівців, резервістів, автотранспорт); резервних медичних бригад Національної академії медичних наук України (висококваліфіковані кадри за основними спеціальностями, готові виїхати на вимогу до зони АТО (ООС) – 78 фахівців з науково-дослідних інститутів: нейрохірургії, хірургії та трансплантології, травматології, серцево-судинної хірургії); резервів ліжкового фонду, евакуаційного транспорту Запорізької, Дніпропетровської, Харківської та Луганської та Донецької областей. [3, с. 238] Станом на початок 2016 р. було проведено 10 засідань ВЦКІПМД, на яких було прийнято 10 рішень з окремих питань. Усі рішення стосувалися проблемних питань медичного забезпечення та координації сил і засобів військової та цивільної медицини та суміжних галузей. Штаб постійно інформував суспільство про перебіг лікування поранених. На екстреному засіданні штабу прийнято рішення про внесення змін до табеля оснащення бригад швидкої допомоги, проведення контролю навичок надання

домедичної допомоги працівниками патрульної поліції міста Києва. [2, с. 239] Перспективний напрям роботи ВЦКШМД – створення регіональних відділень Штабу, включення Штабу в єдину систему антитерору в Україні. [3, с. 239].

Під час медичного обслуговування військовослужбовців і мешканців у зоні проведення АТО(ООС), МОЗ України співпрацює з представниками громадських організацій України, представниками та консультантами місій ВООЗ тощо [3, с. 247], що приносить позитивні результати. Для прикладу, для лікування та реабілітації поранених, Червоним Хрестом надано допомогу медикаментами, хірургічними матеріалами та медичним обладнанням, засобами індивідуального захисту госпіталям та медичним установам, посилено потенціал загонів першої допомоги Червоного Хреста, проведено навчання населення навичкам надання першої допомоги, організовано поставки гуманітарної допомоги [6, с. 293].

Таким чином, війна на Донбасі сприяла створенню єдиного медичного простору, завдяки якому стало можливо надавати медичну допомогу військовим в цивільних медичних закладах (ЦРЛ), що розташовані в зоні АТО (ООС), а також надання медичної допомоги цивільним у медичних закладах бригад та військових госпіталях. В подальшому ця взаємодія сприяла наданню спеціалізованої та високоспеціалізованої допомоги та реабілітації в ВМКЦ ЗСУ, цивільних закладах МОЗ України, а також за кордоном. Але особливо військово-цивільна взаємодія сприяла покращенню відносин між Сходом та Заходом, цивільним населенням та військовими.

Список використаних джерел:

1. Бакай А. Міжвідомча взаємодія з організації медичної взаємодопомоги в надзвичайних ситуаціях. Медичне забезпечення антитерористичної операції: науково-організаційні та медико-соціальні аспекти: збірник наукових праць. К., 2016.
2. Корчинська А. Результати роботи військово-цивільного координаційного штабу медичної допомоги та необхідність організації таких штабів в областях. Медичне забезпечення антитерористичної операції: науково-організаційні та медико-соціальні аспекти: збірник наукових праць. К., 2016.
3. Кравченко В. Стан і проблеми медичного забезпечення населення та сил антитерористичної операції: правові, ресурсні та організаційні аспекти. Медичне забезпечення антитерористичної операції: науково-організаційні та медико-соціальні аспекти: збірник наукових праць. К., 2016.
4. Про утворення Військово-цивільного координаційного штабу медичної допомоги: Наказ Міноборони, МОЗ, МВС, СБУ, НАМН України. від 13.05.2015 № 207/272/556/311/34 [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua.

5. Рощін Г.Г., Мазуренко О.В., Набоченко О.З., Кліменко П.М. Цивільно-оперативний військовий центр як різновид систем управління при подоланні медико-санітарних наслідків надзвичайних ситуацій. Медичне забезпечення антитерористичної операції: науково-організаційні та медико-соціальні аспекти: збірник наукових праць. К., 2016.

6. Усіченко І. Діяльність Товариства червоного хреста України з надання медико-соціальної допомоги постраждалим від наслідків збройного конфлікту на Сході України та анексії Криму. Медичне забезпечення антитерористичної операції: науково-організаційні та медико-соціальні аспекти: збірник наукових праць. К., 2016.

Євген КАСАТКІН
Олександр МУЗИКА
Геннадій ЄФМОВ
НАСВ ім. гетьмана Петра Сагайдачного
ORCID: 0000-0003-4786-0756
E-mail: ydjinkas@ukr.nen

ДЕЯКІ АСПЕКТИ ЦИВІЛЬНО-ВІЙСЬКОВОГО СПІВРОБІТНИЦТВА

Військово-політичним керівництвом Північноатлантичного альянсу приділяється значна увага розробці нормативно-правової бази та відпрацюванню завдань, що покладаються на органи цивільно-військового співробітництва (CIVIL-MILITARY CO-OPERATION - CIMIC) [1]. Розвитком цього напряму стало розроблення Доктрини цивільно-військового співробітництва (AJP-09 NATO CIVIL-MILITARY CO-OPERATION (CIMIC) DOCTRINE), в якій дається визначення поняття цивільно-військового співробітництва − "координація і взаємодія між командуванням НАТО і цивільними учасниками конфлікту (населенням зони конфлікту, органами влади, міжнародними, національними і неурядовими організаціями та агенціями) з метою забезпечення виконання силами поставлених завдань" [2]. При цьому, слід звернути увагу, що основний акцент робиться на те, що значна частина завдань може бути вирішена без застосування військової сили або загрози силою, за рахунок узгодження дій військового командування з цивільним населенням.

Тривалий час у нашій державі цьому важливому напряму діяльності не приділялося належної уваги. Діяльність Збройних Сил (ЗС) України з організації цивільно-військового співробітництва (ЦВС) фактично була розпочата з травня 2014 року у зоні проведення Антитерористичної операції (АТО), яка сприяла набуттю певного досвіду роботи створених підрозділів ЦВС в умовах ведення бойових дій.

Але, лише наприкінці 2017 року Міністерством оборони (МО) затверджується "Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України", в якому визначається, що Управління цивільно-військового співробітництва ЗС України є одним із основних суб'єктів системи стратегічних комунікацій, діяльність якого є важливим елементом розвитку комунікацій, зокрема у частині сприяння та підтримки процесу розвитку та налагодження зв'язків з громадськістю та зв'язків з громадськістю у воєнній сфері [3]. Одночасно розробляється та наказом Генерального штабу Збройних Сил України затверджується "Положення про цивільно-військове співробітництво Збройних Сил України" [4]. При цьому мета цього співробітництва була окреслена лише двома напрямами: перший − формування позитивної громадської думки про діяльність військових формувань; другий − забезпечення сприятливих умов для виконання покладених на них завдань та функцій.

В подальшому розробляється та затверджується "Тимчасова настанова з цивільно-військового співробітництва у ході підготовки та застосування Збройних Сил України" [5], в якій викладені основні положення щодо планування, організації та управління заходами ЦВС у ході підготовки та проведення АТО, зокрема дається визначення поняттю "системи ЦВС", як сукупності функціонально взаємопов'язаних суб'єктів (органів, сил, засобів) ЗС України, інших військових формувань та об'єктів цивільного середовища, а також технологій впливу на них з метою створення умов для успішного виконання військами (силами) завдань.

На підставі отриманого досвіду проведення АТО (в подальшому операції Об'єднаних сил), як сукупність поглядів на завдання, роль і місце ЦВС у ході повсякденної діяльності та під час застосування ЗС України та інших складових сил безпеки та сил оборони (СБтаСО) держави, була розроблена та затверджена Головнокомандувачем ЗС України Доктрина "Цивільно-військове співробітництво" [6], в якій викладені як основні принципи організації, функції, сутність, складові системи ЦВС, так і вже розглянути особливості організації цивільно-військового співробітництва у різних формах застосування ЗС України та переданих в підпорядкування Головнокомандувачу ЗС України сил і засобів інших складових СБтаСО. При цьому не тільки у районах їх дислокації, а також в районах виконання завдань за призначенням. Одним з головних положень є окреслення основних шляхів розв'язання комплексних міжвідомчих питань (супутніх завдань), які виходять за межі завдань ЗС України та інших складових СБтаСО.

Збройна агресія російської федерації проти нашої держави змусила керівництво держави більш динамічно проводити зміни у процесах реагування складових СБтаСО держави на зміни обстановки з метою нарощування зусиль щодо відбиття агресії, одночасно наочно продемонструвала необхідність постійного моніторингу цивільного середовища, всебічного вивчення і прогнозування впливу громадянського суспільства на дії складових СБтаСО держави. Саме це забезпечує ефективне здійснення заходів ЦВС під час відбиття широкомасштабної збройної агресії.

Аналіз публікацій у відкритих мережах дозволяє зробити попередній аналіз напрямів діяльності структурних підрозділів ЦВС, який включає: налагодження певних зв'язків з громадськістю шляхом встановлення визначених каналів зв'язку ("гарячих ліній") та взаємодії із зацікавленими організаціями та окремими громадянами; організація роботи з волонтерськими організаціями з метою отримання волонтерської допомоги в інтересах дій військових формувань (транспортні засоби, медичне обладнання та устаткування, засоби зв'язку, індивідуального захисту тощо); організація координації дій з міжнародними організаціями, фондами та волонтерськими рухами з отримання та сприяння у розподілі гуманітарної допомоги постраждалому населенню від наслідків бойових дій; проведення заходів щодо інформування населення та культурно – просвітницької роботи (заходи мінної безпеки, безпеки під час обстрілів, комендантської години, інформування про діяльність складових СБтаСО, спільних спортивних та культурних заходів тощо); участь у поширенні офіційних інформаційних повідомлень від органів військового управління, контрпропаганді у соціальних мережах (шляхом спростовування неправдивих повідомлень противника); участь у розшуку та здійсненні транспортування тіл полеглих при відбитті агресії через центри комплектування та соціальної підтримки, організація комунікацій з родинами тих, хто загинув, зник безвісти, або потрапив у полон (інформування родин про соціальні гарантії військовослужбовцям, яка гарантує держава).

Таким чином, на відміну від поглядів та досвіду застосування системи ЦВС країн НАТО в збройних конфліктах сучасності (поза межами країн НАТО), де пріоритетом є положення про те, що значна частина завдань може бути вирішена без застосування військової сили за рахунок узгодження дій військового командування з цивільним населенням, вітчизняна система ЦВС, яка функціонує в умовах ведення бойових дій, направлена на досягнення певного паритету між діями військових формувань та цивільним середовищем, як в інтересах військ так і цивільного населення, які значною мірою взаємопоєднані. Разом з тим, у напрямках діяльності структурних підрозділів ЦВС, залишається значна кількість проблемних питань, особливо в організації взаємодії зі штабами зон (районів) територіальної оборони. Тому проблеми цивільно-військового співробітництва потребують глибоких досліджень, з метою пошуку та впровадження на практиці ефективних механізмів функціонування цієї системи в умовах війни.

Список використаних джерел:

1. Стратегічна Концепція Альянсу держав НАТО: затв. главами держав і урядів, які взяли участь в засіданні Північноатлантичної ради у Вашингтоні 23-24.04.1999 року (Федеральний округ Колумбія) [Електронний ресурс]. – Режим доступу: https://www.nato.int/cps/uk/natolive/official_texts_27433.htm.

2. AJP-09 NATO CIVIL-MILITARY CO-OPERATION (CIMIC) DOCTRINE, червень 2003 [Електронний ресурс]. – Режим доступу: https://www.nato.int/ims/docu/aqp/-9.pdf.

3. Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України: затв. наказом Міністерства оборони України від 22.11.17 № 612 [Електронний ресурс]. – Режим доступу: http://www.mil.gov.ua/content/mou_orders/612_nm_2017.pdf.

4. Положення про цивільно-військове співробітництво Збройних Сил України: затв. наказом Генерального штабу Збройних Сил України від 20.12. 2017 №446 [Електронний ресурс]. – Режим доступу: https://www. shrotyvg7com.ua/uploads/2022/05.

5. Тимчасова настанова з цивільно-військового співробітництва у ході підготовки та застосування Збройних Сил України: затв. наказом наказом Генерального штабу Збройних Сил України від 06.04.2019 №140 [Електронний ресурс]. – Режим доступу: https://www.dy.nayka.com.ua.?op=1&z=1459.

6. Доктрина "Цивільно-військове співробітництво" ВКП9-00(01).01: затв. наказом Головнокомандувача Збройних Сил України від 02.07.2020 №15860 [Електронний ресурс]. – Режим доступу: https://www.shrotyvg7com.ua/wp-contenent/uploads/2022/03/СП-9-0001.01.

Тарас КРАВЕЦЬ, к.г.н., доц.
НАСВ ім. гетьмана Петра Сагайдачного
ORCID: 0000-0001-5398-7441
E-mail: taras-kravets@ukr.net

НАЛАГОДЖЕННЯ КОНТАКТУ ВІЙСЬКОВИХ З ВОРОЖО НАСТРОЄНИМ НАСЕЛЕННЯМ

На сучасному етапі ведення бойових дій, коли міжнародні конфлікти та внутрішні напруги зберігають свою актуальність, питання налагодження контакту військових з ворожо настроєним населенням стає надзвичайно важливим і складним завданням для військових лідерів та політичних регуляторів. Здатність встановити конструктивні відносини з цивільним населенням в зоні конфлікту визначає не лише успішність ведення воєнних операцій, але й важливий аспект забезпечення довгострокового миру та стабільності в регіоні. Ми розглянемо ключові аспекти цієї проблеми, а також стратегії та підходи, які допомагають військовим встановити позитивний контакт з ворожо настроєним населенням та сприяють досягненню більш мирних та стабільних результатів у зоні конфлікту.

Аналіз ситуації та розуміння контексту. Першим і найважливішим кроком в налагодженні контакту військових з ворожо настроєним населенням є ретельний аналіз ситуації та розуміння контексту конфлікту. Це включає в себе вивчення історії конфлікту, релігійних та культурних особливостей регіону, демографічних та економічних факторів. Важливо також з'ясувати, хто є ключовими гравцями у ворожому настроєнні населення та які їхні мотивації та цілі.

Будівництво довіри та взаєморозуміння. Для встановлення контакту з ворожо настроєним населенням необхідно створити платформу для будівництва довіри та взаєморозуміння. Це може включати в себе взаємодію з лідерами та представниками цивільного населення, проведення громадських заходів, надання гуманітарної допомоги та розвитку інфраструктури.

Залучення місцевих ресурсів та експертів. Для ефективного налагодження контакту необхідно залучити місцевих ресурсів та експертів. Це можуть бути місцеві лідери, представники громадських організацій, духовні лідери та інші особи, які мають авторитет в регіоні. Їхні знання та вплив можуть сильно сприяти налагодженню контакту.

Комунікація та публічність. Ефективна комунікація є важливою складовою налагодження контакту з ворожо настроєним населенням. Вона включає в себе розробку стратегії зв'язку, яка передбачає інформування громадськості про наміри та дії військових, вислуховування скарг і побажань місцевих жителів, а також активну роботу з місцевими ЗМІ та соціальними медіа.

Постійна оцінка та адаптація стратегії. Ситуація в зоні конфлікту може змінюватися, тому важливо постійно оцінювати ефективність стратегії налагодження контакту та адаптувати її до нових умов. Це може вимагати перегляду підходів, зміни тактики чи введення нових ініціатив.

Завершуючи, налагодження контакту військових з ворожо настроєним населенням є складним і багатоаспектним завданням. Проте, застосування вищезазначених стратегій та підходів може сприяти зменшенню конфліктів, створенню сприятливого клімату для миру та співіснування в регіонах, де це найбільше потрібно.

На власному досвіді та через вивчення різних конфліктних ситуацій зони бойових дій можна зробити висновок, що налагодження контакту військових з ворожо настроєним населенням є ключовим аспектом досягнення миру, стабільності та реконструкції в конфліктних регіонах. Ретельний аналіз ситуації, будівництво довіри, залучення місцевих ресурсів, ефективна комунікація та постійна адаптація стратегії грають критичну роль у цьому процесі.

Важливо пам'ятати, що взаємодія військових з цивільним населенням має бути спрямована на зменшення страждань, підвищення безпеки та сприяння мирному врегулюванню конфлікту. Це вимагає від військових лідерів та

політичних регуляторів великої розсудливості, чутливості до потреб місцевого населення і здатності адаптувати стратегії до змінних обставин.

Тільки шляхом співпраці та взаєморозуміння ми можемо сприяти відновлення миру і стабільності в регіонах, які відчувають найбільше впливу від бойових дій.

Список використаних джерел:

1. Ucko, D. H. (2008). The New Counterinsurgency Era in Critical Perspective. Contemporary Security Policy, 29(2), 189-221.

2. Gentile, G. P. (2009). A Strategy of Tactics: Population-centric COIN and the Army. Parameters, 39(1), 21-30.

3. Arreguin-Toft, I. (2005). How the Weak Win Wars: A Theory of Asymmetric Conflict. International Security, 26(1), 93-128.

Микола МИТНИК, к.т.н, доц.
Андрій КРИСЬКОВ, д.і.н., доц.
ТНТУ ім. Івана Пулюя
ORCID: 0000-0003-1437-4823
E-mail: Kryskov.te@gmail.com

ГІБРИДНА ВІЙНА ТА СКЛАДНІСТЬ ПРИЙНЯТТЯ РІШЕНЬ ПІД ЧАС НЕЇ (лютий 2014 – січень 2022)

Напад російської федерації на Україну спричинив руйнівні наслідки для систем європейської та світової безпеки. Війна не тільки порушила регіональну стабільність, а й створила та підсилила глобальні ризики. Для ефективного спротиву агресору Україні та її міжнародним партнерам необхідно мати чітке розуміння природи й характеру цієї війни, яку російське керівництво різними способами веде з лютого 2014 р. Навіть зараз росіяни зазначають, що це лише спеціальна операція, а не війна.

Поняття гібридної війни виявилося теоретично й практично найбільш придатним для визначення специфіки дій російської федерації, яка, поєднуючи мілітарні, квазімілітарні, дипломатичні, інформаційні, економічні засоби, не гребуючи ядерним шантажем, послідовно намагається досягти в Україні власних, не зовсім зрозумілих міжнародній спільноті політичних цілей. Гібридна війна охоплює явище набагато ширше, ніж сучасні форми ведення бойових дій. Фактично – це новий вид глобального протистояння у сучасному дестабілізованому світі, це заміна “холодної війни” ланцюгом збройних конфліктів, ускладнена і нестабільна форма міжнародних відносин [4, с.17]. Гібридна війна перетворюється на домінантний вид війни у майбутньому. Тут діє та сама аргументація, що й за часів холодної війни, та ж

сама заборона переступати певні межі, щоб не спровокувати стратегічного опонента на застосування реальних військових дій [2, с.99].

Напад росії на Україну продемонстрував, що гібридний конфлікт може бути за своєю сутністю міждержавним. Специфіка російської гібридної агресії проти України полягає навіть не стільки в загальних методах та цілях гібридної війни, як у беззастережному та свавільному порушенні нею системи базових міжнародно-правових угод, великих масштабах заподіяних ушкоджень, значній тривалості конфлікту. Досвід протидії з боку України продемонстрував принципово нові можливості захисту в умовах гібридної агресії та водночас виявив точки вразливості країни, яка стала об'єктом нападу і втратила територіальну цілісність.

Гібридна війна є війною, коли військові моделюють себе як цивільних, а цивільні можуть ставати військовими, беручи до рук зброю. Прикладом перших є "зелені чоловічки", а других – терористи. У гібридній війні задіяні всі види протиставлень: військові проти військових, військові проти цивільних, цивільні проти військових і цивільні проти цивільних. Усе це створює хаос, у якому вигравatиме організованіша сторона, для якої розвиток подій не буде несподіваним.

Ще одна складність полягає в тому, що військові не готові до боротьби з цивільними, а цивільні – з військовими. Усе це складніша система, ніж звичайна війна, де ворог/не-ворог дуже чітко диференційовані й заздалегідь задано набір дозволених/заборонених дій. Це веде до напруження не тільки зовнішнього інформаційного конфлікту, але й внутрішнього, коли опоненти відразу трактуються як зрадники. Інформаційний конфлікт симетричний військовому, оскільки й тут кожна зі сторін намагається захопити чужий/утримати свій інформаційний простір.

Гібридна війна віддаватиме перевагу тому, хто вміє працювати з масовою свідомістю, з інформаційним супроводом війни. Сторона, що атакує, повинна доводити справедливість своїх дій як власному народові, так і народові, на який спрямована атака. А атакованій стороні досить важко давати відсіч такій неоголошеній війні. Гібридна війна стала здобутком нашого часу саме тому, що багато потрібних для неї завдань можна виконати за рахунок інформаційного компонента [1, с.119]. Що сильнішим стає його розвиток, то легшим буде виконання цих завдань.

Гібридна війна в російському варіанті виявилася дуже продуманим варіантом впливу на прийняття рішень різними сегментами населення та інститутами української держави. Українська армія, наприклад, у випадку з Кримом виявилася повністю бездіяльною. Україна, її армія, її державні інститути, її населення виявилися не готовими до викликів у Криму. Щодо Донбасу ситуація була переламана, але знову не за рахунок державних інститутів, а завдяки добровольчим батальйонам і волонтерському руху, що виникли ніби нізвідки. У гібридній війні швидкість фізичних дій випереджає швидкість розуміння того, що відбувається, і, відповідно, прийняття рішень. Нападник рухається по запланованій ним траєкторії, тоді як атакована сторона сприймає цей рух як якесь випадкове непорозуміння.

Модель нерозуміння противником того, що відбувається, вдала для нападника ще й тим, що під таку реакцію мімікрують ті, хто взагалі не хоче або боїться реагувати. Вони уникли покарання відповідно до закону. Жодна особа, наприклад, не була покарана за здачу Криму. В українському варіанті війни був різко скорочений фізичний простір розвитку дії з одночасним різким розширенням інформаційного простору. Україна отримала майже нескінчену кількість інтерпретацій та інтерпретаторів, які просували зовсім протилежні розуміння. Така невідповідність призвела до того, що "ворог" мімікрував під "друга", а військові "забували" застосовувати зброю. Українські військові, яким виплачували гроші, роздавали звання й нагороди, в Криму зразка лютого-березня 2014 р. раптом стали цивільними. Вони перетворилися на глядачів того, що відбувалося перед ними.

Важливу роль у цьому відіграла спільність інформаційного і віртуального просторів, які переконували, що обидві країни – принципово братні, а воєнні дії між ними є неможливими. Проте неможливе абсолютно спокійно почало реалізовуватися, "зелені чоловічки", на яких вчасно і адекватно не зреагували в Криму, уможливили появу "ополченців" на Донбасі. До слова, росія утримувала імідж випадкового й непідготовленого варіанта розвитку подій, який би мав інше реагування, якби це була звичайна війна. Усе це можна визначити як ситуацію, в якій Україну змусили слідувати чужому алгоритму.

Війна завжди передбачає три інформаційні фронти, що вимагають активних дій [3, с.295]. Це, по перше, домашній фронт, бо населення має підтримувати своїх військових. Це, по друге, робота з населенням супротивника. І це, по третє, робота з населенням інших країн. У кожному випадку масова свідомість має отримати свій власний матеріал для прийняття потрібного рішення. Однак, якщо для власного населення альтернативна точка зору завжди буде поза мейнстрімом, то для населення супротивника та для населення інших країн завжди домінуватиме контрінтерпретація, що вимагає серйозної та креативної контрпропаганди.

Гібридна війна спрямована на таку корекцію картини світу в усіх її учасників, яка буде вигідна нападникам. Причому для цього активно використовуються три простори: інформаційний, фізичний та віртуальний. Задіяні фізичні об'єкти мають чіткі інформаційні та віртуальні складові, наприклад, подача "зелених чоловічків" як ввічливих людей, штучних постановок – як документальних сцен, загарбання чужих територій – як звільнення їх від "нацистської влади" тощо. Тобто, відбувається блокування невигідних агресорам інтерпретацій.

Всі війни, у тому числі й гібридні, колись закінчуються. Але їхні уроки живуть набагато довше і спрямовані на недопущення їх у майбутньому.

Список використаних джерел:

1. Криськов А., Криськова С., *Інформаційний простір як складова частина гібридної війни,* Integracion de las ciencias fundamentales y aplicadas en el paradigma de

la sociedad postindustrial. Матеріали міжнародної науково-практичної конференції (Барселона, 24.04.2020). Vol. 3, с.118-120.

2. Почепцов Г. Від покемонів до гібридних війн: нові комунікативні технології XXI століття. Київ, 2017. 260 с.

3. Почепцов Г. Смисли і війни: Україна і Росія в інформаційній і смисловій війнах. Київ, 2016. 316 с.

4. Світова гібридна війна: український фронт. Харків, 2017. 496 с.

Сергій ОРЕЛ, к.т.н., с.н.с.
НАСВ ім. гетьмана Петра Сагайдачного
ORCID: 0000-0002-5887-3483
E-mail: orelsm0@gmail.com

ВПЛИВ СОЦІАЛЬНИХ МЕДІА НА ЦИВІЛЬНО-ВІЙСЬКОВІ ВІДНОСИНИ

Інтернет об’єднав суспільство та відкрив інформацію для загального споживання з безпрецедентною швидкістю та обсягом. Як частина суспільства, військовослужбовці не захищені від здатності споживати та ділитися ідеями, даними та думками у соціальних мережах майже миттєво. Однак, незважаючи на деякі переваги, соціальні медіа становлять ризики для сучасного стану цивільно-військових відносин. Розглянемо ці ризики, спираючись на результати деяких закордонних дослідників [1].

Почнемо з переваг соціальних мереж: Вест-Пойнт і Університет національної оборони (NDU) [2] визначили п’ять ключових переваг платформ соціальних медіа: інтерактивний досвід і можливість повідомляти про події та реагувати на них, коли вони відбуваються; інформаційна інтеграція та здатність синтезувати інформацію між проблемами; широка аудиторія та можливість обміну з кількома групами одночасно; миттєвість даних і доступ до інформації в режимі реального часу; логічні, прості комп'ютерні інтерфейси, які забезпечують зручність використання. З огляду на те, що так багато військовослужбовців щодня використовують платформи, а темпи військових операцій у всьому світі так швидко змінюються, соціальні медіа пропонують військовим офіцерам можливість співпрацювати, ділитися передовим досвідом, вчитися на досвіді один одного та бути в курсі актуальних тем до своїх підрозділів у режимі реального часу, ділитися точною інформацією, а не ставати жертвою пліток і чуток.

Іншою складовою є взаємодія засобів масової інформації і військових. Військові історично скептично ставилися до ЗМІ через секретний характер більшості військових операцій, побоюючись, що вороги можуть виявити тактику, методи, процедури чи стратегічні плани. Однак ера Інтернету почала

перевизначати те, що є “медіа”, що, відповідно, змінює складність відносин ЗМІ та військових і, зрештою, цивільно-військових відносин. Таким чином, потенційно неперевірені та недостовірні репортажі про військові питання можуть охопити широку аудиторію. Оскільки соціальні медіа надають більше простору для створення контенту новин, перевірені джерела змушені конкурувати з дедалі більшою кількістю неперевіреної інформації. Ширший і швидший доступ до інформації – це добре в теорії, але це шкідливо в контексті цивільно-військових відносин, оскільки, мабуть, він не створив більш поінформовану громадськість, а натомість більш цинічну. Таким чином, поширеність соціальних медіа загрожує цивільно-військовим відносинам через їх здатність зменшувати довіру суспільства до уряду та військових.

Ще однією складовою впливу соціальних медіа є те, що їх використання в Збройних силах створює ризик втрати ними своєї позапартійної позиції. Опитування West Point і NDU, згадане вище [2], також виявило, що 83 відсотки військовослужбовців і курсантів були свідками того, як їх друзі – військові публікували посилання на політичні історії, ставили “лайки” або рекламували політичні теми, які опублікували інші, або стежили за політичними діячами в соціальних мережах. Примітно, що респондентами NDU були офіцери у званнях майорів, підполковників і полковників, тобто званнях, згідно яким офіцери мають більшу владу та вплив у війську. Ця подія має два помітні наслідки для цивільно-військових відносин. По-перше, військовослужбовці (особливо молодші офіцери, сержанти та солдати) можуть інтерпретувати таку поведінку як прийнятну військову поведінку та розглядати її як неофіційний дозвіл робити те саме. По-друге, невійськові друзі в соціальних мережах, які переглядають ці публікації, можуть інтерпретувати політичні та особливо партійні публікації та поведінку як відображення офіційної позиції Міністерства оборони. Разом з тим, численні нормативні акти, меморандуми та керівні документи наголошують на необхідності військовослужбовців залишатися позапартійними та уникати публічних заяв або внесків у політичні партії. Наприклад, Директива Міністерства оборони (DODD) 1344.10 містить конкретні вказівки для всіх військовослужбовців США щодо того, що є прийнятним, а що заборонено під час політичної поведінки. Наслідки політичної участі військових у соціальних мережах для цивільно-військових відносин є величезними. Якщо військові фактично не зможуть підтримувати належний порядок і дисципліну в епоху соціальних медіа, довіра з боку громадськості та цивільного керівництва, безсумнівно, впаде, а довіра є фундаментальною складовою для підтримки здорового цивільного контролю над армією.

Очевидно, що у майбутньому військове керівництво має робити більше, щоб впливати на те, як його офіцери залучаються до соціальних мереж. По-перше, мають бути навмисні дії проти офіцерів, які висловлюють партійну думку в соціальних мережах. Якщо військові хочуть притягувати своїх членів до

відповідальності та підтримувати належний порядок і дисципліну, їм слід інвестувати в певну форму моніторингу соціальних мереж, щоб проводити регулярні перевірки облікових записів військовослужбовців у соціальних мережах. Зрозуміло, що неможливо позбавити військовослужбовців права мати облікові записи в соціальних мережах через їхню поширеність у повсякденному житті, однак для притягнення до відповідальності потрібні більш відчутні дії, щоб передбачити відповідні рівні покарання залежно від порушення. По-друге, облікові записи в соціальних мережах повинні бути включені до розслідування при перевірці безпеки. Крім того, військові повинні мати чітке визначення того, що є "політичною діяльністю в соціальних мережах" [3].

Нижче наведемо висновки, що витікають із розглянутих матеріалів закордонних (переважно американських) дослідників, що стосуються впливу соціальних медіа на цивільно-військові відносини, які, на нашу думку, в значній мірі можуть бути справедливими для Збройних Сил України.

Висновки: Військові по праву користуються перевагами спілкування в соціальних мережах, але не можуть протистояти тому, як цивільний сектор бачить військову діяльність на різних платформах. Зменшення суспільної довіри до державних установ у поєднанні зі здатністю соціальних медіа поширювати необґрунтовану та недостовірну інформацію призводить до каскадного ефекту, який загрожує довірі до уряду в цілому та потенційно здатності військових залишатися позапартійними. Це серйозний ризик для цивільно-військових відносин з двох причин. По-перше, це послаблює принцип цивільного контролю над армією. По-друге, це загрожує здатності військових підтримувати належний порядок і дисципліну у відомстві. Соціальні медіа фактично нормалізували політичну поведінку в армії, тому міністерство оборони має вжити більш комплексних і продуманих заходів, щоб припинити політичну активність військовослужбовців. Це сприятиме тому, щоб цивільно-військові відносини залишалися здоровими та міцними.

Список використаних джерел:

1. Giroux Holly. "Social Media's Impact on Civil-Military Relations: Balancing the Good with the Bad." URL: https://www.airuniversity.af.edu/Wild-Blue-Yonder/Articles/Article-Display/Article/2871481/social-medias-impact-on-civil-military-relations-balancing-the-good-with-the-bad/ (дата звернення: 18.09.2023).
2. Heidi A. Urben. Like, Comment, Retweet. The State of the Military's Nonpartisan Ethic in the World of Social Media. Washington, D.C.: National Defense University Press, May 2017. 66 p.
3. Losey Stephen, "Pentagon Eyes Plan to Intensify Social Media Screening in Military Background Investigations," Military News, Military.Com (blog), March 3, 2021. URL: https://www.military.com/ (дата звернення: 19.09.2023).

Володимир ПАШИНСЬКИЙ, д.ю.н, доц.
Дмитро СТУПАК
НУОУ

ВІЙСЬКОВІ АДМІНІСТРАЦІЇ ЯК СУБЄКТ СИСТЕМИ ВІЙСЬКОВО-ЦИВІЛЬНОГО СПІВРОБІТНИЦТВА

Розпочата широкомасштабна російська військова агресія та запровадження у зв'язку з цим в Україні адміністративно-правового режиму воєнного стану зумовили зростання інтересу з боку суб'єктів публічної адміністрації та наукової спільноти до підвищення рівня цивільно-військового співробітництва у зв'язку з необхідністю створення умов для успішного виконання військами (силами) завдань за призначенням.

До системи цивільно-військового співробітництва належить сукупність суб'єктів (органів, сил, засобів) ЗС України, інших складових сил оборони, об'єктів цивільного-середовища та технологій впливу на них. В свою чергу до основних об'єктів цивільного-середовища зокрема належать: цивільне населення, громадські організації, міжнародні урядові та неурядові організації, система і структура влади, правоохоронні органи, інфраструктура забезпечення життєдіяльності та техногенно небезпечні об'єкти [1].

Однією з особливих ознак адміністративно-правового режиму воєнного стану є створення нових суб'єктів забезпечення цього правового режиму, зокрема військових адміністрацій – тимчасових спеціальних державних органів створених на забезпечення правового режиму воєнного стану. Виходячи з останнього, військові адміністрації є елементом системи військово-цивільного співробітництва на який також покладаються завдання з забезпечення нагальних потреб населення та функціонування об'єктів цивільного середовища.

Правове регулювання діяльності військових адміністрацій, як суб'єктів забезпечення правового режиму воєнного стану, здійснюється ст.ст. 4 та 15 Закону України "Про правовий режим воєнного стану", відповідно до яких військові адміністрації є тимчасовими органами, які можуть утворюватися за рішеннями, прийнятими Президентом України на територіях, на яких введено воєнний стан. Структуру і штатний розпис військових адміністрацій населених пунктів затверджує начальник Генерального штабу – Головнокомандувач Збройних Сил України за поданням начальника відповідної військової адміністрації. Система військових адміністрацій складається з: військових адміністрацій областей; військових адміністрацій районів; військових адміністрацій населених пунктів [2 ст. 166-167]. Також, в населених пунктах, для виконання заходів правового режиму воєнного стану, військовою адміністрацією можуть призначатися військові коменданти.

Основним завданням військових адміністрацій є забезпечення дії Конституції та законів України, забезпечення разом із військовим командуванням запровадження та здійснення заходів правового режиму воєнного стану, оборони, цивільного захисту, громадської безпеки і порядку, захисту критичної інфраструктури, охорони прав, свобод і законних інтересів громадян [3].

Відповідно до положень Закону України "Про правовий режим воєнного стану" до повноважень військових адміністрацій населених пунктів з забезпечення адміністративно-правового режиму воєнного стану належать: запровадження та здійснення заходів правового режиму воєнного стану; сприяння організації мобілізації громадян; забезпечення доведення до підприємств, установ та організацій незалежно від форми власності, а також населення наказу військового комісара про оголошення мобілізації; сприяння організації виробництва і поставок у війська підприємствами та організаціями, що перебувають у комунальній власності, замовленої продукції, послуг, енергоресурсів; прийняття рішень про заборону торгівлі зброєю, сильнодіючими хімічними і отруйними речовинами, а також алкогольними напоями та речовинами, виробленими на спиртовій основі; прийняття рішень про внесення пропозиції до Ради національної безпеки і оборони України, погодженої обласною військовою адміністрацією, щодо здійснення примусового відчуження або вилучення рухомого майна, та інші [3].

Районна, обласна військові адміністрації здійснюють на відповідній території зокрема такі повноваження: прийняття у межах, визначених законом, рішень з питань захисту населення і територій від надзвичайних ситуацій, ліквідації наслідків надзвичайних ситуацій; прийняття рішень про заборону торгівлі зброєю, сильнодіючими хімічними і отруйними речовинами, а також алкогольними напоями та речовинами, виробленими на спиртовій основі; прийняття рішення щодо визначення переліку підприємств, виробничі потужності яких підлягають переміщенню (евакуації) із зони бойових дій [3].

Спрямування, координацію та контроль за діяльністю обласних військових адміністрацій з питань забезпечення оборони, громадської безпеки і порядку, захисту критичної інфраструктури, здійснення заходів правового режиму воєнного стану здійснює Генеральний штаб Збройних Сил України, а з інших питань - Кабінет Міністрів України у межах своїх повноважень [3].

Аналіз повноважень дає підстави стверджувати, що у разі утворення військових адміністрацій останні здійснюють повноваження як місцевих державних адміністрацій так і органів місцевого самоврядування. Однак з огляду на підстави їх утворення, основний напрямок їх діяльності зосереджений на виконанні завдань із забезпечення правового режиму воєнного стану. Слід зауважити, що законодавством не передбачено обов'язкового припинення діяльності визначених Конституцією та законами України органів державної влади і органів місцевого самоврядування у разі утворення військових

адміністрацій. Досвід утворення військових адміністрацій в Україні показав можливість їх спільної роботи.

Прикладами безпосередньої реалізації повноважень військовими адміністраціями можна навести рішення (спільні рішення) військових адміністрацій щодо обмеження торгівлі алкогольними напоями на відповідних територіях громад [4,5,6], накази військових адміністрацій про заборону масових заходів [7], встановлення комендантської години [8], та інші.

Таким чином, військові адміністрації є елементом системи цивільно-військового співробітництва та спеціальними тимчасовими державними органами, які створюються та діють виключно в період дії адміністративно-правового режиму воєнного стану та основним їх призначенням є забезпечення виконання заходів цього правового режиму. В той же час, військові адміністрації мають особливий правовий статус. З одного боку, вони, як органи державної влади, відносяться до об'єкту військово-цивільного співробітництва, з іншого, враховуючи коло наданих повноважень, діяльність військових адміністрацій та суб'єктів військово-цивільних адміністрацій об'єднані однією метою – створення сприятливих умов у цивільному середовищі для досягнення військових цілей, що відносить їх до суб'єктів системи цивільно-військового співробітництва. Зазначене залишає перспективи подальших розвідок у даному напрямі.

Список використаної літератури:

1. Доктрина "Цивільно-військове співробітництво", затверджена Головнокомандувачем Збройних Сил України 01.07.2022 р.
2. Голуб В.О. Становлення та розвиток інституту адміністративно-правового режиму воєнного стану: автореф. дис. на здобуття наукового ступеня кандидата юрид. наук : спец: "12.00.07" адміністративне право і процес; фінансове право; інформаційне право. Київ, 2017. 11 с.
3. Про правовий режим воєнного стану: Закон України від 12 трав. 2015 р. № 389-VIII. Відомості Верховної Ради. 2015. № 28. Ст. 250. URL :http://zakon3.rada.gov.ua/laws/show/389-19 (дата звернення: 24.09.2023).
4. Про заборону торгівлі алкогольними напоями на території Запорізької області: Наказ військового командування і Запорізької обласної військової адміністрації від 11 березня 2022 року №3. URL : https://www.zoda.gov.ua/files/WP_Article_File/original/000183/183653.pdf. (дата звернення: 24.09.2023).
5. Про заборону продажу алкогольних напоїв в умовах правового режиму воєнного стану: Розпорядження начальника Синельниківської районної військової адміністрації від 09 травня 2022р.№ Р-89/0/115-22. URL : https://snrda.dp.gov.ua/rishennya-gromadi/pro-zaboronu-prodazhu-alkogolnih-napoyiv-v-umovah-pravovogo-rezhimu-voyennogo-stanu. (дата звернення: 24.09.2023).

6. Про заборону торгівлі алкогольними напоями на території Запорізької області: Наказ голови Запорізької обласної державної адміністрації від 21.02. 20 23 р. № 85. URL : https://www.zoda.gov.ua/news/64575/pro-zaboronu-torgivli-alkogolnimi-napoyami-na-teritoriji-zaporizkoji-oblasti.html. (дата звернення: 24.09.2023).

7. Про заборону проведення масових заходів: Наказ Хмельницької обласної адміністрації від 19.07.23 р. № 192/558/2023-нс. URL :https://www.adm-km.gov.ua/doc/orders/2023/07/192_558ns_190723.pdf. (дата звернення: 24.09.2023).

8. Про встановлення комендантської години на території області 16 квітня 2023 року: Наказ Хмельницької обласної військової адміністрації від 11.04.2023 р. № 87/2023-н. URL : https://www.adm-km.gov.ua/doc/orders/2023/04/087n_110423.pdf (дата звернення: 24.09.2023).

Вадим ТОРІЧНИЙ
д.н. з держ.упр., доц.
ORCID: 0000-0003-3336-6386
Володимир КАЛЮЖНИЙ
НАДПСУ ім. Богдана Хмельнитцького
ORCID: 0009-0006-8057-3897

МОДЕЛЬ РЕАЛІЗАЦІЇ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ У ДЕРЖАВНІЙ ПРИКОРДОННІЙ СЛУЖБІ

Система стратегічних комунікацій у прикордонній службі України, основні механізми її реалізації, базуються на принципах пріоритету права, законності, захисту національних інтересів, захисту прав та свобод громадян та людей, демократичної підзвітності, прозорості діяльності, позапартійності. Для отримання цілісного уявлення про стратегічні комунікації здійснено інтеграцію кожної сутнісно-змістової складової у відповідну організаційну модель [1].

У представленій організаційній моделі проаналізовані: підстави використання стратегічних комунікацій у прикордонній службі (сучасні соціальні запити; євроінтеграційні процеси; демократизація реформ), особливості реалізації такого контролю (забезпечення відповідності вимогам чинного законодавства та відомчим наказам); основні механізми стратегічних комунікацій (правовий, організаційний, громадська експертиза та консультації, державно-приватне партнерство); об’єкти впливу (Адміністрація прикордонної служби, органи охорони державного кордону); зміст механізмів стратегічних комунікацій (проведення аудиту, розслідувань і перевірок; запобігання і виявлення розтрат, шахрайства і зловживань; збільшення економії та підвищення ефективності; перевірка відповідності виконавчим розпорядженням і принципам; вивчення

оперативної діяльності; вивчення проектів законів і постанов; надання регулярних звітів начальникам служб; надання регулярних звітів органам виконавчої влади, законодавчій владі або наглядовій комісії; надання звітів за запитами законодавчої влади чи наглядової комісії; розслідування скарг на службу; забезпечення належної поваги до прав людини; забезпечення відповідності постановам про передачу документів та інформації тощо).

Усі демократичні країни, зазвичай, мають свою модель стратегічних комунікацій у секторі безпеки та оборони, оскільки і система безпеки і національні особливості особливі в усіх [2]. Проте, незважаючи на таку різноманітність моделей стратегічних комунікацій у секторі безпеки і оборони, їх можна вважати ідентичними. Суттєві відмінності між моделями згаданих комунікацій полягають в наявності обмежень щодо надання громадянських прав та свобод військовослужбовцям та працівникам (висловлювання своїх думок, здійснення політичної діяльності, участі у громадських об'єднаннях, професійних спілках і т. д.), а також у відсутності однозначного уніфікованого підходу у реалізації президентського або парламентського контролю.

Загалом, призначення організаційної моделі стратегічних комунікацій у прикордонній службі полягає у реалізації ключових принципів управління правоохоронною організацією у будь-якому суспільстві:

забезпечення системи стримування та противаги державних формувань під контролем парламенту;

прозорість структури з метою уможливлення демократичної конкуренції;

взаємодія прикордонного відомства із суспільством;

регулярна публічна звітність про діяльність.

Отже, за допомогою організаційної моделі стратегічних комунікацій у прикордонній службі можна відтворити шлях державотворення, оскільки така модель повинна містити функціонуючий правовий фундамент, свідчити про реформування інституції, не бути формальною та концентруватись лише на президентові держави.

Список використаних джерел:

1. Вичалківська Ю. С. Організаційно-правове регулювання демократичного цивільного контролю над сектором безпеки і оборони України. *Інвестиції: практика та досвід*. Київ, 2018. № 1. С. 116–121.

2. Сіцінська М. В. Передумови виникнення недоліків системи демократичного цивільного контролю над правоохоронними органами України. Журнал "*Інвестиції: практика та досвід"* № 24, 2011, с. 84–86.

Ігор УШАКОВ
аспірант ІДУ та НД з ЦЗ, НУОУ
ORCID: 0000-0002-0231-085X
E-mail: i.ushakov@edu.nuou.org.ua

ІНСТРУМЕНТИ ВДОСКОНАЛЕННЯ МЕХАНІЗМІВ РЕАЛІЗАЦІЇ ЦИВІЛЬНО-ВІЙСЬКОВОГО СПІВРОБІТНИЦТВА У СЕКТОРІ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

До інструментів вдосконалення механізмів реалізації цивільно-військового співробітництва у секторі безпеки і оборони України (далі – ЦВС у СБіО України) ми відносимо політико-дипломатичні, організаційно-правові та інформаційно-комунікативні заходи.

До політико-дипломатичних заходів вдосконалення механізмів реалізації ЦВС у СБіО України ми пропонуємо віднести: "…імплементацію міжнародних програм, спрямованих на впровадження ЦВС у СБіО України; залучення до співробітництва у сфері ЦВС міжнародних урядових та неурядових організацій; формування довіри суспільства до воєнної політики держави задля підтримки курсу з набуття членства в ЄС та НАТО, забезпечення підтримки України на політичному рівні провідними державами світу" [1, с. 107]; багатостороннє та двостороннє співробітництво з державами-партнерами України у сфері ЦВС; навчання та підвищення кваліфікації представників суб'єктів ЦВС на базі держав-членів НАТО; обмін досвідом застосування сил і засобів ЦВС з державами-партнерами України; залучення та супроводження діяльності міжнародних урядових, неурядових та гуманітарних організацій в постконфліктний період на деокупованих територіях тощо.

До організаційно-правових заходів вдосконалення механізмів реалізації ЦВС у СБіО України ми пропонуємо віднести: створення та організацію навчально-наукових центрів ЦВС у закладах вищої освіти складових сил безпеки та оборони України "…відповідно до стандартів, прийнятих державами-членами НАТО" [1, с. 107], в тому числі задля підготовки нової генерації науковців у сфері ЦВС; розвиток системи підготовки та підвищення кваліфікації спеціалістів ЦВС у складових СБіО України; забезпечення ефективної міжвідомчої та міжгалузевої координації в розробленні принципів співпраці у сфері ЦВС з урахуванням досвіду держав-партнерів, власного історичного надбання у зазначеній сфері, а також стану соціально-економічного розвитку країни та територіальних особливостей; "…узгодження правових норм з питань розвитку ЦВС у СБіО України" [1, с. 107] з урахуванням загроз інформаційного характеру, а також регулювання питань цивільно-військових відносин тощо.

Створення навчально-наукових центрів ЦВС у закладах вищої освіти складових сил безпеки та оборони України передусім буде сприяти розвитку

безпосередньо ЦВС у сфері забезпечення національної безпеки і оборони, удосконаленню системи підготовки та підвищення кваліфікації фахівців ЦВС з урахуванням набутого бойового досвіду, запровадженню інтегрованої системи контролю за якістю цієї підготовки шляхом розробки нових освітньо-кваліфікаційних характеристик, концентрації наукової діяльності у сфері ЦВС, впровадження стандартів підготовки держав-членів НАТО, відповідно до доктринальних документів НАТО та держав-партнерів України з питань ЦВС [2, 3, 4, 5, 6] тощо.

А задля зменшення відчуття у певної частини населення України відсутності зовнішніх загроз інформаційного характеру та чіткого розуміння причин і джерел їх появи, до інформаційно-комунікативних заходів вдосконалення механізмів реалізації ЦВС у СБіО України ми пропонуємо віднести: навчання співробітників у сфері ЦВС кризовим і стратегічним комунікаціям та стратегічному плануванню; використання комунікативних можливостей держави задля просування загальнодержавного наративу, формулювання та впровадження ключових повідомлень для підвищення розуміння суспільством діяльності складових СБіО України.

Надзвичайно важливим в згаданому контексті є активне залучення галузевих асоціацій, громадських організацій, соціальних фондів та інших інститутів громадського суспільства для просування згаданого наративу.

Реалізація зазначених заходів надасть можливість показати комплексний характер ЦВС та механізмів його реалізації.

Список використаних джерел

Ушаков І.В. Аналіз проблемних питань механізмів реалізації цивільно-військового співробітництва у секторі безпеки і оборони України. *Інвестиції: практика та досвід.* 2022. № 22. С. 103-109.

MC 411/1 NATO Military Policy on Civil-Military Cooperation. 2001. URL: http://www.nato.int/ims/docu/mc411-1-e.htm. (accessed: 19 Sep 2023).

NATO Civil-Military Cooperation (CIMIC) Doctrine (AJP-9). 2003. URL: https://www.nato.int/ims/docu/ajp-9.pdf. (accessed: 19 Sep 2023).

Allied Joint Doctrine for Civil-Military Cooperation (AJP-3.4.9 Edition A). 2013. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757583/archive_doctrine_nato_cimic_ajp_3_4_9.pdf. (accessed: 19 Sep 2023).

Allied Command Operations Manual (AM) 86-1-1 (ACO CIMIC Tactics, Techniques and Procedures). 2012. URL: https://www.handbook.cimic-coe.org/8.-annex/reference-docs/TTPs.pdf. (accessed: 19 Sep 2023).

Allied Command Operations. Civil-Military Co-operation Functional Planning Guide. 2017. URL: https://www.handbook.cimic-coe.org/8.-annex/reference-docs/Civil-Military%20Cooperation%20Functional%20Planning%20Guide.pdf. (accessed: 19 Sep 2023).

Олег ФАРІОН, д.військ.н., проф.
НАДПСУ ім. Богдана Хмельнитцького
ORCID: 0000-0001-6751-0468
E-mail: foleg71@ukr.net

ОБ'ЄКТИ ІНФОРМАЦІЙНОГО ВПЛИВУ СПЕЦСЛУЖБ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ НА БЕЗПЕКОВИЙ ПРОСТІР УКРАЇНСЬКО-МОЛДОВСЬКОЇ ДІЛЯНКИ ДЕРЖАВНОГО КОРДОНУ

В період підготовки до збройного вторгнення та під час бойових дій в Україні діяльність спецслужб Російської Федерації спрямовувалась на пошук нових способів дестабілізації обстановки як в Україні так і на її кордонах. З цією метою держава-агресор активно використовує наявний потенціал інформаційно-психологічних операцій та здійснює інформаційний вплив на розвиток негативних змін в обстановці на державному кордоні України.

За результатами аналізу безпекового простору українсько-молдовської ділянки державного кордону за період з 2022 по теперішній час встановлено, що спецслужби Російської Федерації створюють умови для поширення факторів, що ускладнюють обстановку через інформаційний вплив на:

пункти пропуску через державний кордон з метою порушення режиму їх функціонування через різке збільшення інтенсивності пасажиро-транспортного потоку;

громадян України призивного віку з метою ухилення їх від мобілізації, що збільшує кількість спроб незаконного перетину державного кордону як в пунктах пропуску так і поза ними;

населення прикордонних районів Придністровського сегменту державного кордону, що через закриття пунктів пропуску зумовлює збільшенню порушень державного кордону;

осіб, що проживають в прикордонних районах України та Республіки Молдови з метою отримання достовірної інформації про об'єкти спрямування та наслідки ракетних ударів і уражень ударними безпілотними повітряними суднами;

канали протиправної діяльності з метою поширення терористичної діяльності, контрабанди зброї, боєприпасів та вибухових речовин;

Придністровський регіон з метою створення сприятливих умов для проникнення екстремістів на територію України;

економічну ситуацію прикордонних регіонів України і Республіки Молдови з метою поширення контрабандної діяльності;

родинні зв'язки мешканців прикордонних регіонів з метою порушення державного кордону.

Таким чином, узагальнено основні об'єкти, за якими спецслужби Російської Федерації здійснюють інформаційний вплив на дестабілізацію прикордонної безпеки українсько-молдовської ділянки державного кордону.

Віталій ФЕДОРІЄНКО, к.т.н.
НУОУ
ORCID:0000-0002-0921-3390
E-mail: v.fedoriienko@edu.nuou.org.ua
Марія ПОДИБАЙЛО, к.і.н.
НУОУ
ORCID:0000-0002-4681-5753
E-mail: mariiapodybailo@gmail.com
Олег ТЕМНИЙ
НУОУ
ORCID:0009-0009-3173-094X
E-mail: o.temnyi@edu.nuou.org.ua

АСПЕКТИ ВИКОРИСТАННЯ OSINT ДЛЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙНИХ ДІЙ НА ТИМЧАСОВО ОКУПОВАНИХ ТЕРИТОРІЯХ

Сьогодні Україна зіткнулася із війною де основним вектором зусиль є боротьба з російським агресором. Для цього треба бути всіляко обізнаним про його діяльність і консолідувати це в знання щоб згуртувати усі сили оборони та населення України особливо на тимчасово окупованих територіях.

Очевидно, зазначену обізнаність можливо досягти шляхом залучення основних сил і засобів. І серед них – це консолідація використання спільних інструментів взаємодії між стратегічними комунікаціями та розвідки з відкритих джерел (OSINT).

Мета – висвітлення деяких шляхів спільного використання популярних інструментів та ресурсів в Україні, які набули поширення з початком повномасштабної російсько української війни на основі досвіду шляхів використання OSINT на тимчасово окупованих територіях України.

Головними аспектами розвідки з відкритих джерел сьогодні стає її зв'язок з іншими дисциплінами розвідки. Стратегічні комунікації є, певною мірою, "парасолькою" для п'яти дисциплін розвідки [1]:

HUMINT (Human Intelligence);
SIGINT (Signals Intelligence);
MASINT (Measurement and Signature Intelligence);
GEOINT (Geospatial Intelligence) + IMINT (IMAGERY Intelligence);
OSINT + CSINT (Closed-Source Intelligence) + Open SOCMINT (Social Media Intelligence).

Адже стратегічні комунікації та OSINT використовують схожі підходи та інструменти. Очевидно, що решта дисциплін розвідки можуть надавати інформацію, що є важливою для формування загальної оцінки інформаційного середовища. Саме це лежить в основі завдань стратегічних комунікацій.

OSINT-джерела часто поділяють на категорії потоку інформації: засоби масової інформації, інтернет, державні урядові дані, професійні та наукові публікації, комерційні дані, сіра література.

Враховуючи розвиток OSINT головна увага зосереджена на таких категоріях інформаційного потоку, як мас-медіа та інтернет. А також - на субдисципліни Social Media Intelligence - складовій OSINT.

Сьогодні, поняття "розвідки з відкритих джерел інформації" є майже повним синонімом інформації, яка надходить з інтернету.

За даними Finances Online, 93,4% користувачів Інтернету та 58,4% населення планети користуються соціальними мережами [2]. Ці цифри які вказують на майже повну охопленність інтернет користувачів та відносне число користувачів соціальних мереж. Наразі територія України має покриття мобільного зв'язку і відповідного інтернету, який є дешевим, а кількість абонентів становить у 1,5 рази більше за населення України.

Дослідження понятійного апарату розвідки з відкритих джерел є достатньо повним. В деяких теоретичних нових баченнях авторів з країн які є членами НАТО збігається з практикою в Україні [3]. Це стало яскраво відчутно після повномасштабного вторгнення російської федерації. Наприклад, у доктора Кіри Вірст [4] стратифікація демократизації розвідки щодо проводиться з урахуванням появи нових акторів - місцеве населення, медіа ведучі, та провайдери та вендори цих послуг на рівні національних і глобальних комерційних компаній. Вочевидь нові актори перебувають в умовах впливу росту даних, їх достатності, їх швидкості, та нових технологій їх використання. Це відбувається за типовими етапами, фазами та кроками відповідно до класичного циклу розвідки. Це все відповідає сучасній діяльності в Україні також.

Щодо демократизації розвідки в Україні, то Закон Про національну безпеку України (2018), по своїй суті, легалізує розвідку з відкритих джерел у суспільстві. Розвідувальні органи, сили цивільного захисту, а також громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки України перебувають під демократичним цивільним контролем.

Для загальної оцінки середовища в рамках стратегічних комунікацій необхідно врахувати усі під-середовища (Physical & Information environment, Land environment, Humans environment). Важливо оцінку інформаційного середовища здійснювати за шарами, які належать до трьох вимірів – когнітивного, віртуального та фізичного.

Страткому, доступ до семи шарів ГІС (Social, Cognitive, Virtual personal, Logical, Physical network, Physical, Geographical) потрібен частково, у частині формування ситуаційної обізнаності. Тому, що будь яка дія або бездіяльність має комунікативний ефект.

Якщо ми говоримо, наприклад, що війна ведеться а економічному фронті, то вона має для стратегії держави ключові ризики, аварійне відключення електрики чи газу має пряме відношення до військових також. Війна зараз має комплексний характер – змішаний, тобто має, гібридний.

Усі фахівці або власники цих шарів мають працювати зі стратегічними комунікаціями, а стратегічні комунікацій мають пронизувати їх mindset. Щоб вони розуміли, що це має вплив на національну безпеку країни та, в цілому, на безпеку людства.

Від час широкомасштабного вторгнення рф в Україну застосовуються воєнні дії щоб забезпечити саме це - безпеку людства. Адже сьогодні ЗСУ – на передньому рубежі оборони Європи. А Україна знищує самі загрози від росії – агресивна політика, де вони чітко говорять, що воюють з НАТО, ядерний шантаж, запуск балістичних ракет по об'єктам цивільної інфраструктури, у тому числі, по житловим багатоповерхівкам, удари по критичній інфраструктурі, атаки на різі країни, застосування хімічної зброї тощо.

Сьогодні, росія є причиною і створює загрозу для всього світу у тому числі в інформаційному просторі. Очевидно, що знищуючи цю загрозу Україна допомагаємо людству. Ці твердження є підтвердженням положень документів НАТО про те, що збройні сили захищають у першу чергу людей. А в Україні на під тимчасово окупованих територіях ворогом існує реальна катастрофа існування цивільного населення.

З оглядом на ретроспективу, стає зрозумілим, що на початку війни, росіяни, думали, у своїй більшості українці не будуть чинити спротив. Але і, наприклад, кияни цього не бачили в своєму майбутньому. Думка, про те, що цього нападу рф на Україну бути не може через низьку чисельність російськомовних громадян у Києві та Київській області, насправді, в українському суспільстві панувала з 2014 року. Тож, суспільство й експерти часто помиляються.

Під час війни сил розвідувальних структур часом стає недостатньо. Тому, на допомогу приходить розвідка з відкритих джерел для суспільства і від суспільства. Зазвичай OSINT сприймають, як інформацію зі ЗМІ. Наприклад, коли були окуповані Буча та Ірпінь – інформація від людей і в соціальних мережах була лише єдиним джерелом для прийняття рішення.

Що вважається сучасним OSINT-ом? Це не той OSINT про який всі знають з класичних джерел до початку російсько-української війни. Під час окупації територій противником поширеним явищем стало те, що військова розвідка не діставалася до всіх локацій, а розвідки з інтернету було недостатньо. Хто ще є носіями розвідки? Це суспільство – місцеве населення на тимчасово окупованих територіях. Саме воно відіграло вагому роль в успішному звільненні українських міст місцеве населення та соціальні мережі, де згадувалося про дії ворога, де їх штаб, де їх техніка, де ховаються місцеві жителі тощо.

Коли почалося вторгнення рф, першочергово силам оборони України потрібна була інформація та відповідні інструменти до цього. Якщо на певній території діяв підготовлений рух опору, то на іншій, де задіювали місцеве населення, – отримати структуровану інформацію ставало досить складно. Але при цьому був відсутній інтернет, і ворог впливав на навігаційні частоти. Відчувався значний морально-психологічний тиск і деморалізація на тимчасово окупованих територіях. Але треба розуміти, що для ворога – також. Бо цей ворог є на нашій землі.

Досить поширений в країнах-членах НАТО є веб ресурс https://osintframework.com (OSINT Фреймворк), який надає величезну кількість інструментарію, число яких має тенденцію до росту. Ця структура може бути ширшою чи видозміненою враховуючи особливості використання інструментів OSINT.

Зокрема, практичне використання досвіду інструментарію OSINT включає можливості щодо збору інформації для спостереження за активністю ворога на тимчасово окупованих територіях України та поширення цієї інформації між задіяними гравцями.

Досить часто робота ведеться з інформацією, яка не є доступною для усього суспільства, а лише для малих груп, зокрема в соцмережах. Часто маємо працювати на упередження, тобто забезпечити збір інформації на ранніх етапах.

Рекомендаціями можуть стати наступні кроки:

забезпечити знання інструментів OSINT серед суспільства;

проводити тренінги серед експертів та осіб, які приймають рішення щодо формалізації у аналізі та поширенні інформації в критичних умовах (загроза життю і здоров’ю, і відсутність зв'язку);

створити позаштатні групи щодо обробки різнорідних даних за визначеними правилами від місцевого населення;

впроваджувати спільні алгоритми потоку інформації;

поширювати правила боротьби з дезінформацією;

спонукати до проактивного реагування;

переглянути поняття OSINT.

Отже, було визначено місце стратегічних комунікацій, комунікативних структур, і розвідки OSINT. Також, був відзначений взаємний зв’язок між

суспільством та особами, які приймають рішення за допомогою підходів OSINT. При цьому була відзначена роль стратегічних комунікацій.

Список використаних джерел

1. RAND analysis. RAND RR1964-2.1.
2. Williams, H., & Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise.
3. Kira Vrist Rønn, The ‘Democratization’ of Intelligence, Conference “War and Intelligence in the Information Age”, NDUC, Oslo, 2022.
4. DPKO-DFS Policy on Peacekeeping Intelligence, United Nations Department of Peacekeeping Operations / Department of Field Support. – 2019.
5. Conceptual Framework by Hague Centre for Strategic Studies (2021).
6. Van Haaster et al., “Manoeuvring and Generating Effects in the Information Environment”.
7. Communication Strategy of the AFU 2023, Kyiv, (Order of HQ AFU №943 Feb 22, 2022).
8. Low of Ukraine “On Cloud Services” Document 2075-IX, valid, Feb 17, 2022.

Максим ЦВІЛЬ
ORCID: 0009-0007-8099-9115
E-mail: maxxx0351@gmail.com

АНАЛІЗ ЧИННИКІВ, ЯКІ ВПЛИВАЮТЬ НА ЦИВІЛЬНО-ВІЙСЬКОВЕ СПІВРОБІТНИЦТВО ЗБРОЙНИХ СИЛ УКРАЇНИ

2014 рік датується роком початку збройної агресії російської федерації проти України, саме цей рік заставив переосмислити та перепрацювати нові (до того часу невідомі Збройним Силам України) виклики, ризики, загрози та вимоги сучасних війн.

Цей воєнний конфлікт, на території Донецької і Луганської областей, окупація російською федерацією півострову АР Крим змусили змінити погляди військово-політичного керівництва нашої Держави на ведення воєнних дій у різних формах застосування ЗС України та інших складових сил оборони. Російські наративи та пропаганда настільки глибоко проникли у свідомість місцевого населення, що навіть до початку агресії рф, за результатами соціологічного опитування проведеного Київським міжнародним інститутом соціології у 2014 році, на пряме запитання про необхідність “від'єднання від України та приєднання до росії” у тей період 30% опитуваних у Луганській області і 28% - у Донецькій відповіли позитивно. Це призвело до опору місцевого

населення, протидії своїм військам, сприянні ворогу, повної невизначеності чи байдужості до долі свого регіону. Таким чином початок Антитерористичної операції, використання агресором не тільки військових формувань, а ще й цілого комплексу невійськових методів протидії та боротьби, світовий досвід ведення бойових дій, підштовхувало керівництво ЗС України до створення надійного механізму тісної взаємодії між цивільною і військовою складовою суспільства, що ґрунтувався б на принципах довіри та поваги до своєї армії. Таким механізмом стали підрозділи цивільно-військового співробітництва (Civil Military Cooperation), які увійшли до системи стратегічних комунікацій Збройних Сил України та Міністерства оборони України.

Отож основними завданнями цивільно-військового співробітництва (далі – ЦВС) відповідно керівних документів та документів НАТО являється:

підтримка дій своїх військ, це діяльність спрямована на зменшення впливу цивільного середовища на діяльність військ, а також забезпечення (за необхідністю) доступу військ до ресурсів та об’єктів цивільного середовища;

налагодження цивільно-військової взаємодії між військовим командуванням та об’єктами цивільного середовища;

підтримка об’єктів цивільного середовища, тобто робота направлена на своєчасне відновлення порушених спроможностей в інтересах виконання завдань військами;

Повномасштабне вторгнення російської федерації 24.02.2022 року підтвердило, що чинники в ході проведення заходів ЦВС здебільшого залежать обстановки та умов, що склалися, тому і мають визначатися, виходячи з оцінки цивільного середовища на тактичному та оперативному рівнях [4].

Так виконання завдань ЦВС було зумовлено значною динамікою подій на фронті (стрімкий захват територій противником, перехід від оборонних до наступальних (контрнаступальних) дій і навпаки, евакуація цивільного населення, тощо), що вимагало від підрозділів ЦВС швидких дій, рішень та нестандартних способів дій.

Чи не вперше після 2014 року робота підрозділів ЦВС зумовлювалася настільки значним інформаційно-психологічним впливом ворога, не тільки на місцеве населення, а й на органи державної влади. Ворог використовував весь свій агітаційно-пропагандистський арсенал, а в регіонах де його було недостатньо вдавався до звичних рф заходів: розповсюдження чуток, залякування, дезінформація, маніпулювання, тощо. В деяких випадках навіть після де окупації Українською армією окремих територій, слід російської інформаційної присутності залишався.

Отож такий чинник як інформаційний чи інформаційно-психологічний вплив рф в майбутньому має бути в подальшому врахований під час виконання завдань ЦВС та під час їх визначення. Для забезпечення ефективності виконання заходів ЦВС має бути досягнута взаємодія структури ЦВС з іншими складовими

стратегічних комунікацій (інформаційно-психологічні операції, зв'язки з громадськістю, та іншими).

Під час планування або виконання заходів ЦВС значну увагу слід приділяти не просто інформуванню в розділі стратегічних комунікацій об'єктів ЦС, а саме інформаційному впливу на них. Найоптимальніше визначення якого на мою думку запропоноване [3] і представляє вплив на підсвідомість особи чи населення або їх свідомість з ціллю внесення змін в їх світогляд і поведінку. Базовими методами якого є переконання та сугестія (навіювання).

Для успішного виконання завдань в ході інформаційного впливу слід враховувати, що методи переконання мають бути доступними для інтелекту та рівня об'єкту впливу та мають спиратися на загальновідомі факти (або ті що легко перевіряються). Переконання мають містити узагальнені пропозиції для об'єкта впливу і складатися з несуперечливих конструктивів та мати емоційне забарвлення.

Список використаних джерел:

Український соціологічний журнал. 2017. № 1-2.

СП 9-00(01).01 Доктрина "цивільно-військового співробітництво"

Історія інформаційно-психологічного протиборства: підручник заг. ред. Є.Д. Скуліша.

Тимчасова інструкція з оцінки цивільного середовища, затверджена наказом Генерального штабу від 24.04.2019 року № 159.

Вадим ЯКОВЕНКО, д.т.н., доц.
ORCID: 0000-0001-8591-6998
E-mail: yakob@ukr.net
Наталія ФУРМАНОВА, к.т.н., доц.
НУ "Запорізька політехніка"
ORCID: 0000-0002-8670-2948
E-mail: nfurmanova@gmail.com

МЕТОДИКА ВИБОРУ ЗАСОБІВ УКРИТТЯ ЦИВІЛЬНОГО НАСЕЛЕННЯ ВІД АТАК РАКЕТАМИ ТА УДАРНИМИ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

В умовах збройної агресії російської федерації (рф) проти України актуальною проблемою є захист цивільного населення в міських районах, які не зазнають воєнних дій. рф використовує це обставину для атак на дітей, жінок і літніх людей за допомогою ракет і ударних дронів, які атакують мирні міста.

Питання щодо створення інфраструктури, що здатна забезпечити захист від смертей і травм, потребують негайних відповідей. Необхідно негайно створити фонд захисних споруд по всій державі.

Формування фонду захисних споруд можна здійснити через:

виконання вимог інженерно-технічних заходів цивільного захисту у частині будівництва (пристосування) захисних споруд та споруд подвійного призначення на підставі відповідних розділів (схем) містобудівної та проектної документації об'єктів будівництва;

комплексне використання підземного простору міст і інших населених пунктів для розміщення соціальних, виробничих та господарських споруд;

створення та облік існуючих споруд подвійного призначення та примітивних укрить, а також об'єктів іншого призначення, які експлуатуються, включаючи підземні та наземні будівлі, гірські роботи та інші підземні приміщення;

будівництво швидкозбірних захисних споруд та облаштування примітивних укрить;

забезпечення наявністю та утриманням спеціальних конструкцій для швидкого монтажу та використання захисних споруд, зокрема, блок-модульного типу, через їх попереднє придбання або виготовлення в мирний час.

З метою планування вибору засобів цивільного захисту населення необхідно розробити методологічний підхід для аналізу початкових даних та вибору критерію оптимальності.

Для визначення узагальненого показника лінійної моделі вибору засобів укриття в умовах атак ракетами та ударними дронами в міських районах, проводиться розрахунок узагальненого критерію оптимальності у вигляді коефіцієнтів формування регресії.

Для оцінки вибору засобів укриття потрібно мати набір фізичних (технічних) характеристик цих засобів, які мають величини та ознаки, що дозволяють оцінити їх надійність. Це вимагає створення і впровадження нової системи понять, яка базується на більш докладному обліку результатів захисту цивільного населення.

Вихідними даними для розрахунку є характеристика урбанізованості району та його інфраструктури [1]; наявний перелік засобів укриття та їх захисні властивості; тип літального об'єкту противника; кількісний стан цивільного населення та віковий показник.

Вагові критерії надають змогу визначити, наскільки окремі засоби є актуальними в конкретній ситуації, що підвищить ефективність планування вибору засобів укриття [2]. Використання розробленої методики дозволяє оцінити ймовірність ураження цивільного населення та вибору більш безпечних укрить.

Крім того, автори роботи вважають, що доцільно взяти до уваги досвід Ізраїлю і розглянути можливість відмови від майбутніх громадських укрить та переходу до індивідуальних укрить у власних житлах громадян України. Це пов'язано із тим, що час підльоту балістичних ракет вимірюється у хвилинах;

існує проблема ігнорування повітряних тривог у суспільстві; крім того, утримання колективних засобів укриття є складною та фінансово обтяжливою задачею.

Список використаних джерел:

1. Іщенко А. В., Кобець М. В. Засоби і методи виявлення вибухових речовин та пристроїв у боротьбі з тероризмом: навчально-практичний посібник – К.: Національна академія внутрішніх справ України, 2005. 144 с.

2. Yakovenko V., Volochiy B., Sydorenko Y., Furmanova N., Malyi O., Tkachenko A., Olshevskyi, Y. Building a model of the process of shooting a mobile armored target with directed fragmentation-beam shells in the form of a discrete-continuous stochastic system // Eastern-European Journal of Enterprise Technologies, 2021, 6(4 (114). P. 51–63.

СЕКЦІЯ 7: ІНШІ АСПЕКТИ РОЗВИТКУ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ

Ірина АНДРУСЯК, к.ю.н., доц.
НУ "Львівська політехніка"
ORCID: 0000-0001-6887-0510
E-mail: iryna.p.andrusiak@lpnu.ua

ДОМАШНЄ НАСИЛЬСТВО: ПРОБЛЕМИ АКТИВІЗАЦІЇ В ПЕРІОД КРИЗИ ДЕРЖАВНОЇ БЕЗПЕКИ

У початковий період повномасштабної агресії Росії спостерігалися суттєве збільшення чисельності випадки домашнього насильства. Вказане зумовлене тим, що соціально-побутові обставини є одними з ключових, що впливають на вказану проблему. Військові дії, перебування людини в арені бойових дій чи на території, яка "відносно безпечна" все ж провокує суттєвий психологічний стрес, що так само як і будь-яка кризова ситуація, лише поглиблює труднощі людей, які існували до війни. Джинан Уста, Хана Мурр і Рана Ель-Джарра (Jinan Usta, Hana Murr, Rana El-Jarrah) вказують, що зростання насильства відбувається через зростання напруженості в домогосподарствах, підвищені фактори ризику насильства для злочинця, економічних тягарів і обмеженого доступу постраждалих до послуг підтримки. Для війни всі ці чотири проблеми постають особливо гостро [1].

Перманентно вказане впливає на сферу індивідуального життя. Під час конфлікту домашнє насильство стає загальним явищем, яке є ще більш небезпечним, ніж у мирний час. Людям, які стали жертвами складніше знайти вихід – вони часто обмежені в переміщенні, у них немає кому звернутися за підтримкою, вони залишаються ще більш залежними від своїх агресорів, як фізично, так і матеріально.

Наш сьогоднішній день українське суспільство спостерігає тенденцію до поглиблення цього явища. Це пояснюється тим, що під час військового конфлікту люди втрачають навички спокійної взаємодії і збільшує вплив осіб, які мають фізичну перевагу, і вони хочуть її для вирішення конфліктів.

Нині слід вести мову про поступову нормалізацію ситуації в контексті потенціалу реагування держави, тобто відновлення публічного механізму запобігання та захист від домашнього насильства. Вказане зумовлено не тільки адаптацією людського організму до зовнішніх обставин інформаційної та військової загрози, але й нормалізацією роботи органів публічної влади, які виконують повноваження щодо охорони та захисту прав та свобод громадян. Насьогодні покращується реагування владних суб'єктів, зокрема, Національна

поліція України на випадки домашнього насильства, що змогли адаптувати свої методи діяльності до сучасних умов.

Однак за даними аналітиків “безпекова ситуація в українських родинах в умовах війни в кожному регіоні держави є різною. Приміром, виявлено, що в західних областях України, які порівняно з іншими не мають безпосередньої близькості до бойових дій, частіше фіксуються і розглядаються справи, що стосуються домашнього насильства. Наводиться статистика, що у Львівській області за підсумками першого півріччя 2022 року суди розглянули більшу кількість справ порівняно з іншими областями – 38%, в Києві – 27%” [2]. Особливо складні ситуації відбуваються на територіях з активними військовими діями, де реагування на випадки домашнього населення ускладнене.

Фахівці звертають увагу ще на одну проблему – збільшення кількості зброї, яка надходить до країни під час військового конфлікту, що значно збільшує ймовірність виникнення критичної ситуації, що спричинятиме домашнє насильство і ускладнює перебіг ситуації для жертв.

Окрім того в період стресових ситуацій зростають випадки алкоголізму, що є ще одним фактором для домашнього насильства. За даними австралійських фахівців від 24% до 54% інцидентів домашнього насильства, про які повідомили в поліцію, були класифіковані як пов’язані з алкоголем [3].

На жаль, проблема не зникне сама собою навіть після успішної перемоги України. Соціальне та економічне напруження підвищилось. Багато сімей вимушені шукати притулок у більш безпечних районах, і це часто обмежує їх простір. Деякі сім'ї втратили своє житло та роботу, тобто на зміну безпековим загрозам наступатиме економічна проблема, яка також є тригером для активації правової проблематики домашнього насильства.

Список використаних джерел:

1. Usta J., Murr H., El-Jarrah R.COVID-19 Lockdown and the Increased Violence Against Women: Understanding Domestic Violence During a Pandemic. *Violence and Gender*. 2021. Vol.8 Is. 3. P. 133-139.http://doi.org/10.1089/vio.2020.0069

2. Війна по обидві сторони фронту: чому бойові дії в країні посилюють агресію сімейних насильників. 7 листопала 2022. URL: https://nsirogozy.city/articles/248589/vijna-po-obidvi-storoni-frontu-chomu-bojovi-dii-v-kraini-posilyuyut-agresiyu-simejnih-nasilnikiv-

3. Mayshak R., Curtis A., Coomber K., Tonner L., Walke, A., Hyder S., Liknaitzky P., Miller P. Alcohol-Involved Family and Domestic Violence Reported to Police in Australia. *Journal of Interpersonal Violence*, 2022. Vol. *37*(3–4).P.1658–1685. https://doi.org/10.1177/0886260520928633

Андрій БУЛАЙТІС
НУЦЗУ
ORCID: 0000-0002-7128-4835
E-mail: bulaytiss@nuczu.edu.ua

ЩОДО ПИТАННЯ РОЗРОБКИ ПРОГРАМНО-АПАРАТНОГО СИМУЛЯТОРА ПРОФЕСІЙНО-ПСИХОЛОГІЧНОЇ ПІДГОТОВКИ ПІРОТЕХНІКІВ ДСНС

Після початку повномасштабної війни росії проти України Державна служба України з надзвичайних ситуацій (далі-ДСНС) зіткнулась з рядом нових викликів та завдань. Нагальним питанням сьогодення стала проблема гуманітарного розмінування території України. Всього, з початку широкомасштабного військового вторгнення російської федерації на території України, знешкоджено 429318 вибухонебезпечних предметів та 2892 кілограм вибухової речовини, у тому числі 3090 авіаційних бомб. Обстежено територію площею близько 94211 гектар. Найчастіше піротехнічні підрозділи працювали: в Харківській області 22700 разів, Київщині – 8706, Донеччині – 7888, Миколаївщині – 5958, Херсонщині – 7540, Чернігівщини – 4930, Сумщині – 2490, Черкащині – 1289 [1].

Такий великий обсяг робіт вимагає від фахівців піротехнічних підрозділів ДСНС приділяти більш значну увагу підготовці до бойових виїздів. Одним із основних завдань піротехнічних підрозділів є очищення місць ведення боїв від боєприпасів, які не детонували або не спрацювали за цільовим призначенням[2]. Виходячи з вищевикладеного виходить, що піротехніки потребують таких умов підготовки та тренувань, що будуть максимально наближені до бойових. На нашу думку, допомогти в цьому може створення програмно-апаратного симулятора для підготовки піротехніків ДСНС, що віртуально імітує реальне відчуття управління дроном чи виконання завдання для забезпечення максимально успішної практики [3]. Для саперів це може бути корисним починаючи з етапу вступу на службу до етапу безпосереднього відпрацювання навичок пошуку, транспортування та знешкодження вибухонебезпечних предметів.

Ось кроки та компоненти, які на нашу думку, можуть бути включені в програмно-апаратний симулятор:

1. Апаратна частина:

А) Віртуальні навчальні інструменти: у віртуальний симулятор включити різноманітні інструменти та обладнання, яке використовується піротехніками, такі як вибухові пристрої, інструменти для роботи з піротехнічними матеріалами, системи безпеки тощо. Ці інструменти мають віртуальну реалістичну модель і можуть бути керовані користувачем.

Б) Симуляція вибухів і пожеж: додати можливість симулювати вибухи та пожежі в контрольованому оточенні. Це дозволить практикувати процедури евакуації та гасіння пожежі без реальної небезпеки.

В) Віртуальне навчальне поле**:** створити віртуальне навчальне поле або тренувальний центр з різними сценаріями для тренувань, включаючи будівлі, транспортні засоби, ліси та інші місця, де можуть виникнути надзвичайні ситуації.

2. Програмна частина:

А) Віртуальна реальність (VR) або 3D-середовище: використання VR або 3D-моделі для створення іммерсивного навчального середовища дозволить піротехнікам отримати реалістичний досвід тренування.

Б) Сценарії тренувань: розробити різні сценарії надзвичайних ситуацій, які можуть включати вибухи, пожежі, рятувальні операції, обробку вибухонебезпечних предметів та інші завдання.

В) Система оцінювання: створити систему оцінювання та звітності, щоб підготовка піротехніків була ефективною. Це можливо зробити, з використанням відеозапису та даних з симулятора для оцінки виконання завдань.

3. Управління та інтерфейс:

А) Керування інтерфейсом: розробити зручний інтерфейс для користувачів, щоб вони могли взаємодіяти з симулятором і керувати віртуальними інструментами.

Б) Можливість налаштувань: надати можливість налаштування параметрів тренувань, включаючи складність сценаріїв та будь-які додаткові параметри з можливістю різноманітних комбінацій.

4. Безпека:

Завжди слід звертати увагу на безпеку при роботі з будь-якими стимуляторами, оскільки це може бути небезпечно. Тренування повинно проводитися під наглядом кваліфікованих інструкторів та включати заходи безпеки для попередження травм та нещасних випадків.

5. Навчання та підтримка:

А) Навчання користувачів: проводити навчання піротехніків з використання симулятора та інструкції з безпеки.

Б) Технічна підтримка: розробити систему технічної підтримки для вирішення можливих проблем користувачів та вдосконалення програмно-апаратного забезпечення.

Наведені вище кроки та компоненти – лише приблизний перелік того, що можливо зробити для розробки програмно-апаратного симулятора. Актуальність цього питання є вкрай важливим та вимагає від нас продовжувати роботу в цьому напрямку для збереження життя та покращення навчання піротехніків ДСНС.

Список використаних джерел:

1. Інформація щодо діяльності піротехнічних підрозділів ДСНС. https://dsns.gov.ua/uk. URL: https://dsns.gov.ua/uk/news/nadzvicaini-podiyi/informaciia-shhodo-diialnosti-pirotexnicnix-pidrozdiliv-dsns-168 (дата звернення: 13.09.2023).
2. Про затвердження Порядку здійснення першочергових заходів щодо знешкодження (знищення) вибухонебезпечних предметів на території України та організації взаємодії під час їх виконання. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/z0014-23#Text (дата звернення: 14.09.2023).
3. ELAKPI: Програмно-апаратний симулятор для підготовки операторів БПЛА. ELAKPI: Home. URL: https://ela.kpi.ua/handle/123456789/49603 (дата звернення: 14.09.2023).

Ганна ЄРШОВА,
слухач НУОУ
ORCID: 0009-0002-5774-3967
E-mail: annasanina887@gmail.com

АНАЛІЗ ЧИННИКІВ, ЯКІ ВПЛИВАЮТЬ НА ЗАХОДИ ПСИХОЛОГІЧНОГО ВПЛИВУ

Актуальність проведення аналізу чинників, які впливають на заходи психологічного впливу, обумовлена стрімкістю змін умов обстановки як на полі бою, так і в інформаційному просторі. Швидкість змін обстановки призводить до необхідності детального та перманентного аналізу чинників, що впливають на ефективність проведення психологічної операції. Ефект від проведення психологічної операції напряму залежить від якості та ефективності підготовки та ведення заходів психологічного впливу а також врахування чинників, які на це впливають.

Аналіз останніх досліджень і публікацій [2–3] показує, що одним з основних чинників, що можуть впливати та впливають на ефективність та результативність заходів психологічного впливу є оцінка інформаційної обстановки, яка здійснюється емпірично та теоретично. Сутність емпіричного оцінювання полягає в отриманні вихідних даних із усіх можливих джерел та їх первинна обробка. В ході теоретичного оцінювання здійснюється поглиблений аналіз вихідних даних і формування висновків по елементах та в цілому, в тому числі побудова моделі обстановки, її дослідження з виявленням тенденцій зміни ситуації на найближчий та віддалений проміжок часу.

У роботі [2] наголошується, що при аналізі чинників, які впливають на ефективність проведення заходів психологічного впливу, першочерговим є важливість врахування фактору високої динамічності змін в обстановці та оцінка інформаційної обстановки. Однак, відповідні твердження потребують уточнення. Зокрема, на практиці доведено, що одним з основних чинників, що безпосередньо впливають на заходи психологічного впливу це дії противника, а саме інформаційно-психологічний вплив противника на населення та особовий склад Збройних сил України.

Зважаючи на зазначене, **метою тез є** аналіз чинників, які впливають на ефективність заходів психологічного впливу, а саме інформаційно-психологічного впливу противника, що дозволить якісно нівелювати відповідний вплив та безперешкодно проводити заходи психологічного впливу в інтересах операції Сил оборони України.

Виклад основного матеріалу. На основі аналізу чинників, що впливають на заходи психологічного впливу, а також беручи до уваги досвід планування та проведення заходів психологічного впливу, можна констатувати, що основним чинником є дії противника, а саме інформаційно-психологічний вплив противника. Передусім інформаційно-психологічний вплив противника спрямований на особовий склад Збройних Сил України та підрозділи, що здійснюють підготовку та проведення психологічного впливу, зокрема. Основними методами відповідного деструктивного впливу є навіювання та дезінформація.

Метою здійснення інформаційно-психологічного впливу противника на особовий склад Збройних Сил України є формування, підтримання у їх свідомості соціальних ідей, поглядів, уявлень, переконань, негативних емоцій і почуттів, які спрямовані на виведення зі строю військовослужбовців та унеможливлення ними якісно виконувати завдання.

З метою проведення ефективної протидії інформаційно-психологічному впливу противника, доцільно детально розібрати основні методи впливу противника. Так, навіювання – це найпоширеніший метод, який здійснюється шляхом залучення всіх сил і засобів противника, як військових, так і загально національних медіа засобів. Навіювання здійснюється як на особовий склад Збройних сил, так і населення України.

Проаналізувавши меседжи, що поширюються противником та є елементом інформаційно-психологічного впливу, доречно виділити основні напрямки навіювання, зокрема:

формування невдоволення діями політичного і військового керівництва;

переконання в безперспективності здійснення заходів спрямованих на захист країни від агресії рф;

залякування загрозою життю та здоров’ю;

провокування протестних настроїв в суспільстві за допомогою імітації наявності політичних, релігійних, міжетнічних, культурних, соціальних протиріч.

До основних напрямків дезінформації можна віднести наступні:

хибне висвітлення та перекручення інформації щодо заходів, які здійснює політичне та військове керівництво;

підрив міжнародного авторитету держави, ускладнення її співпраці з країнами-партнерами;

дискредитація та дегуманізація Збройних Сил України шляхом викривлення інформації, що стосується ведення бойових дій.

Перелічені напрямки інформаційно-психологічного впливу є результатом діяльності системи органів інформаційної боротьби противника та національної мережі засобів масової інформації, які діють за вказівками та наказами вищого військово-політичного керівництва російської федерації.

З метою якісної оцінки та подальшого нівелювання фактів здійснення інформаційно-психологічного впливу противника на особовий склад Збройних Сил України, що є ключовим чинником, який впливає на заходи психологічного впливу, доцільно проаналізувати приклади інформаційно-психологічного впливу, які мали найбільшу ефективність. Так, на особовий склад Збройних Сил України безпосередньо впливає інформація спрямована на дискредитацію та дегуманізацію Збройних Сил України.

З боку російської федерації перманентно поширюється дезінформація щодо незадовільної підготовки військовослужбовців, недостатнього матеріально-технічного забезпечення, некомпетентності командного складу, постійного знищення західних зразків озброєння та військової техніки, масової здачі в полон українських військових тощо. Відповідний інформаційно-психологічний вплив противника спрямований на зниження морально-психологічного стану та бойових спроможностей особового складу, а також зниження привабливості приєднання до Збройних сил цивільного населення. Прикладом інформаційно-психологічного впливу є поширення фейків, які вражають своєю безглуздістю, а саме активного поширення на російських пропагандистських каналах поширення інформації набули твердження, що “нацисти ЗСУ заварюють люки танків, щоб екіпаж йшов у наступ і не мав змоги здатися в полон”; “українські військові через великі втрати замість медичної допомоги забирають органи у поранених та залишають їх помирати”.

Запорукою успішної протидії інформаційно-психологічному впливу є формування критичного сприйняття. Враховуючи той факт, що російська федерація веде тривалу інформаційно-психологічну операцію, вона сформувала мережу засобів впливу, що діють в інформаційному середовищі України. Щоб ефективно протидіяти деструктивному інформаційно-психологічному впливу, ми

маємо виокремити пропагандистські ресурси та навчити суспільство критично сприймати інформацію.

Висновки. В умовах ведення активних бойових дій та високої інформатизації суспільства інформаційно-психологічний вплив противника, який впливає на проведення психологічної операції, може змінюватися постійно, а швидкий його аналіз та врахування у проведенні операції є критичним для швидкості прийняття та реалізації життєво важливих рішень. Таким чином, аналіз інформаційно-психологічного впливу та протидія є важливою складовою підготовки до проведення заходів психологічного впливу та ключовим елементом загальної системи інформаційної безпеки.

Список використаних джерел

1. Кацалап В. О., Кирпічніков О. Д., Саунін Р. Д. Методичний підхід до оцінювання рівня інформаційно-психологічного впливу противника в інтересах інформаційної операції Збройних Сил України, URL: https://doi.org/10.33099/2304-2745/2022-3-76/24-31
2. Пєвцов Г. В., Залкін С. В., Сідченко С. О., Хударковський К. І. Інформаційно-психологічні операції планування, протидія, технології// Монографія. Харків 2020. С. 41-45, 135-140.
3. Кацалап В. О., Сніцаренко П. М., Саричев Ю. О. Методичний підхід до визначення критеріїв оцінки рівня інформаційного впливу на елементи інформаційної інфраструктури воєнної організації держави // Збірник наукових праць в/ч А1906. 2011. № 31. С. 126–139
4. Дзюба М.Т., Жарков Я.М., Ольховой І.О., Онищук М.І. Нарис теорії і практики інформаційно–психологічних операцій // Навчальний посібник. Київ 2006.

Віталій КАЦАЛАП, к.в.н., доцент,
НУОУ
ORCID: 0000-0003-4804-8022
E-mail: v.katsalap@edu.nuou.org.ua

КОГНІТИВНА БЕЗПЕКА В УМОВАХ ВІДБИТТЯ ШИРОКОМАСШТАБНОГО ВТОРГНЕННЯ рф

На сучасному етапі розвитку суспільства, пов'язаного з масовим використанням інформаційних технологій виникає необхідність формування когнітивної безпеки керівника (начальника). Це питання пов’язане з процесами створення дієвої системи інформаційних заходів. Значну увагу цьому питанню

приділяється в діяльності Міністерства оборони України та Збройних Сил України.

Сьогодні когнітивної безпеки керівника (начальника) є часнтною його світогляду, який формує медіа-, кібер-, діджитал- та комунікаційно-контентна складові його діяльності [1].

В умовах повномасштабного вторгнення основними завданнями реалізації когнітивної безпеки можна вважати:

супроводження інформаційними засобами виконання завдань оборони України;

підтримання зв'язків МО України та ЗСУ з українськими та іноземними засобами масової інформації щодо висвітлення ситуації в усіх операційних районах відсічі збройної агресії;

протидію спеціальним інформаційним операціям, спрямованим проти Збройних Сил України та інших військових формувань;

донесення достовірної інформації до військовослужбовців Збройних Сил України, інших військових формувань, зокрема через засоби масової інформації Збройних Сил України.

Крім того, варто звернути увагу на так званий “дезінформаційний тиск” на військово-політичне керівництво нашої країни. Тому протистояння дезінформації рф потребує взаємодії з інформаційними ресурсами країн, які підтримують Україну, спрямовуючи та координуючи спільну роботу не тільки на роз’яснення поточних російських інформаційних акцій, а й на їх упередження та активну протидію.

Засоби масової інформації та Інтернет контролюються патріотично налаштованими людьми що впливає на об’єктивність висвітлення інформації та формування української нації.

Іншим напрямком в цій сфері може бути подальше підвищення спроможностей підрозділів, що відповідають в системі заходів МО України та Збройних Сил України за інформаційну безпеку, кібербезпеку та підтримання стратегічних комунікацій [2].

Важливою тенденцію останніх місяців є інтенсивності інформаційних заходів рф. Це призводить до формування у керівників (начальників) хибної думки, що Україна поступово втрачає підтримку європейської спільноти щодо західної орієнтації, більшість європейських країн визнає статус Криму як частини Росії. На відміну - США, Великобританія (не є членом ЄС), Канада, Австралія та Ізраїль продовжують підтримку прозахідних прагнень України та не визнають анексію Криму.

В ЄС зростає розкол, в тому числі і на тлі інформаційного впливу РФ, що приводить до збільшення рівня неконтрольованої міграції. У зв'язку із цим декілька країн розглядають питання щодо можливості виходу зі складу союзу.

В подальшому недосягнення мети інформаційної кампанії з руйнування української державності при зниженні підтримки України ЄС, може привести до поширення воєнної агресії рф проти України.

Для виправдання перед світовою спільнотою відкритого вторгнення угруповань збройних сил рф на територію України, ймовірно, буде здійснюватися активізація інформаційних впливів:

шляхом проведення провокацій, спрямованих на дискредитацію ЗС України в очах міжнародної спільноти та місцевого населення шляхом фальсифікації фактів щодо використання важкого, забороненого домовленостями озброєння, випадків свавілля та безчинств українськими військовослужбовцями на території Донецької, Луганської, Запорізької, Миколаївської та Херсонської областей;

водночас, з метою дестабілізації соціально-політичної обстановки в інших регіонах України, буде активізуватися діяльність проросійських організацій і рухів у південних і східних регіонах, провокуватимуся акції протесту і непокори, невдоволення політикою керівництва України, чим можливо будуть створені панічні настрої серед окремих верств населення та сформований імідж РФ, як "держави-миротворця".

Отже, сьогодні основне завдання системи забезпечення інформаційної безпеки МО України та Збройних Сил України полягає у цілеспрямованому формуванні когнітивної безпеки керівника в основі якої є об'єктивна оцінка інформації. Але самої оцінки інформації є недостатньо. Тому потребує дослідження певні обмеження, які дозволять визначитись із ефективними заходами протидії інформаційним загрозам росії.

Список використаних джерел

1. Інформаційно-аналітичні матеріали до проекту попереднього опису майбутнього безпекового середовища «Майбутнє без пекове середовище 2030. Аналіз стратегічного передбачення». – К.: ЦНДІ ЗСУ, 2019. – 37 с.

2. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства Аналітичний документ. Київ, 2018. – [Електронний ресурс]. – Режим доступу: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf.]

Юлій КОНДРАТЕНКО, д.ф.
НУОУ
ORCID:0000-0002-9575-5101
E-mail:crack1980@ukr.net

ПЕРЕВІРКА АДЕКВАТНОСТІ МЕДІА ІНФОРМАЦІЇ ЩОДО ОЦІНОК СПРОМОЖНОСТЕЙ ЗРАЗКІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ З ВИКОРИСТАННЯ МЕТОДУ ГРУПОВОГО ВРАХУВАННЯ АРГУМЕНТІВ

Оцінка сучасного стану та перспектив розвитку безпекового середовища у світі свідчить про підвищення рівня агресивності деяких країн, що змушує вносити певні корективи щодо сталого розвитку необхідних оборонних спроможностей. Однією з таких країн-агресорів, яка, використовуючи інформацію в якості потужної зброї впливу на світогляд суспільства, є російська федерація, яка спровокувала та розпочала повномасштабну збройну агресію проти України.

Як ми бачимо з досвіду поточних подій на теренах України, основними засобами впливу, окрім газової та енергетичної дестабілізації, є засоби вогневого ураження, тобто множина основних зразків озброєння та воєнної техніки, яка зараз використовується як для залякування європейських країн та країн-членів Північноатлантичного Альянсу через пропагандистські медіа канали, так і для реального вогневого ураження критичної інфраструктури нашої країни.

З аналізу робіт [1] щодо розповсюдження кремлівської пропаганди, можна прийти до висновку щодо достатньо високого рівню неадекватності інформації, яка широко розповсюджується засобами пропагандистських медіа російської федерації, що може свідчити і про низький рівень адекватності оцінок спроможностей основних зразків озброєння та військової техніки (далі ОВТ), які відкрито висвітлюються як в якості реклами, так і в якості шляхів залякування своїх можливих суперників. Це наводить нас на потребу у використанні існуючих або розробки нових методів та методичних підходів для оцінювання адекватності наявних у відкритих джерелах масової інформації оцінок спроможностей основних зразків ОВТ противника.

Для перевірки адекватності наявних оцінок ОВТ(для прикладу висвітлених рангів сучасних зразків танків [2]), які в подальшому формують нав’язану картину щодо можливостей, які можуть суттєво відрізнятися від реальності, автором запропоновано використовувати метод групового врахування аргументів [3].

Даний метод дозволяє побудувати комплексну математичну модель оцінювання типових зразків ОВТ, яка будується за рахунок використання сукупності апріорних статистичних даних щодо кількісно-якісних характеристик цих зразків та наявних їх інтегральних оцінок (рангів).

Метод широко використовується з використанням комп’ютерних технологій, які забезпечують можливість оперативно обробити великий обсяг можливих

комбінацій функцій-претендентів, побудованих комбінаторним методом сполучення, кращі з яких за обраними критеріями поєднуються за рахунок адитивної згортки. Функції-претенденти включають в себе набір факторів (характеристик ОВТ), які здійснюють певний вплив на оцінку зразків ОВТ (її ранг). При згортці функцій-претендентів, необхідно перевіряти їх на явище мультиколінеарності, яка характеризується високою міжфакторною кореляцією, які можуть давати неякісні та неадекватні оцінки при використання загальної математичної моделі, а також на гетероскедастичність, наслідки якої можуть проявитись в різких стрибках значень оцінок при зміні значень характеристик зразків ОВТ, які потребують оцінювання.

Така математична модель формується за рахунок виявлення закономірностей між наявними характеристиками зразків ОВТ, та апріорними оцінками, сформованими експертами в даній області. Порівняння оцінок, отриманих за рахунок математичної моделі з значеннями оцінок, які висвітлені засобами пропагандистських медіа може дати відповідь на реальну їх адекватність.

Список використаних джерел:

1. Юськів Б. М. Аналіз прихованих тем пропаганди Кремля в Україні / Б. М. Юськів, Н. П. Карпчук // Політичне життя. – 2022. – № 1 (2022). – С. 160–171. DOI: https://doi.org/10.31558/2519-2949.2022.1.19.

2. Липатова Е. Неуязвимые: самые мощные танки в мире, которые сейчас находятся на вооружении [Електронний ресурс], 2021. - Режим доступу: https://bit.ly/3sIwtP9ю

3. Ивахненко А.Г. Моделирование сложных систем: (информационный подход). / А.Г. Ивахненко - К.: Вища шк. Головное изд-во, 1987. – 63 с.

Михайло КУХАРЧУК
Слухач навчальної групи 8204
Інститут стратегічних комунікацій
НУОУ
ORCID: 0009-0006-4888-9277
E-mail: manuchakpotapov@gmail.com

АНАЛІЗ ЧИННИКІВ, ЯКІ ВПЛИВАЮТЬ НА ПІДГОТОВКУ ІНФОРМАЦІЙНОГО ВПЛИВУ В ІНТЕРЕСАХ ЗБРОЙНИХ СИЛ УКРАЇНИ

Російська Федерація активно застосовує гібридні методи боротьби, де інформаційний компонент є ключовим. Розуміння чинників, які впливають на підготовку інформаційного впливу, допоможе Збройним Силам України (далі –

ЗСУ) ефективніше протистояти інформаційному агресору. Адекватний аналіз дозволяє покращити не тільки інформаційну стратегію, але й загальну обороноздатність країни, інтегруючи інформаційні дії в загальний план оборони.

Аналіз останніх досліджень і публікацій [1-3] показує, що на сьогодні підготовка заходів інформаційного впливу в інтересах ЗСУ є недосконалою.

Зважаючи на зазначене, метою тез доповіді є аналіз чинників, які впливають на підготовку інформаційного впливу в інтересах ЗСУ.

Аналіз чинників, які впливають на підготовку інформаційного впливу в інтересах ЗСУ є ключовим для розуміння сучасних тенденцій в інформаційній війні. Відповідна стратегія і тактика інформаційного впливу можуть сприяти ефективності воєнних дій.

Чинник №1: Технологічний розвиток

Сучасні технології надають можливість швидкої та ефективної дистрибуції інформації. Це означає, що ЗСУ можуть використовувати різні платформи (соціальні мережі, месенджери, веб-сайти тощо) для передачі потрібного послання в цільовій аудиторії.

Завдяки технологіям аналізу великих даних (Big Data) ЗСУ можуть здійснювати ефективний моніторинг і аналіз інформаційного простору, прогнозувати реакції на різні події та операції.

Технології дозволяють не тільки атакувати, але й захищати. ЗСУ повинні вдосконалювати свої засоби захисту від інформаційних атак, шпигунських програм та інших кіберзагроз.

Штучний інтелект може бути використаний для розробки стратегій інформаційного впливу, а також для автоматизації процесу взаємодії з аудиторією.

Сучасні технології віртуальна реальність (VR) та доповнена реальність (AR) можуть бути використані для створення реалістичних тренувальних симуляцій, ефективного навчання військовослужбовців, а також як інструменти інформаційної війни.

Чинник №2: Стратегічна перспектива

Стратегічна перспектива допомагає визначити довгострокові цілі та завдання. Це орієнтир для всіх подальших дій, в тому числі для розробки контенту, визначення цільових аудиторій та вибору каналів комунікації.

Стратегічний підхід передбачає аналіз майбутніх тенденцій та загроз. Це дозволяє адаптувати інформаційну стратегію до змінюваних умов та використовувати вплив найефективніше.

Знання стратегічних пріоритетів дозволяє ефективно розподіляти ресурси, в тому числі час, людські та матеріальні ресурси, на найважливіші завдання та напрямки діяльності.

Стратегічна перспектива допомагає встановлювати та підтримувати партнерства на різних рівнях, від міжнародних альянсів до локальних співпрацюючих органів.

Збройні Сили, які мають чітку стратегічну перспективу, можуть швидко адаптуватися до змінних обставин. Вони не тільки реагують на події, але й антиципують їх, завдяки чому інформаційний вплив стає більш передбачуваним та контрольованим.

Стратегічний підхід забезпечує систематичний моніторинг та оцінку ефективності інформаційного впливу. За результатами такого аналізу стратегію можна коригувати для досягнення кращих результатів.

Чинник №3: Психологічна підготовка

Психологічна підготовка допомагає зрозуміти, як індивіди сприймають інформацію, які емоції та реакції вона може викликати. Це дозволяє військовим спеціалістам формувати повідомлення таким чином, щоб вони були максимально ефективними.

Знання психологічних особливостей цільової аудиторії дозволяє розробляти стратегії впливу, які враховують ці особливості, щоб створити бажаний ефект.

Психологічна підготовка допомагає військовослужбовцям розуміти психологічні та емоційні реакції на різні ситуації, що підвищує їх стійкість до інформаційного впливу ворога.

Психологічні знання допомагають формувати зрозумілі, переконливі та ефективні повідомлення, що відповідають сприйняттю та потребам аудиторії.

У зонах конфліктів військовослужбовці можуть зіткнутися з травматичними подіями. Психологічна підготовка допомагає їм краще справлятися зі стресом, що забезпечує більшу стабільність і впевненість у діях.

У місцях військових операцій важливо взаємодіяти з місцевим населенням. Психологічна підготовка допомагає розуміти його потреби, культурні та соціальні особливості, що сприяє позитивному сприйняттю та співпраці.

Чинник №4: Інформаційна безпека

Основна мета інформаційної безпеки - забезпечення конфіденційності, цілісності та доступності інформації. ЗСУ повинні мати змогу надійно захищати свої комунікаційні канали та джерела інформації від небажаних втручань, шпигунства та саботажу.

Інформаційна безпека допомагає виявляти та контрувати спроби дезінформації або пропаганди, які можуть бути спрямовані проти Збройних Сил або населення країни.

У разі порушення інформаційної безпеки необхідно швидко та ефективно відновлювати системи та процедури, щоб забезпечити неперервний інформаційний вплив.

ЗСУ, які можуть гарантувати інформаційну безпеку, користуються більшою довірою з боку населення, союзників та партнерів. Це підвищує їхню здатність до ефективного інформаційного впливу.

Інформаційні системи і мережі є основними каналами для розповсюдження інформації. Інформаційна безпека включає в себе захист від вірусів, зломів, шпигунських програм та інших кіберзагроз.

Освічені та підготовлені військовослужбовці будуть краще розуміти значення інформаційної безпеки, її принципи та методи захисту. Це підвищує загальний рівень інформаційного захисту в усьому військовому органі.

Чинник №5: Законодавча база

Законодавство визначає рамки допустимої діяльності для Збройних Сил у сфері інформації, створюючи зрозумілі межі та обмеження.

Законодавство може забезпечувати основу для захисту важливої інформації, визначаючи, яка інформація є конфіденційною або секретною.

Якщо інформаційний вплив проводиться неналежним чином або порушує права інших осіб, законодавча база встановлює механізми відповідальності та покарання.

Законодавча база також відображає міжнародні зобов'язання країни у сфері інформаційної безпеки та прав людини, встановлюючи стандарти для внутрішньої діяльності.

Правильно сформульоване та реалізоване законодавство додає легітимності діяльності Збройних Сил у сфері інформації, підтримуючи довіру громадськості.

Отже аналіз чинників, які впливають на підготовку інформаційного впливу в інтересах Збройних Сил України, дозволяє розробити ефективні стратегії та методи для захисту та просування інтересів держави в інформаційному просторі. Врахування технологічних тенденцій, стратегічних перспектив, психологічних особливостей, інформаційної безпеки та законодавчої бази є ключовими для успіху в сучасних умовах інформаційної війни.

Список використаних джерел

1. Матіос А. В. Небойові втрати української армії за два роки проведення АТО. URL: http:// matios.info/uk/novini/nebojovi-vtraty-ukrayinskoyi-armiyi-za-dva-roky-provedennya-ato (дата звернення: 20.10.2022).

2. Левченко О. В., Косогов О. М., Сірик А. О. Методика оцінювання кількісних показників негативного інформаційного впливу // Сучасні інформаційні технології у сфері безпеки та оборони. 2017. № 1 (28). С. 31–36.

3. Кацалап В. О., Сніцаренко П. М., Саричев Ю. О. Методичний підхід до визначення критеріїв оцінки рівня інформаційного впливу на елементи інформаційної інфраструктури воєнної організації держави // Збірник наукових праць в/ч А1906. 2011. № 31. С. 126–139.

Андрій ЛЕВЧЕНКО
НУЦЗУ
ORCID: 0009 0008 6465 6398
E-mail: andrusha.levchenko@gmail.com

ДО ПРОБЛЕМИ ПСИХОЛОГІЧНОГО СУПРОВОДУ СПОРТСМЕНІВ В УМОВАХ ВОЄННОГО СТАНУ

Військова агресія проти України, яка розпочалася із вторгнення російських військ, викликала неймовірні за силою навантаження на психіку всіх громадян держави, незалежно від віку, статі, соціального положення тощо. Під час війни реакція психіки людини буває різною: від помірного і тимчасового стресу до важких психічних травм, включаючи депресію та травматичні розлади.

Нами було досліджено певні аспекти зниження негативних наслідків, згаданих вище впливів, на психіку спортсменів, які продовжують захищати честь держави на міжнародних спортивних змаганнях та продовжують професійну діяльність у складних умовах обмежень та негативних впливів, які склалися в умовах воєнного стану, через технології спортивного психологічного консультування.

Серед факторів воєнного стану, які визначають виникнення негативних психічних наслідків, нами виділені не тільки загальновідомі, а й ті, що мають специфічне значення для даної категорії досліджуваних. Спортсмени мають продовжувати повсякденну професійну діяльність та показувати високі результати не у звичних умовах, а у відриві від родини, у нових місцях дислокації, у районах, де існує небезпека для життя, у нестандартних умовах організації тренувального процесу, з підвищеною відповідальністю за результати тощо.

Саме тому, ми звернули увагу на необхідність внесення певних змін до методологічних підходів та змісту спортивного психологічного консультування професійних спортсменів в умовах війни задля збереження фізичного, психологічного та соціального здоров'я, профілактики стресу та професійного вигорання.

Загальні теоретичні та певні практичні питання щодо реалізації сучасних технологій психологічного консультування особистісного розвитку спортсменів наведено у нашому сумісному дослідженні [1], у межах якого розглянуто основні завдання та підходи до спортивно-психологічного консультування з питань розвитку особистості тощо.

Нами з’ясовано, що у професійних спортсменів особистісно-професійний потенціал виступає як психологічний засіб подолання величезних фізичних і психічних навантажень у кризових періодах їхнього життя, які часто можуть супроводжуватися невротичними станами, емоційно-особистісними розладами, внутрішніми та міжособистісними конфліктами.

Тому, ми звернулися до висновків досліджень зарубіжних дослідників, які надають сучасне методологічне підґрунтя для змін у реалізації сучасного спортивного психологічного консультування з метою повернення у спортсменів, які пережили та переживають досвід життя та роботи під час війни, почуття стійкості і самоефективності, що має впливати на їхній подальший життєвий та кар'єрний розвиток.

Ми звернули увагу на висновки E. Wethington [2], який у дослідженні переломних психологічних моментів, які визначаються як випадок, коли людина зазнає серйозної трансформації у поглядах на себе та свою ідентичність, зауважує, що цей момент може зіграти для подальшого розвитку людини як позитивну так і негативну роль.

Саме тому, ми маємо сприяти, щоб спортсмени у воєнних умовах за допомогою психолога-консультанта поступово пристосовувалися до нової реальності, відновлювалися та у відповідь на стресові обставини і події відчували піднесення, немовби у них відкривається "друге дихання".

Цей висновок підтверджується і результатами дослідження [3], яке підкреслює важливість втрачених або відновлених ресурсів, самоефективності подолання та долаючої поведінки як важливих змінних у реакції на гостру катастрофу та подальше відновлення людини.

Тож, на нашу думку, у роботі зі спортсменами психологи-консультанти мають звертати додаткову увагу на те, що самоефективність подолання, яку виявляють спортсмени, може слугувати важливим внутрішньо особистісним фактором, який визначає те, як вони управляють втраченими ресурсами.

Використання зазначених вище підходів, на нашу думку, дозволить зменшити вплив негативних факторів воєнного стану на психіку спортсменів та інших категорій населення України.

Список використаних джерел:

1. Tomich L., Levchenko A., Girchenko O., Sikorska L., Nazarov O., Perelygina L. Psychological Counseling as a Means of Developing the Athlete's Personality. BRAIN. Broad Research in Artificial Intelligence and Neuroscience. 2023. № 14 (1). P. 647-661. https://doi.org/10.18662/brain/14.1/439/.

2. Wethington, E. (2003). Turning points as opportunities for psychological growth. In C. L. M. Keyes & J. Haidt (Eds.), *Flourishing: Positive psychology and the life well-lived* (pp. 37–53). American Psychological Association. https://doi.org/10.1037/10594-002.

3. Charles C. Benight , Gail Ironson , Kelli Klebe , Charles S. Carver , Christina W ynings , Kent Burnett , Debra Greenwood , Andrew Baum & Neil Schneiderman (1999) Conservation of resources and coping self-efficacy predicting distress following a

natural disaster: A causal model analysis where the environment meets the mind, Anxiety, Stress, & Coping, 12:2, 107-126, DOI: 10.1080/10615809908248325.

Ярослав МАКАРОВ
НУОУ
ORCID: 0009-0000-0623-935X
E-mail: j.makarov@i.ua

СИНТЕЗ ЧИННИКІВ, ЯКІ ФОРМУЮТЬ БЕЗПЕКОВЕ СЕРЕДОВИЩЕ СИЛ ОБОРОНИ УКРАЇНИ

Широкомасштабна агресія рф проти України вплинула на воєнно-політичну нестабільність на Близькому Сході, боротьбу за вплив на світові фінансові та енергетичні потоки посилюється глобальна воєнно-політична нестабільність. Провідні держави збільшують розміри воєнних витрат, активізують розробку нових зразків озброєння, підвищують інтенсивність військових навчань.

Аналіз джерел [1, 2] показав, що формування та розвиток безпекового середовища у світі відбувається під впливом наступних тенденцій:

посилення суперечностей щодо поділу сфер впливу між світовими центрами сили, збільшення їх агресивності, непоступливості, прагнення порушити на свою користь воєнно-стратегічну рівновагу, зокрема загострення протистояння між США та Російською Федерацією;

загострення безпекової ситуації в країнах Близького Сходу та Північної Африки, активізація релігійного екстремізму та поширення ідей радикального ісламу в країнах Центральної Азії, суперечності між азіатсько-тихоокеанськими державами щодо належності острівних зон;

сучасна криза та невизначеність засад нової системи міжнародної безпеки, послаблення ролі міжнародних безпекових інститутів, спроби посилити роль воєнної сили поза наявними механізмами міжнародної безпеки;

перенесення ваги у воєнних конфліктах на асиметричне застосування воєнної сили не передбачені законом збройними формуваннями, зміщення акцентів у веденні воєнних конфліктів на комплексне використання воєнних і невоєнних інструментів (економічних, політичних, інформаційно-психологічних тощо), що принципово змінює характер збройної боротьби;

порушення норм і принципів міжнародного права, закріплених у Статуті ООН, Заключному акті Наради з безпеки та співробітництва в Європі 1975 року та інших міжнародних договорах;

послаблення законодавчих обмежень щодо застосування воєнної сили державами за межами власної території;

глобальні кліматичні зміни, зменшення запасів природних ресурсів, дефіцит питної води, продуктів харчування, посилення міграційних процесів, а також зростання ризиків виникнення масштабних надзвичайних ситуацій природного та техногенного характеру;

розширення масштабів тероризму, піратства, інших явищ, пов'язаних із застосуванням збройного насильства.

При цьому в Стратегії інформаційної безпеки України визначено, що актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері залишається:

здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

інформаційне домінування держави-агресора на тимчасово окупованих територіях;

недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Отже, синтез чинників, які формують безпекове середовище сил оборони України показує, що формування постійне використання Росією в офіційній (МЗС РФ) та політичній площині спеціальних наративів та інформаційних ярликів з метою делегітимізації української влади (“партія війни”, “київська хунта”, “бандерівці”, “фашисти”, “нацисти”), а також кодування суспільної свідомості українців комплексом “молодшого брата”

Список використаних джерел

1. Leigh Armistead “Information Operations. Warfare and the Hard Reality of Soft Power”, Potomac Books, INC, Washington D.C.

2. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства Аналітичний документ. Київ, 2018. – [Електронний ресурс]: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf.]

Марія МАРТИНОВА
Слухач навчальної групи 8204
Інститут стратегічних комунікацій
НУОУ
ORCID: 0009-0002-1706-2948
E-mail: karinalegka8@gmail.com

АНАЛІЗ ЧИННИКІВ ЯКІ ВПЛИВАЮТЬ НА ЗАХОДИ ВЕДЕННЯ ПРОТИВНИКА В ОМАНУ

Російсько-українська війна вимагає поглибленого розуміння та аналізу чинників, що впливають на заходи ведення противника в оману. Країни-члени НАТО звертають особливу увагу на інформаційні операції, спрямовані на дезінформацію, психологічний тиск та спроби деморалізації противника.

Аналіз заходів введення противника в оману [1, 2] показує, що на сьогоднішній день найактуальнішим є дезінформація, яка забезпечує швидке розповсюдження недостовірної інформації, ефективно впливаючи на рішення та дії противника в сучасних умовах розвитку інформаційних технологій.

Метою тези є аналіз чинників які впливають на заходи ведення противника в оману для обґрунтування рекомендації щодо підвищення ефективності заходів дезінформації.

Введення противника в оману є одним із давніх та водночас сучасних засобів ведення військових операцій. Застосування обмани може допомогти зберегти життя особового складу, збільшити ефективність бойових дій та внести зміни у плани противника. Далі я би хотіла проаналізувати які саме чинники впливають на ефективність цих заходів.

В першу чергу розглянемо такий чинник як технічна оснащеність та компетентність особового складу.

Сучасні військові операції потребують високого стандарту технічної оснащеності та професійної підготовки особового складу. Високоякісне обладнання може забезпечити передові технічні можливості для введення противника в оману, від автоматизованих систем розвідки до сучасних засобів радіоелектронної боротьби. Однак без належної підготовки військовослужбовців навіть найкраще обладнання може виявитися недостатнім.

Аналізуючи вище зазначене, можемо виділити ще один важливий чинник, такий як розвиток технологій та його вплив на противника.

У сучасному технологічному світі способи введення противника в оману постійно адаптуються і еволюціонують. До прикладу, безпілотні літальні апарати не лише дозволяють вести розвідку з безпечної відстані, але й можуть бути використані для створення "фальшивих" цілей або відволікання уваги противника. Також, такий елемент як електронна розвідка та кібероперації дозволяють втручатися в комунікаційні системи противника, створюючи ілюзію невірної інформації або завдавши шкоди його інфраструктурі. Водночас сучасні програмні рішення дозволяють моделювати різні сценарії, передбачаючи можливі реакції противника на заходи обману. Таким чином, технологічні інновації роблять тактику введення в оману набагато більш різноманітною, ефективною та адаптивною до сучасних умов ведення бойових дій.

Наступним чинником розглянемо інформаційне середовище.

В епоху цифровізації, канали комунікації та доступ до інформації стали незрівнянно ширшими та різноманітнішими. Інформаційний потік не лише збільшився, але й став складнішим за структурою і впливовішим у соціально-політичному контексті. Соціальні мережі, новинні портали, блоги та інші платформи дозволяють інформації розповсюджуватися миттєво, досягаючи глобальної аудиторії.

В цьому контексті, спритні інформаційні кампанії, спрямовані на масове впровадження дезінформації або пропаганди, можуть використовуватися як потужний інструмент ведення противника в оману. Ці стратегії можуть маніпулювати громадською думкою, формувати неправильне сприйняття подій і, в кінцевому результаті, впливати на стратегічні рішення противника.

Також важливо зазначити роль кібербезпеки. З допомогою кібератак можна не тільки отримати доступ до конфіденційної інформації, але й змінити або знищити дані, створюючи хаос та невпевненість у рядах противника.

Тому, розуміння механізмів інформаційного розповсюдження та розробка ефективних стратегій у цій сфері є ключовими для успішного введення противника в оману в сучасних умовах..

Аналіз чинників, які впливають на заходи введення противника в оману, свідчить про їх складний та багатоаспектний характер. У сучасних умовах ведення бойових дій, успіх заходів ведення противника в обману залежить від комбінації технологічних, психологічних, культурних та інформаційних факторів.

Технологічний прогрес приносить нові інструменти і можливості для ефективного обману, однак це також ставить нові виклики та потреби в адаптації. Розуміння психологічних та культурних особливостей противника є ключовим для створення і реалізації обманних стратегій, які будуть максимально ефективними. Інформаційна епоха, в свою чергу, робить обман однією з найважливіших частин сучасної військової стратегії, з акцентом на швидкість, гнучкість та адаптивність.

Отже, для досягнення успіху в заходах обману, необхідно поєднання глибоких знань, високої технічної підготовки, а також здатності швидко адаптуватися до змінюваного бойового середовища.

Список використаних джерел

1. Іжутова І.В., Історико-ретроспективний аналіз формування та розвитку системи стратегічних комунікацій у секторі безпеки і оборони України. https://doi.org/10.33577/2313-5603.35.2021.3-17.

2. Гребенюк М. В. Основи стратегічних комунікацій за стандартами НАТО : навч. посіб. – К. : НУОУ ім. Івана Черняховського, 2017. - 180 с.

Владислав МОЗАЛЬОВ, к.пед.н.
НУОУ
ORCID: 0000-0002-1764-9063

ПЕРЕГОВОРИ ЯК ФОРМА КОЛЕКТИВНОГО ОБГОВОРЕННЯ

Поряд з індивідуальною бесідою важливу роль у житті людини відграють різні форми колективного спілкування. Завдяки ним реалізується роль людини у суспільстві, її участь у вирішенні спільних проблем, її вплив на процеси, що стосуються багатьох. Висока культура коллективного спілкування безпосередньо сприяє не тільки олюдненню людини, але й духовному збагаченню членів суспільства, а завдяки цьому – прискоренню демократичних процесів, зростанню матеріального добробуту.

Переговори як форма колективного вирішення проблеми використовуються не державному рівні, у корпоративних і навіть у сімейних відносинах. Вони відбуваються між людьми, які по-дружньому ставляться одне до одного і, навпаки, насторожено; які хочуть об’єднатися заради спільної справи і, навпаки, хочуть розійтися. Преговори йдуть і тоді, коли люди про це навіть не здогадуються. На жаль, більшість людей вести переговори не вміє. Вони нестерпно ставляться до чужої позиції, погано слухають інших, намагаються нав’язати свою думку, легко переводять розмову у сварку і псують взаємини та настрій один одному [2].

Вміння вести переговори – це ціла наука, якою слід якомога раніше оволодівати кожному.

Переговори – це обмін думками, як правило, з певною діловою метою.

На думку фахівців існує декілька стратегій, підходів до ведення переговорів. Перша стратегія ведення переговорів зводиться до протистояння крайніх позицій

партнерів. М’яка за характером людина бажає уникнути міжособистісного конфлікту і заради досягнення згоди з готовністю йде на різні поступки. Вона хоче полюбовного вирішення питання, але справа нерідко закінчується тим, що саме вона залишається ображеною. Жорсткий учасник переговорів розглядає кожну ситуацію як змагання волі, де той, хто виявляє крайню позицію і вперто стоїть на своєму, отримує більше. Він хоче лише перемоги, але це веде до того, що опонент теж вимушений зайняти жорстку позицію. Розв’язання проблеми затягується, псуються настрій, відносини [3].

Другий стратегічний підхід – це середина між м’якістю та жорстокістю. Але це далеко не завжди вдається, бо важко дотримуватися саме середини, тобто і досягти своєї мети, і не зіпсувати відносини з людьми.

Завдяки третьому підходу передбачається вирішення проблеми, виходячи із змісту справи, а не торгу з приводу того, чи йде кожна сторона на якісь поступки. За цією стратегією передбачається жорсткий підхід до розгляду суті справи, але м’який підхід до відносин між учасниками переговорів. Вона дає можливість прийняти справедливе рішення і водночас застерігає тих, хто хоче скористатися порядністю іншого. Такий підхід розроблено в рамках Гарвардського проекту і називаються ці переговори принциповими. Завдяки даному підходу люди намагаються максимально знайти взаємну користь. Там де інтереси не співпадають, вони прагнуть до такого результату, який був би обґрунтований якимись справедливими нормами, критеріями незалежно від волі жодної із сторін.

Переговори мають три стадії: 1) аналіз ситуації, проблем учасників, їх емоцій, відносин, інтересів, можливих варіантів прийняття рішення, критеріїв для вирішення проблеми; 2) планування; 3) дискусія. Доцільно відвести певний час на попередній аналіз майбутніх переговорів з позицій та інтересів їх учасників.

Час та зусилля, які використано для попереднього аналізу майбутніх переговорів, послужать запорукою успіху.

На думку психологів варто виділити наступні принципи ведення переговорів:

- розмежування учасників та предмету переговорів;
- врахування інтересів обох сторін, а не їх пропозицій;
- аналіз всіх можливих варіантів розв’язання проблеми;
- виділення певного критерію для прийняття рішення.

Щодо поведінки людей під час переговорів. Річ у тім, що людина бачить світ виходячи із своєї позиції і тому нерідко плутає своє сприймання проблеми із реальністю. Дуже часто вона не може зрозуміти, що саме має на увазі інший. Врешті-решт виясняється, що людина не зуміла передати свою думку так, щоб її адекватно зрозуміли. Треба добре зрозуміти позицію кожного учасника

переговорів стосовно основної проблеми, заради якої люди зустрілися. Оскільки часто продовження відносин важливіше, ніж результат переговорів, тому необхідно:

- з'ясувати характер відносин між учасниками переговорів, проаналізувати свої і, по можливості, чужі почуття. Важливо також своєчасно "випустити пару", щоб не спалахували пристрасті. Для цього можна пожартувати, використати якісь жести, змінити інтонацію, або, при необхідності, вибачитись;
- якщо відчувається непорозуміння, то слід спокійно вислухати іншого (можна перепитати про його найважливіші думки), а потім вже, при потребі, уточнити, нейтралізувати, спростувати його аргументи;
- для того, щоб зрозуміти хід думок партнерів, варто поставити себе на їх місце, а потім вже спільно обговорювати проблему.

За протилежними позиціями нерідко стоять інтереси, які або різняться, або, навпаки, можуть бути схожими. І це треба добре усвідомлювати, бо нерідко існує думка про те, що у опонента, який спростовує вашу точку зору, інтереси – протилежні вашим. А вони якраз можуть співпадати з ними.

Виявити інтерес не завжди легко, бо він може бути погано висловленим, малопомітним, замаскованим. Але це все-таки необхідно зробити. Для цього слід поставити себе на місце іншого і запитати: "чому так?" або "чому ні?" Інтереси розрізняються за ступенем важливості. Найсильніші інтереси – це ті, що виражають основні людські потреби (безпеку, матеріальний добробут, почуття приналежності до якоїсь певної групи, визнання тощо).

Зазвичайно, важливо також визначити свої інтереси, знайти аргументи для їх захисту, а вже тоді переходити до висновків і пропозицій. Захищаючи їх, треба виявляти твердість. Водночас, там, де можна, бажано поступитися партнеру у переговорах, враховуючи його інтереси. Навряд чи інша сторона прислухається до вас, якщо ви не будете виявляти уваги до її інтересів і пропозицій. Для того, щоб переговори були результативними, треба шукати взаємовигідні варіанти розв'язання проблеми.

Іноді думають, що позитивний результат переговорів: перемога одного – поразка іншого. Проте, завдяки дослідженням психологів, багато хто розуміє, що найкращій вихід із ситуації, коли має певний виграш кожна сторона [1].

Психологи відмічають чотири прорахунки, які заважають людям під час переговорів дійти до згоди:

а) передчасні судження; б) пошук єдиного варіанту розв'язання проблеми; в) впевненість у неможливості "збільшити пиріг"; г) думки типу "їх проблема – це їх

проблема, і нехай вони її вирішують". Для того, щоб попередити такі позиції, доцільно при обговоренні проблеми розглядати декілька варіантів її вирішення. Для їх пошуку можна використати метод "мозкового штурму", виділити найбільш обіцяючи ідеї, а потім повернутися до загального підходу, де ідея – лише один із варіантів. Важливо для одержання позитивного результату подивитися на проблему очима різних людей, іноді сторонніх. Можна також розділити проблему на частини і приймати рішення поетапно.

Запропоновані варіанти угоди можуть мати різні якості: сильні (суттєві, постійні, всеохоплюючі, остаточні, безумовні, зобов'язуючи, першорядні) та слабкі (процедурні, тимчасові, часткові, умовні, другорядні). Але в будь-якому випадку найкраще виконуватися буде та угода, яка прийнята шляхом згоди.

Якщо угода більше виражає інтерес однієї із сторін, то треба полегшити іншій стороні її прийняття. Для цього слід скласти список декількох можливих рішень, у тому числі й тих, які може прийняти партнер. Потім необхідно розглянути можливі наслідки, якщо після переговорів ці рішення будуть реалізованими. Продумати треба також, як обґрунтувати свій підхід. Це легше зробити, якщо виходити з об'єктивних критеріїв. Чим більше при розгляді проблеми і пошуку варіантів її вирішення обидві сторони будуть звертатися до прецедентів, що вже мали місце, тим швидше вони дійдуть згоди.

Для того, щоб отримати позитивний результат, треба використати або об'єктивні критерії по суті питання, або здійснити справедливі процедурні дії. Якщо обом сторонам важко зупинитися на якомусь критерії, можна звернутися за порадою до третіх осіб.

Посередник може зіграти велику роль на переговорах, якщо вони повільно йдуть до успішного завершення. Йому не обов'язково глибоко вникати в позицію кожної сторони. Головне, виходячи із їх інтересів, знайти кращі варіанти можливого вирішення проблеми і допомогти прийняти спільне рішення. Посередник готує текст угоди, пропонує його сторонам і з врахуванням їх зауважень доводить цю роботу до логічного завершення.

Іноді, ще до початку переговорів, видно, що інша сторона сильніша. Як захистити себе від прийняття невигідної угоди, яку нав'яже опонент? Перш за все, згоду на підписання угоди слід давати тільки тоді, коли враховані ваші інтереси. Якщо це не вдається, можна запропонувати своє альтернативне рішення або ж відкласти переговори до більш зручного моменту.

Буває так, що переговори ще до початку приречені на невдачу, бо одна із сторін хоче їх провалити. Причому тут є така залежність: чим більше бажання це

зробити, тим з більшою енергією відстоюються власні інтереси і ті основи, на яких повинна вибудовуватись угода.

Що робити, якщо хтось не переговорах з метою їх зриву використовує такі методи, як обдурювання, погрози, тиск тощо? Доцільно, виявивши сам факт їх використання, винести це питання на обговорення, а також висловити свою думку з цього приводу і домовитися про подальші правила роботи. Як про це говорилося раніше, треба відділити поведінку людей від змісту проблеми, яку слід вирішити, і разом шукати спільне рішення [3].

Якщо ж з боку іншої сторони відчувається намагання обдурити партнера, краще за все відразу в угоду вписати такі положення, які б не дозволили це зробити. Іноді буває, що на переговорах ведеться "психологічна війна": опоненти роблять особистісні випади, не дивляться в очі, зловживають зауваженнями, вимагають повторювати одне і те ж по декілька разів, не відповідають на запитання або навіть перекручують їх. У цьому випадку краще за все швидше закінчити зустріч. Якщо справа дійде до погроз, то слід стриматися і не відповідати на них, бо переговори ніколи не будуть доведені до успішного кінця.

Іноді на переговорах вживають тактику позиційного тиску. Тобто використовують такий маневр як відмова від переговорів. Це – хитрощі, розраховані на те, що інша сторона пішла на максимальні поступки. У цьому випадку треба виявити інтереси опонента і, виходячи з них, внести свої пропозиції. Якщо відчувається, що апетити у опонентів ростуть і вимоги все збільшуються, то краще зробити перерву і, проаналізувавши ситуацію, відмовитися від переговорів взагалі.

Буває корисним використати прийом заставки. Суть його в тому, щоб не концентрувати увагу на поведінці іншої сторони, а обговорювати принципові питання так, щоб опонентові було легше відступити.

Є ще один прийом – розрахована затримка. У цьому випадку слід створити таку ситуацію, у якій можливості іншої сторони з часом будуть зменшуватися. Можна використати також тактику "берете чи не берете?" Опонентам слід дати зрозуміти, що вони можуть втратити все, якщо переговори не будуть завершені. Але водночас важливо дати їм можливість "врятувати своє обличчя". Не треба перетворювати їх або себе в жертву.

Ситуація, коли кожна сторона в переговорах займає свою певну позицію і жорстко захищає її, як зазначалося вище, називається позиційним торгом. Чим більше людина захищає певну позицію, тим більше вона себе з нею зв'язує. Тому тут протистояння буде йти з приводу позицій, а не інтересів сторін. Такий торг

приводить до укладення нерозумних угод або до суперечки. Причому вона, як правило, неефективна, довго тягнеться, вимагає певних зусиль. Це може взагалі загрожувати результативності переговорів.

Позиційний торг нерідко перетворюється в змагання волі. В результаті перемоги однієї із сторін у іншої виникають гнів та образа. Якщо причин буде декілька, то позиційний торг поглиблюється. Причому, найчастіше, буває так, що той, хто займає м'яку позицію, стає переможеним, а той хто проявляє жорстокість, виграє. У таких випадках переможений – це потенційний ворог. Ця людина буде недоброзичливо ставитися до переможця. Щоб уникнути цього, слід прагнути до іншого результату, а саме: перемога - перемога.

Список використаних джерел

1. Корнеліус Х., Фейр Ш. Виграти може кожен. / Сімферополь: Стрінгер, 1992.
2. Томан І. Мистецтво говорити. / Пер.з чеш. – Київ, 1986
3. Фішер Р., Юрі У. Щлях до згоди, або переговори без поразки. / Пер. з. англ. Київ, 1992. С. 21-32.

Дмитро ОСАДЧИЙ
ORCID**:** 0009-0008-9638-7030
E-mail:osadchuy19944@gmail.com

АНАЛІЗ ЧИННИКІВ ЯКІ ВПЛИВАЮТЬ НА ЕФЕКТИВНІСТЬ МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ ЗБРОЙНИХ СИЛ УКРАЇНИ

У кожному інформаційному заході є відповідні показники, за якими оцінюється характеристики інформації та визначаються умови за якими може застосовуватись деструктивна спрямованість для будь-яких інформаційних заходів (дій, фактів) в інформаційному просторі держави. Враховуючи, що зазначені складові мають свою інформаційну корекцію, виявлені в інформаційному просторі держави (дій, фактів) або явища можуть знижувати рівень морально-психологічного стану особового складу військ) до стану коли особовий склад не в змозі ефективно виконувати завдання.

Мета тез: аналіз чинників які впливають на ефективність моніторингу інформаційного простору Збройних Сил України задля об'єктивної необхідності відслідковування перебігу подій у державі (світі) в онлайн-режимі (використовуючи креативні технологічні рішення) та одночасно застосовувати технології упередженої дії щодо можливого розвитку ситуації (як процесів, а не персон);

необхідно усвідомити недоліки наявних моніторингових технологій та розробити підходи до переходу на новий рівень осмислення інформаційного простору із використанням конвергентних технологічно-стратегічних рішень комплексно-комбінованого аналізу.

Традиційно моніторинг визнається як технологічне рішення (інструмент), за допомогою якого адекватно вивчається інформаційний простір (ІП) країни. Сам же ІП сприймається як стала величина і досить часто при його аналізі не беруться до уваги зміни в джерельній базі та інноваціях каналів подачі інформації. Моніторингові системи не аналізують інформаційно-контентні поля за змістом, вони ведуть пошук за визначеними параметрами, які формуються на підставі попиту чи управлінсько-посадових кон'юнктур.

Моніторинг - це постійне відстеження ходу робіт (в рамках проекту, програми або організації) для порівняння поточного стану справ з планом. Систематичний збір інформації про хід робіт (в рамках моніторингу) - свого роду «сканування» ситуації - проводиться як рутинна процедура, призначена, головним чином, для того, щоб вчасно виявляти відхилення від накреслених планів. Добре працююча система моніторингу допомагає керівнику організації (проекту, програми) своєчасно реагувати на згадані вище відхилення.

Аналіз публічних контентних масивів інформаційного простору іноземного походження щодо України в цілому традиційно формувався на підставі лінійного бачення спеціальних підрозділів різного функціонального навантаження (ГУР, ГШ ЗСУ, СБУ тощо), які вимірювалися зазвичай поточними або часто-густо авральними проблемами національної безпеки. До того ж вони часто орієнтувалися не на геостратегічну кон'юнктуру геополітичних моделей інтересів державно-суспільного розвитку України, а на кон'юнктуру політико-економічних груп впливу. Така кон'юнктура характеризувалася публічними проявами прямого (очевидного) негативу у трактуванні проблем оборони на засадах минулих безпеково-доктринальних підходів, без сучасного поділу потокового негативу за такими індикаторами як виклики, ризики, загрози.

Пошук предметів аналізу здійснювався за так званим індексним моніторингом. Індексний моніторинг (ІМ) – це збирання в певному полі інформації за деякими попередньо заданими ознаками (наприклад, пошук у мережі Інтернет інформації за заданим словом), або пошук у всіх спеціалізованих виданнях, присвячених якомусь окремому аспекту теми. Слід зазначити, що інформаційний простір України ніколи системно в державних вимірах не був об'єктом і предметом постійного дослідження.

Моніторинговий пошук за таких умов може поділятися на новинний, тематичний, ситуаційний, прогнозний тощо, що зазвичай поєднуються (повністю або частково).

Джерельною базою для проведення моніторингу є преса, телебачення і радіо, інтернет-мережа в усіх вимірах, бази даних (зокрема, спеціальні) тощо.

Традиційний моніторинг ґрунтується на застосуванні ключових слів (тегів) для пошуку або формуванні пошукового профілю.

Агрегатор новин - це веб-сайт, програма або мобільний додаток, який збирає новини з різних джерел і відображає їх у зручному форматі для користувачів. Такі платформи дозволяють людям отримувати інформацію з різних джерел на одному ресурсі, що робить їх важливими для тих, хто хоче бути в курсі поточних подій.

Таргетування поведінки ЦА - це стратегія дій, коли спеціальна інформація та спец дії спрямовані на користувачів, враховуючи їхні попередні дії, уподобання, історію переглядів інформіція, та інші аспекти їхньої поведінки. Цей підхід дозволяє створювати специфічні та персоналізовані повідомлення та пропозиції, які відповідають потребам та інтересам конкретних груп користувачів для подальшого впливу на них. Ось деякі ключові аспекти таргетування поведінки ЦА:

Аналіз Поведінки:

Вивчення дій користувачів на веб-сайті, інтеракції з контентом, часу перебування на сторінках, та інших активностей для розуміння їхньої поведінки.

Сегментація ЦА: Розділення ЦА на групи за певними характеристиками поведінки, такими як частота перегляді відео, підписка на новини, тощо.

Персоналізація Контенту:

Створення персоналізованого контенту та пропозицій на основі дій користувачів, що спонукає їх до більш активних взаємодій з спеціальними органами.

Ретаргетинг: Спрямування спеціакльних повідомлень на користувачів, які раніше взаємодіяли з веб-сайтом, виразили інтерес до інформації.

Спостереження за Змінами в Поведінці: Аналіз змін у поведінці користувачів та відповідне адаптування спеціальних стратегій для відповіді на ці зміни.

Тестування та Оптимізація: Проведення A/B тестів, щоб визначити, які види контенту та акцій найефективніше реагують на зміни у поведінці ЦА, і відповідно оптимізувати стратегії.

Тобто Таргетування поведінки ЦА дозволяє створювати більш персоналізовані та релевантні комунікації, що підвищує шанси на привертання уваги та взаємодії користувачів, що врешті-решт призводить до підвищення конверсії та лояльності підрозділів моніторингу ЗС України

Висновки. Застарілі технологічні рішення, на які спираються нинішні моніторингові технології, відіграють роль баласту в процесі оперативного визначення проблемних аспектів сучасного інформаційного простору.

Поглиблений моніторинг має здійснюватися із застосуванням сучасних вимірів тегового структурування чи навіть фреймів (які виступають прообразом майбутніх систем моніторингу, що спиратимуться на штучний інтелект).

Серед проблемних питань моніторингу інформаційного простору найпершою є така – не всі джерельні потоки, які обслуговують інформаційний простір України, є 100% в мережі Інтернет (ми ще не досягли реального тотального цифрового інформаційного простору, а працюємо в межах гібридних поєднань різних епох розвитку джерельно-контентного виробництва). Інші проблеми (назвемо це особливістю вивчення контентних масивів) містить в собі безпосередньо мережа Інтернет – складність в алгоритмах вибірки та обробки значних масивів інформації, їхньої агрегації та попереднього аналізу, недостатній рівень розвитку адекватних за продуктивністю технологічних рішень, зокрема створення інтелектуально-технологічних пошуковиків, визначення первинності контентного явища за часовим виміром та геопозиційною приналежністю, також встановлення рівнів довіри до контенту та виняткового права авторства тощо

Несвоєчасність отримання необхідної для аналізу інформації та неспроможність застарілої методологічної бази продукувати інноваційні комунікаційно-сценарні поліваріантні рішення призводять до програшу в інформаційному протистоянні.

Формалізовані підходи до аналізу інформаційного простору мають залишитися в минулому, поступившись місцем конвергентним технологічно-стратегічним рішенням комплексно-комбінованого аналізу

Список використаних джерел

1. Кацалап В. О., Кирпічніков О. Д., Саунін Р. Д. Методичний підхід до оцінювання рівня інформаційно-психологічного впливу противника в інтересах інформаційної операції Збройних Сил України, URL: https://doi.org/10.33099/2304-2745/2022-3-76/24-31
2. Пєвцов Г. В., Залкін С. В., Сідченко С. О., Хударковський К. І. Інформаційно-психологічні операції планування, протидія, технології// Монографія. Харків 2020. С. 41-45, 135-140.
3. Дзюба М.Т., Жарков Я.М., Ольховой І.О., Онищук М.І. Нарис теорії і практики інформаційно–психологічних операцій // Навчальний посібник. Київ 2006.

Володимир ПАТОЛА
НУОУ
0009-0004-3299-035X
patolavolodimir@gmail.com

КОГНІТИВНА БЕЗПЕКА ОСОБОВОГО СКЛАДУ СИЛ ОБОРОНИ УКРАЇНИ

Найчастіше у медіа, популярній літературі і навіть професійних колах дії в інформаційному просторі, якими російські окупанти забезпечують та підтримують свою збройну агресію, називають “інформаційною агресією” або “інформаційною війною”. Рідше ми можемо почути термін “інформаційно-психологічна операція”, який, зазвичай, у масовому вжитку застосовується невірно – для позначення фейків, недостовірної інформації чи виявлених окремих елементів інформаційних або інформаційно-психологічних акцій. Ці поняття не відображають найнебезпечніших особливостей ворожих дій, спрямованих проти свідомості представників Сил оборони України, українських громадян та громадян інших країн. Актуальність теми доповіді полягає у тому, що максимально просте, коротке і зрозуміле роз’яснення понять “когнітивна війна” та “когнітивна безпека”, а також загальне розуміння когнітивних процесів можуть суттєво підвищити можливості опору когнітивному впливу представників Сил оборони України, які на даний момент є першочерговою ціллю для такого впливу з боку ворога. Крім того, доцільно підняти питання вироблення та розгортання комплексної стратегії забезпечення когнітивної безпеки щонайменше на рівні з кібербезпекою та інформаційною безпекою загалом.

Когнітивна сфера – це новий простір, де відбуваються змагання, поряд із сухопутною, морською, повітряною, кібернетичною і космічною сферами. Сьогодні когнітивна війна, заради досягнення своїх цілей, поєднує в собі

кібернетичні, інформаційні, психологічні засоби, а також засоби соціальної інженерії [1]. Когнітивна війна стає системною та цілеспрямованою діяльністю ворога у ході контролю за інформаційними потоками[2].

Поняття "інформаційна безпека" є ширшим за обсягом поняттям, ніж "безпека інформації" і включає в себе останню. Часто поняття "інформаційної безпеки" ототожнюють з "кібербезпекою". Усі держави без винятку приділяють багато уваги кібербезпеці і мало тому, що можна позначити терміном "когнітивна безпека". У кібербезпеці захищають кіберресурси, у когнітивній безпеці – розум людини[7].

Зазвичай, поняття "когнітивної війни" розглядають на макрорівні, на прикладах впливу на цілі держави і їхні суспільства. Військовий злочинець країни агресора, відповідальний за інтерпретацію та розвиток концепції когнітивної війни в росії, керівник так званого "центру наукової політичної думки та ідеології" Степан Сулакшин у 2014 році сформулював визначення "когнітивної зброї" як "впровадження в інтелектуальне середовище країни противника помилкових наукових теорій, парадигм, концепцій, стратегій, які впливають на її державне управління в бік ослаблення оборонно-значущих національних потенціалів"[3, 4].

Заступник директора Науково-дослідного інституту українознавства МОН України, доктор історичних наук Дмитро Вєдєнєєв зазначає, що когнітивна складова сучасного конфлікту охоплює сферу вироблення й прийняття рішень та передбачення дій противника з урахуванням національної психології й ментальності, цивілізаційних факторів. [5]. При цьому сутність так званої "когнітивної зброї" полягає у досягненні інтелектуальної переваги над супротивником та маніпулюванні його свідомістю за допомогою наукових і псевдонаукових конструкцій[6].

Одним із важливих факторів ефективності когнітивного впливу є той факт, що він апелює до автоматизованих неконтрольованих процесів пізнавальної діяльності, які за своєю природою властиві людській психіці. Існує ряд типових когнітивних помилок, що є побічним продуктом в цілому ефективної системи мислення, заснованої на взаємодіях як "автоматизованих", так і контрольованих свідомих процесів обробки інформації. Специфічні особливості функціонування когнітивного апарату у певних ситуаціях створюють умови для так званого "феномену ментального забруднення". Т. Уілсон та Н. Брекке вводять поняття "ментальні забруднювачі" для опису факторів, що сприяють набуттю небажаних суджень, емоцій чи поведінки завдяки процесам обробки інформації, що є несвідомими чи неконтрольованими. Небажаність у даному випадку означає, що особа під час формування судження не бажала б піддаватись впливу несвідомих автоматизованих процесів[8].

У суспільстві загалом та серед особового складу Сил оборони України є розуміння того, що завданнями ворожих інформаційних дій, зокрема інформаційних та психологічних акцій, може бути зміна переконань, ставлень або

оцінок об’єкта атаки. Зазвичай особовий склад Сил оборони України, особливо якщо мова йде про професійних військових, ветеранів бойових дій та добровольців, є достатньо сильними, цілісними, сформованими, вмотивовованими особистостями, для яких не характерно легко змінювати свої переконання, оцінки та ставлення під впливом зовнішніх факторів, особливо – ворожої пропаганди. Вплив когнітивного характеру порушує насамперед не зміст розумової діяльності людини (що людина думає), а форму (як людина думає)[1], і тільки потім можуть наставати або не наставати наслідки у вигляді зміни оцінок, ставлень та переконань. Таким чином, застосування когнітивного впливу небезпечне навіть для тих, кого прийнято вважати стресостійкими особистостями з усталеним світоглядом, шляхом впливу через неусвідомлені процеси мислення прямо на мотиваційну сферу, так би мовити “обходячи” опір ставлень, переконань, оцінок, здатності до критичного мислення і, певною мірою, свідомості загалом, які виступають захистом особистості від дії класичних засобів пропаганди. Крім того, когнітивні помилки легше допускаються у стані виснаження когнітивних ресурсів, простими словами – фізичної і моральної перевтоми, інформаційного перевантаження, що загалом характерно для учасників бойових дій. Враховуючи викладене існує необхідність спрямованого дослідження засобів когнітивного впливу, які використовує ворог, а також розробки та реалізації системи заходів посилення когнітивної безпеки передусім представників Сил оборони України, та громадян України загалом.

Список використаних джерел

1. http://surl.li/zych. Сайт відвідано 03.10.2023. Протидія когнітивній війні: інформованість і стійкість. Університет Джона Хопкінса та Лондонський імперський коледж. НАТО Ревю 20.05.2021
2. http://surl.li/ltfhl Сайт відвідано 03.10.2023. Стрельбицький М., Гринь М. Когнітивна війна проти України. Наукові праці Міжрегіональної академії управління персоналом. Випуск 1 (64), 2023
3. http://surl.li/lthre Сайт відвідано 03.10.2023. Сухарков А., Новакова О. Політична система України в контексті російської інформаційної та когнітивної воєн. Освіта і наука. Київ. –2021
4. http://surl.li/lthvx . Зубар Н., Рущенко І. Когнітивна зброя і когнітивна безпека: постановка питання. Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення. М. Маріуполь 2017. 311 с.
5. http://surl.li/ltiiz – сайт відвідано 03.10.2023. Вєдєнєєв Д. “Вишукана” гібридна зброя: ураження свідомості керманичів та інтелігенції. Частина ІІ. Оборонно-промисловий кур’єр. 04.06.2020.

6. Вєдєнєєв Д., Семенюк О. Сутнісні риси та функціональні компоненти сучасної неконвенційної (гібридної) конфліктності. Стратегічна панорама. № 1-2 2021.

7. http://surl.li/ltjop – сайт відвідано 03.10.2023. Криволап Є.В. Співвідношення понять "інформаційна безпека", "безпека інформації", "кібербезпека", "когнітивна безпека" як стійкість проти інформаційно-психологічних впливів на людину і суспільство. Тези науково-педагогічних працівників, аспірантів та здобувачів вищої освіти. Національний авіаційний університет. 2023

8. http://surl.li/ltkhl – Сайт відвідано 03.10.2023. Яременко С.О. Когнітивні упередження як внутрішній фактор ефективності дезінформації у засобах масової інформації. "Інформація і право" № 1(13)/2015.

Дмитро ПОРАДА
НУОУ
ORCID: 0009-0006-1671-3509
E-mail: d-advice@ukr.net

АНАЛІЗ ЧИННИКІВ, ЯКІ ВПЛИВАЮТЬ НА ФУНКЦІОНУВАННЯ СИСТЕМИ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ

Україна, яка є мішенню рф у повномаштабній війні, гостро потребує дієвих і апробованих засобів протидії. Полем битви наразі є не тільки фізичний простір країни, а предметом – її суверенітет і територіальна цілісність, а й "серця та розум" українських громадян і, відповідно, лояльність та підтримка світової спільноти. У цій війні переможе той, чия розповідь (наратив) переможе. Отже, критичної ваги набувають механізми формування цього наративу, канали його поширення, прийнятність сформованого наративу для аудиторії, перехід від політики реагування до проактивної політики.

Аналіз інформаційного простору показує, що до основних чинників, які впливають на функціонування системи стратегічних комунікацій відносяться всім відомі методи пропаганди рф.

Тому метою тез є повести аналіз чинників, які впливають на функціонування системи стратегічних комунікацій для її удосконалення.

Стратегічні комунікації передусім є діяльністю з гармонізації тем, ідей, образів і дій. Прийнято вважати, що стратегічні комунікації це не просто питання "повідомлення", "відправника" і "отримувача" за класичною схемою комунікативного акту. Стратегічні комунікації передбачають діалог і підхід до побудови відносин на основі уважного ставлення до культурних та історичних особливостей, місцевих способів ведення справ і виявлення місцевих лідерів думок.

У військовій сфері, як правило, йдеться про гармонізацію всіх заходів у сфері публічної дипломатії, зв'язків із громадськістю та (військових) інформаційних операцій. Отже, стратегічні комунікації є одночасно і процесом (узгодження слів і справ з метою впливу та надання інформації), і результатом цього процесу[1, 2, 3].

Мета.

Стратегічні комунікації в інтересах війни рф проти України передусім мають бути спрямовані на підрив, викриття та порушення роботи методів пропаганди противника у спосіб набуття підтримки й визнання з боку місцевого населення, електорату своєї країни, міжнародної громадськості та всіх інших цільових груп. Сутність стратегічних комунікацій полягає в тому, що сформульовані для різних цільових аудиторій меседжі не конфліктують один з одним.

Основна частина.

Ключові компоненти процесу реалізації стратегічних комунікацій:

а) розуміння владою суспільства, його інформування та залучення для просування інтересів і цілей через вплив на сприйняття, установки, переконання та поведінку;

б) узгодження дій, зображень, висловлювань на підтримку політики й планування з метою досягнення всеосяжних стратегічних цілей;

в) визнання того, що всі операції і види діяльності є важливими компонентами процесу комунікації, оскільки все, що говорить і робить НАТО, має передбачувані й непередбачувані наслідки для цільових і нецільових аудиторій;

г) визнання того, що стратегічні комунікації є не додатковими діями, а невід'ємною частиною планування та реалізації усіх воєнних операцій та видів діяльності.

Висновки.

Отже,змістовим ядром стратегічних комунікацій є формування [стратегічного] наративу – переконливої сюжетної лінії, яка може пояснити події аргументовано і з якої можна дійти висновків щодо причин перебування держави в конфлікті, значення цього становища та щодо перспектив держави в разі успішного виходу з нього.

Список використаних джерел

1. Paul C.Getting Betterat Strategic Communication / Christopher Paul; RAND Corporation. – SantaMonica, 2011. – 18 p.

2. Strategic Communications and National Strategy : A Chatham House Report/ Paul Cornish, Julian Lindley French and ClaireYorke. – London, 2011. – 42 p.6 Код OF5 (стосується сухопутних військ) системи уніфікованих військових звань НАТО є еквівалентним званню полковника.Стратегічні пріоритети, № 1 (34), 2015 р. 152 стратегічні комунікації: досвід НАТО

3. US Department of Defense : Report on Strategic Communication [Електронний ресурс]. – Режим доступу:

http://www.au.af.mil/au/awc/awcgate/dod/dod_report_strategic_communication_11feb10.pdf

4.Почепцов Г.Г.Стратегические коммуникации: стратегические коммуникации в политике, бизнесе и государственному правлении. – К. : Альтерпрес, 2008. – 216 с.

Анатолій РИБИДАЙЛО, к.т.н., с.н.с.
ORCID: 0000-0002-6156-469X
Юрій КІРПІЧНІКОВ, к.т.н.
НУОУ
ORCID: 0000-0001-6893-3569

ШЛЯХИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ З МЕТОЮ СТІЙКОГО ФУНКЦІОНУВАННЯ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

В умовах воєнно-політичної кризи та збройної агресії Російської Федерації (РФ) проти України, її державним інститутам, зокрема Міністерству оборони (МО) України, належить виробити і застосувати нові сучасні підходи до розвитку власного інформаційного простору, забезпечення його стійкості та безпеки. Одним із пріоритетних напрямів є цифровізація діяльності та впровадження сучасних інформаційних технологій у сфері оборони для оперативного забезпечення посадових осіб різних рівнів управління Збройними Силами (ЗС) України певними комунікаційними, інформаційними та специфічними за напрямами їх діяльності функціональними сервісами [1].

Під *інформаційною інфраструктурою* розуміють сукупність інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування.

Інформаційна інфраструктура Міноборони та ЗС України – комплексна структура, яка об’єднує програмно-технічні засоби, організаційні заходи, нормативні документи, персонал та забезпечує функціонування, розвиток інформаційної взаємодії та інформаційного середовища Міноборони та ЗС України.

Проблемним питанням є той факт, що існуюча інформаційна інфраструктура Міністерства оборони України за даним напрямом тільки починає розвиватися, а окремі теоретичні дослідження не охоплюють всього циклу її розвитку.

Нагальною вбачається задача аналізу сучасних підходів стосовно розбудови (модернізації/удосконалення) інформаційної інфраструктури (ІнфІ) Міністерства

оборони (МО) України, яка є основою Єдиного інформаційного середовища воєнного відомства, для надання можливості обґрунтування управлінських рішень, які приймаються керівництвом Збройних Сил (ЗС) України. Особливу значущість означене завдання приймає в умовах збройного конфлікту.

Основні чинники, які можуть впливати на функціонування інформаційної інфраструктури в умовах збройного конфлікту наведені Табл. 1.

Таблиця 1

Чинники впливу на функціонування інформаційної інфраструктури

№	ЧИННИКИ	НАСЛІДКИ ВПЛИВУ
1	*Фізичне пошкодження ІІ*	Фізичне пошкодження інформаційних мереж, комп'ютерів, серверів та інших пристроїв, які є складовими частинами ІІ
2	*Відключення від мережі*	Відключення від мережі телекомунікаційних операторів, хостинг-провайдерів та інших постачальників послуг, що може призвести до відключення частини ІІ
3	*Вразливість мережевої безпеки*	Зростання рівня кіберзагроз: кібератаки, хакерські атаки та віруси, що можуть порушити функціонування ІІ та зашкодити їй
4	*Втручання в управління*	Може включати: цензуру, блокування доступу до деяких веб-сайтів та інших дій, що можуть обмежити доступ до інформації та вплинути на функціонування ІІ
5	*Недоступність ресурсів*	Ресурси: електроенергія та доступ до Інтернету, що може обмежити доступ до ІІ та забезпечення її функціонування
6	*Нехватка кваліфікованих кадрів*	Відтік кваліфікованих спеціалістів з інформаційної технології, що може призвести до нестачі кваліфікованих кадрів для підтримки ІІ
7	*Соціальні фактори*	Зміна соціального середовища, що може вплинути на здатність людей до використання інформаційної інфраструктури, а також на довіру до неї (для цивільної ІІ)

Побудова інформаційної інфраструктури для оборонних потреб може бути реалізована за допомогою підходів, які наведені у Табл. 2.

Таблиця 2

Підходи до реалізації інформаційної інфраструктури

№	ПІДХОДИ	ТЛУМАЧЕННЯ	ВИКОРИСТАННЯ
1	*Централізований*	Вся інформація зберігається в єдиній централізованій базі даних (центр обробки даних), яка забезпечує доступ до інформації всім зацікавленим сторонам у реальному часі	Великі організації та органи управління
2	*Децентралізований*	Кожний підрозділ має власну базу даних (центр обробки даних), яка зберігає інформацію, необхідну для	Організації, де різні підрозділи мають спеціалізовані функції

		виконання своїх завдань	
3	*Гібридний*	Використовуються елементи як централізованого, так і децентралізованого підходів	Територіальна розгалуженість споживачів
4	*Датацентричний*	Всі компоненти інфраструктури повинні бути побудовані навколо датацентру та підкорятися його вимогам та потребам, що дозволяє досягти оптимальної ефективності, надійності та безпеки роботи інфраструктури	Дозволяє забезпечити оптимальний рівень обробки і зберігання даних та досягти високої надійності і безпеки роботи інфраструктури
5	*Хмарний*	Інформаційна інфраструктура реалізується на основі сервісів, які надаються приватною хмарою або хмарними провайдерами	Необхідність високої гнучкості та масштабованості
6	*З використанням блокчейну*	Інформація зберігається в розподіленій мережі вузлів, які забезпечують високий рівень безпеки та захисту даних	Необхідність високого рівня безпеки та конфіденційності даних

Проведений аналіз дозволяє дійти висновку – кожному з підходів притаманні власні переваги і недоліки та їх використання доцільне за певних умов і цілей створення інформаційної інфраструктури. Отже, у якості рекомендацій стосовно шляхів удосконалення інформаційної інфраструктури МО України для забезпечення її функціонування та надійного застосування в умовах збройної агресії нагальним вважається поєднання розглянутих підходів для послаблення недоліків кожного з підходів та посилення їх переваг при комплексному використанні.

Для реалізації об’єднаного підходу при створенні інформаційної інфраструктури, яка має зберігати необхідний рівень стійкості в умовах збройної агресії необхідно провести аналіз можливостей та потреб у рамках конкретного контексту конфлікту (або збройної агресії). Такий аналіз має враховувати не лише технічні аспекти, а й культурні, соціальні та політичні аспекти. Крім того, потрібно врахувати потреби посадових (службових) осіб МО і ЗС України. Тобто, необхідно розробити стратегію доступу до інформації та зв’язку у межах повноважень посадових осіб.

Удосконалення інформаційної інфраструктури на основі об’єднаного підходу із забезпеченням можливості її функціонування в умовах збройного конфлікту є складним проєктом. У Табл. 3 сформульовані вимоги до удосконаленої інформаційної інфраструктури, які потрібно задовольнити при реалізації проєкту.

Таблиця 3

Вимоги до нової інформаційної інфраструктури МО України

№	ВИМОГИ
1	Необхідність дотримання міжнародних стандартів безпеки інформації ISO/IEC 27001 і національних стандартів України, якими імплементовані міжнародні стандарти безпеки інформації ISO/IEC 270XX, що забезпечить довіру до інформаційної інфраструктури міжнародних партнерів
2	Врахування можливих ризиків та уразливостей системи – DDOS-атаки, кібершпигунство, виток даних та інші види кіберзагроз. для чого необхідно включити в проєкт заходи захисту інформації та введення механізмів швидкого реагування на інциденти безпеки
3	Визначення стратегії резервного копіювання та відновлення даних в умовах збройної агресії може відповідно до плану резервного копіювання даних та процедури відновлення
4	Визначення процедур керування доступом до інформації. Для запобігання несанкціонованому доступу до даних відповідно до стратегії управління доступом на основі рольової моделі доступу, двофакторної автентифікації та інших сучасних методів
5	Визначення місця розміщення *ІнфІ* для забезпечення можливості захисту від можливих ударів та терористичних актів супротивника, а також забезпечити її захист від природних катастроф, таких як землетруси, повені та інші
6	Врахування вимог до енергозабезпечення. В умовах збройної агресії можливі перебої в енергопостачанні, тому необхідно врахувати цей фактор під час вибору місця розміщення компонентів ІнфІ та визначення резервних джерел живлення
7	Розробка стратегії моніторингу та аналізу інформації про стан ІнфІ у режимі реального часу для оперативного реагування на можливі загрози та вразливості
8	Кадрове забезпечення. Для забезпечення ефективної роботи ІнфІ необхідно готувати професійних фахівців, які мають відповідні знання та досвід роботи з сучасними ІТ-технологіями
9	Визначення плану дій при евакуації у разі виникнення загрози життю та здоров'ю персоналу

Для успішної реалізації такого проєкту потрібне проведення організаційних заходів, які наведені на рис. 1.

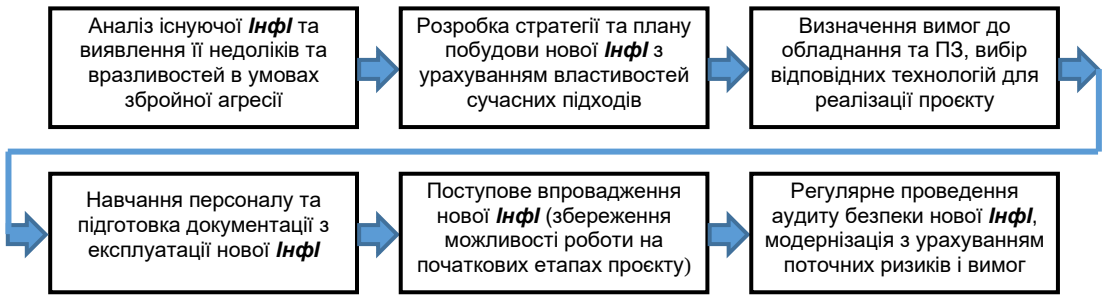


Рис. 1. Порядок удосконалення інформаційної інфраструктури МО України

Розвиток інформаційної інфраструктури МО України має збільшити швидкість, точність та якість процесу прийняття рішень, які є критичними для прийняття стратегічних рішень та успіху операцій і бойових дій. Це дозволить в повній мірі використовувати переваги обміну потрібною інформацією через всі домени інформаційного простору – від стратегічної до тактичної ланки, усунути принцип "ізольованості" існуючих інформаційних систем та забезпечити задоволення потреб в інформації, яка необхідна для швидкого прийняття рішень.

Список використаних джерел:

1. Концепція розвитку ІТ-інфраструктури Міністерства оборони України та Збройних Сил України.

Дмитро СИТНІКОВ
Слухач навчальної групи 8204
Інститут стратегічних комунікацій
НУОУ
ORCID: 0009-0000-7876-4439
E-mail: Dm_mail_s@ukr.net

АНАЛІЗ ЧИННИКІВ, ЩО ВПЛИВАЮТЬ НА СТВОРЕННЯ ШТУЧНОЇ ГРОМАДСЬКОЇ ДУМКИ

У сучасних умовах важливим є розвиток науки щодо управління громадською думкою, що виступає підґрунтям прикладних досліджень у галузі громадських зв'язків (public relations – далі ПР). Для України дані процеси відображають виваженість сучасної інформаційної політики держави, що відповідно сприяє зміцненню її позицій у всьому світі, подальшій демократизації суспільства, протистоянню у війні.

Громадська думка набуває все важливішого значення в світі, оскільки її пріоритетність є важливою для відкритого демократичного суспільства, прозорості влади, звітності перед платниками податків. Вона є проміжної ланкою у системі «влада – народ», обумовлюючи їх взаємозалежність, оскільки справляє вплив як на соціальні владні інститути, так і на суспільство загалом. У даному процесі провідна роль належить лідерам громадської думки та ЗМІ.

Отже, громадська думка є соціальним феноменом, який визначає загальне ставлення суспільства до певної проблеми. Найбільш виразним прикладом соціального акта, формою вираження громадської думки є політичні вибори [3, с. 25].

Механізмом управління громадською думкою є політичні ПР, результативність яких залежить від обраних виборчих технологій та здатності до впливу на поведінку виборців. Даний процес ускладнюється через те, що суб'єкти громадської думки одночасно потрапляють під вплив конкуруючих політичних сил, агітації, дезінформації, пропаганди, політичної реклами, а також штучно створеного політичного іміджу відповідних лідерів.

З боку держави реалізується інформаційна політика, котра є цілеспрямованим процесом впливу на свідомість громадян та формування штучної громадської думки з використанням засобів ПР. Передбачено, що даний процес в цілому спрямований на зміцнення держави.

У сучасних іноземних дослідженнях здійснено всебічне вивчення чинників, які справляють на громадську думку. Зокрема, виділяється роль расової неоднорідності соціуму у цьому процесі. У багатьох країнах, зокрема у США, розтає кількість расових меншин у суспільстві, що надає підстави розглядати расу як гнучкий та динамічний соціальний конструкт. Модель раси включає наступні значущі параметри, як місце, час, ціль та об'єкт сприйняття та, що повинно враховуватися у процесі впливу на створення громадської думки [2, с. 40].

Порівняльні дослідження в даній галузі є досить актуальними для політичної психології й для українського суспільства загалом, так як обумовлює необхідність орієнтації на національну ідентичність, врахування інтересів не тільки регіонів, але й представників різних етнічних груп, дотримання толерантності у під час впливу на різні частини цільової аудиторії за етнічною ознакою, що є основою єдності держави.

У сучасних дослідженнях досліджується роль соціальних мереж, зокрема Facebook, Instagram, Twitter тощо як політичної та медіа-галузі. Концептуальна основа даних досліджень базується на теорії поля П. Бурдьє, яка використовується соціальними медіа під час вивчення опосередкованих соціальних просторів [2, с. 41].

Розвиток комунікаційних технологій надав можливість не тільки запровадити нові напрямки взаємодії аудиторії з новинами, але й творив нові способи, котрими журналісти можуть здійснювати контроль за поведінкою аудиторії в Інтернеті. З допомогою нових інформаційних систем, зокрема таких, як вебаналітика, вплив аудиторії на конструювання новин, аудиторія в цілому зростає.

Науковці стверджують, що алгоритми формування громадської думки є результатом, а не заміною медіалогіки, вони ґрунтуються на поєднанні інтересів громадськості з медіалогікою. Оскільки саме ЗМІ є одним з основних каналів впливу на громадську думку, ефективність взаємодії ЗМІ з публікою є визначальним щодо електоральної поведінки. У процесі вивчення міжпартійної конкуренції інтернет-дослідники цікавляться, яким чином партії конкурують за увагу виборців в Інтернеті, набираючи підтримку через свою мережу.

Основним чинниками, які впливають на перебіг передвиборчої кампанії є наступні:

- тривалий ефект тенденцій партійної ідентифікації електорату;
- середньотривалий ефект показників конкретних особливостей національної економіки;
- короткотривалий ефект від конкретних зусиль політика в передвиборчій кампанії [1, с. 115].

Чинники формування громадської думки, що визначає взаємодію між владою і народом, регулюються лідерами думки та ЗМІ, передбачають як інформаційно-політичні, так і соціально-психологічні аспекти, виявляються в системі політичних ПР. На масову свідомість безпосередньо впливає характер подання політичної інформації, що реалізується ЗМІ, та позиція лідерів думки, забарвлена відповідним іміджем.

Визначення психологічного змісту іміджу та прикладних аспектів його формування дає змогу краще зрозуміти функції іміджу:

1) імідж повинен задавати певне враження, яке зазвичай підпорядковане конкретній меті та відповідає певній стратегії;

2) це позиціювання певної організації чи лідера перед цільовою аудиторією, що ґрунтується на усвідомленні свого призначення та переваг;

3) це спонукання до дій [2, с. 44].

Згідно із психологічними законами людської поведінки, для формування у людини готовності до дії в необхідному напряму необхідно створити установку. Для такої установки потрібна основа, яка задається стереотипним змістом іміджу та цілеспрямованим формуванням потреби в діяльності політичного лідера.

Інформаційно-політичні та соціально-психологічні чинники формування громадської думки виявляються тісно взаємопов’язаними. Їх коректне, адекватне реальності застосування становить підґрунтя для вдосконалення відповідних стратегій, спрямованих загалом на подальше зміцнення та демократизацію Української держави. Серед перспектив подальших досліджень у цій галузі слід визначити розроблення технологій формування громадської думки для різних сегментів цільової аудиторії.

Список використаних джерел

1. Правовий вимір державної інформаційної політики України в умовах глобальних викликів: монографія/ [І. О. Кресіна, В. П. Горбатенко, А. А. Коваленко та ін.]; за ред. І. О. Кресіної. Київ: Ін-т держави і права ім. В. М. Корецького НАН України, 2018. 282 с.

2. Романенко О. В. Чинники формування громадської думки в системі політичних PR. Юридична психологія. 2021. № 1(24). С. 39-45.

3. Соціологія громадської думки та мас-медіа: навч. посіб. для бакалаврів за спеціальністю 054 “Соціологія” / КПІ ім. Ігоря Сікорського; уклад.: Єнін М.Н., Северинчик О.П. Київ: КПІ ім. Ігоря Сікорського, 2021. 81 с.

Олександр СІДЕНКО
Слухач навчальної групи 8204
Інститут стратегічних комунікацій
НУОУ
ORCID: 0009-0006-8995-6528
E-mail: aleksiden@ukr.net

ДОСЛІДЖЕННЯ ШЛЯХІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ЗБРОЙНИХ СИЛ УКРАЇНИ

Актуальність дослідження стратегічних комунікацій Збройних Сил України та пошуку шляхів удосконалення їх механізмів у військовій сфері походить перш за все із гострої необхідності підвищення спроможностей Збройних Сил України та інших військових формувань ефективно виконувати своє фундаментальне завдання за призначенням, яке визначено Основним Законом України – здійснення оборони України, захист її суверенітету, територіальної цілісності і недоторканності.

В умовах тривалої збройної агресії Російської Федерації та повномасштабної війни на території України, обмеженості фінансово-економічних, науково-технологічних можливостей та ресурсів держави, слабкої ефективності державного менеджменту у сфері національної безпеки та оборони, забезпечення українського війська всім необхідним для ведення стратегічної оборонної операції, особливо новітніми зразками озброєння та військової техніки, на сьогодні є надскладним завданням для держави.

Історично склалося так, що стратегічні оборонні запаси нашої держави за роки незалежності різко скорочувалися, а переважна більшість наукових установ, підприємств та організацій оборонно-промислового комплексу, по різним причинам не спромоглися наростити відповідні спроможності та створити достатній рівень виробництва та запасів ОВТ.

Так, на думку ряду воєнних оглядачів, а також за словами Міністра оборони України – з моменту широкомасштабного вторгнення інтенсивність боїв була такою, що до квітня місяця 2022 року власні засоби для ведення оборони, зокрема боєприпаси, досягли критичного мінімуму [1].

Проте, високий рівень консолідованості українського народу, взаємодії державних органів та суспільства, бізнесу та громадськості, результати міжнародної дипломатії, створили високий рівень довіри до України та

переконали західні країни щодо необхідності постачання зброї та боєприпасів, озброєння та військової техніки.

Головним стрижнем успіху є взаємодовіра та консолідованість зусиль країни, єдність всього народу.

Так, ще відомий німецький воєнний теоретик, автор концепції "тотальної війни" генерал піхоти Еріх Фрідріх Вільгельм Людендорф у праці "Тотальна війна" обгрунтував основні її принципи, зокрема те, що однією з головних умов перемоги є духовна єдність нації: "Збройні сили беруть початок у народі, є його складовою, і в тотальній війні міцність армії прямо залежатиме від фізичної, економічної і духовної міцності народу. Саме духовна сила створює, єднає армію та цивільне суспільство, саме ця сила потрібна для боротьби за існування народу в такій війні... Саме духовна єдність є врешті-решт вирішальною для результату боротьби заради збереження народу" [2].

Останнім часом вітчизняні науковці значну увагу приділяють дослідженню стратегічних комунікацій. Сформульовані в дослідженні, теоретичні висновки й практичні рекомендації даної роботи ґрунтуються на працях вітчизняних учених: В.О. Кацалапа, Горбуліна В.П. [4], Войтка О.В., Іжутової І.В. [5], Гребенюка М. В. [6], Сальнікової О. Ф. [7], та інших.

Серед закордонних дослідників дослідження поняття "стратегічні комунікації" займалися Дж. Бернет, Ф. Денс, К. Ларсон, С. Моріарті, Ю. Хабермас, К. Халлахан, В. Шрамм та інші.

Більшість досліджень присвячена в основному теоретичній складовій, в якій розглядаються різні підходи до аналізу потянійного апарату, історичні аспекти створення та розвитку стратегічних комунікацій. Достатня увага приділяється науковцями саме розвитку стратегічних комунікацій в державах-членах НАТО. Водночас стан дослідження шляхів підвищення ефективності застосування механізмів стратегічних комунікацій Збройних Сил України в системі забезпечення національної безпеки України залишається на низькому рівні.

Метою дослідження є обґрунтування теоретичних засад механізмів стратегічних комунікацій Збройних Сил України та визначення шляхів підвищення їх ефективності.

Удосконалення механізмів стратегічних комунікацій Збройних Сил України є важливою задачею для забезпечення ефективного об'єднання комунікативних спроможностей та військової діяльності з метою формування інформаційного середовища для розуміння та підтримки українським суспільством та міжнародною спільнотою діяльності ЗС України, створення сприятливих умов для виконання ними завдань за призначенням.

На основі проведених досліджень та пошуку напрямків удосконалення механізмів стратегічних комунікацій Збройних Сил України розроблено практичні рекомендації, як узагальнений перелік першочергових комплексних заходів, які включають:

Розвиток іміджу та бренду. Стратегічні комунікації Збройних Сил повинні сприяти побудові позитивного іміджу та встановленню сильного бренду, що відображатимуть високу професійність, надійність та відповідальність українських військових.

Використання нових інформаційних технологій. З мірою розвитку технологій, необхідно використовувати нові медіа та інформаційні технології для передачі важливої інформації. Особливу увагу необхідно приділити використанню автоматизованих систем моніторингу інформаційного простору.

Розробка стратегії комунікацій. Ефективні стратегії комунікацій мають бути розроблені з метою взаємодії з різними аудиторіями, включаючи військовослужбовців, громадськість, політичні та військові лідери, міжнародну спільноту тощо. Важливо побудувати чітку стратегію для кожної аудиторії та використовувати відповідні комунікаційні канали та засоби.

Підвищення прозорості та відкритості. Збройні Сили України повинні активно працювати над забезпеченням прозорості своєї діяльності та доступу до інформації. Це може включати публікацію звітів, організацію прес-конференцій, створення відкритих платформ для спілкування з громадськістю тощо.

Зміцнення внутрішнього комунікаційного потенціалу. Важливим аспектом є покращення внутрішнього спілкування між військовослужбовцями та різними підрозділами Збройних Сил. Це можна досягти шляхом створення ефективних комунікаційних мереж, використання внутрішніх комунікаційних платформ, проведення тренінгів та семінарів з комунікаційних навичок, проведення об’єднаних тренувань та навчань.

Ці напрями спрямовані на покращення комунікаційного потенціалу Збройних Сил України, що допоможе встановити ефективний діалог з різними аудиторіями та забезпечити високий рівень сприйняття та розуміння їх діяльності.

Список використаних джерел

1. Річний звіт Міністра оборони України - Основні результати діяльності Міністерства оборони України за період з 4 листопада 2021 по 4 листопада 2022 рр. URL: https://drive.google.com/file/d/1CszO8fgpofFYFJvuqi9u0eN44OoMpF7/view.

2. І. І. Фурман, С. В. Сидоров, Р. І. Пилявець та ін., Історія воєнного мистецтва : підручник / НУОУ ім. Івана Черняховського, 2020. -516 с.

3. Стратегічні пріоритети – науково-аналітичний щоквартальний збірник Національного інституту стратегічних досліджень, № 1 (34), 2015 р.

4. Іжутова І.В., Історико-ретроспективний аналіз формування та розвитку системи стратегічних комунікацій у секторі безпеки і оборони України. https://doi.org/10.33577/2313-5603.35.2021.3-17.

5. Гребенюк М. В. Основи стратегічних комунікацій за стандартами НАТО : навч. посіб. – К. : НУОУ ім. Івана Черняховського, 2017. - 180 с.

6. Сальнікова О. Ф., Основи стратегічних комунікацій у сфері забезпечення національної безпеки та оборони: навч. посіб./ НУОУ імені Івана Черняховського, 2020 - 86 с.

Андрій СКАРЖИНЕЦЬ
Слухач навчальної групи 8204
Інститут стратегічних комунікацій
НУОУ
ORCID: 0009-0007-7350-5586
E-mail: Skarzenets@i.ua

ДЕЯКІ АСПЕКТИ ПСИХОЛОГІЧНОГО ВПЛИВУ НА ПРИЙНЯТТЯ РІШЕНЬ КОМАНДУВАЧЕМ (НАЧАЛЬНИКОМ)

Враховуючи збільшення кількості інформаційних операцій, психологічних акцій та гібридних тактик у російсько-українській війні, ця тема є дуже актуальною. Командувач (начальник) часто стикається з непрямими впливами на процес прийняття рішень, такими як дезінформація, пропаганда або психологічний тиск з боку противника, а також з боку вищого військово-політичного керівництва власної країни. Розуміння того, як психологічні фактори впливають на прийняття рішень на рівні оперативно-тактичного угруповання, може допомогти військовим органам управління підвищити свою ефективність та здатність протистояти негативному психологічному впливу.

Аналіз останніх досліджень і публікацій показує, що концептуальні основи впливу “стадного інстинкту” та “зараження” закладалися ще наприкінці XIX століття такими дослідниками як З. Фройд, К. Юнг, Г. Ле Бон. На сьогодні, в контексті російсько-української війни, окремі аспекти теми дослідження розкривають роботи Осьодло В.І., Траверсе Т.М., Будагьянц Л. М., Гуляк У.М.

Зважаючи на зазначене, метою тез доповіді є дослідження впливу ефектів “стадного інстинкту” та “зараження” на прийняття рішень командувачем (начальником) на рівні органу військового управління оперативно-тактичного угруповання.

Сьогодні інформаційне протиборство країн детермінує появу низки негативних ефектів, які впливають на прийняття рішень органами військового управління. Одними з найнебезпечніших ефектів такого протистояння є “стадний інстинкт” та “зараження”.

Стадний інстинкт - це тенденція до того, щоб наслідувати модель поведінки більшості або керівництва. У контексті даного дослідження це може означати, що

командувач (начальник) може приймати рішення, яке відображає думки або відчуття більшості його підлеглих, незважаючи на свої власні сумніви. Або ж втілювати певні рішення вищого політичного керівництва, навіть якщо вони не є найкращими в даній ситуації.

Не останню роль тут грають лідери думок, які можуть мобілізувати громадськість, що створює соціальний тиск на військових лідерів через політичне керівництво щодо певних рішень у військовій сфері.

Зараження ж вказує на явище, коли емоційний або психологічний стан однієї особи швидко передається іншим. В розрізі теми дослідження це може бути особливо небезпечним, оскільки очікування перемоги або, навпаки, песимізм та страх, навіть надмірний ентузіазм можуть швидко розповсюджуватися серед військовослужбовців, що може завадити об'єктивному та раціональному прийняттю рішень командувачем (начальником).

В поєднанні зазначені ефекти можуть зіграти роль у формуванні "групового мислення", коли командувач (начальник), замість критичної оцінки інформації та різних варіантів дій, намагається підтримувати консенсус в органі військового управління, до того ж, враховувати військово-політичні амбіції вищого керівництва. Такі ситуації призводять до прийняття рішень, які не враховують всіх аспектів бойової ситуації, а ґрунтуються на популярній думці або загальній атмосфері в суспільстві.

І хоча, досвідчені офіцери намагаються залишатися незалежними від зовнішніх впливів і базувати свої рішення на конкретних фактах, розвідці та власному професійному судженні. Проте у відкритих демократичних суспільствах вони не можуть повністю ігнорувати громадську думку і позицію політичного керівництва країни.

Саме тому для російсько-української війни яскравими прикладами впливу цих факторів на прийняття рішень командувачем (начальником) можна назвати затяжне утримання об'єктів та міст, які набули виключно символічного значення в ході інформаційно-психологічного протистояння.

Результатами чого стали:

- затримки проведення операцій: планова ретроградна операція з населених пунктів Сєвєродонецьк та Лисичанськ були затримані, що негативно вплинуло на кількість втрат особового складу та техніки.
- потреби у додаткових резервах: вище командування було змушене відправляти позапланові підкріплення для утримання населеного пункту Бахмут.

Отже, командувач (начальник) відіграє ключову роль у прийнятті рішень в рамках своєї зони відповідальності, при цьому він може стикатися з численними зовнішніми та внутрішніми психологічними викликами, які впливають на прийняття ним рішень. Резистентність до інформаційно-психологічних атак є критично важливою для ефективного командування та прийняття рішень.

Список використаних джерел

Гуляк У.М. “Психологічні механізми впливу стадного інстинкту на бойову активність військовослужбовців” [Електронний ресурс], – Режим доступу: https://nuou.org.ua/assets/documents/coll-npc-fc-pp-22-12-01.pdf

Зеленін В.В. “Основи міфодизайну: Психотехнології керування медіареальністю. Навчально-методичний посібник”, Київ, “Гнозіс”, 2017.

Осьодло В.І., Траверсе Т.М. “Психологія і війна: незасвоєні уроки Густава Ле Бона”, Київ, Парламентське видавництво, 2022.

Віктор СТРІЛЕЦЬ, д.т.н., проф.
НУЦЗУ
ORCID: 0000-0001-5992-1195
E-mail: vstrelec1956@ukr.net
Максим ГРИЦАЄНКО
НДЕВЦ “БрандТРЕЙД”
ORCID: 0000-0002-4436-9382
E-mail: post@firedept.mk.ua

УРАХУВАННЯ ОСОБЛИВОСТЕЙ ГУМАНІТАРНОГО ПІДВОДНОГО РОЗМІНУВАННЯ ЗА КОРДОНОМ В ПРАКТИЧНІЙ ДІЯЛЬНОСТІ УКРАЇНСЬКИХ ВОДОЛАЗІВ-РЯТУВАЛЬНИКІВ

Як в нашій країні, так і за кордоном накопичено величезний досвід щодо попередження та ліквідації наслідків надзвичайних ситуацій, які пов’язані із розмінуванням вибухонебезпечних предметів на суходолі. В той же час питання підвищення ефективності розвідки та розмінування водного середовища, особливо з урахуванням війни з росією вимагають свого покращення, оскільки кількість вибухонебезпечних предметів, які забруднюють мирні акваторії, суттєво збільшується, характерним прикладом чого є акваторія Дніпра нижче підірваної Каховської ГЕС, коли тисячі вибухонебезпечних предметів рознесло не тільки вздовж русла річки, але й по всьому Дніпровсько-Бугському лиману, в якому навіть до 24 лютого 2022 року оставались міни і снаряди після Другої світової війни.

В доповіді наведені результати особливостей попередження надзвичайних ситуацій, пов’язаних з підводним розташуванням вибухонебезпечних предметів, в провідних країнах світу, за результатами збору бібліографічної інформації та аналізу 105 літературних джерел провідних країн світу, в яких розглядаються особливості гуманітарного підводного розмінування на регіональному рівні.

На основі отриманих результатів визначено, що якщо до недавнього часу ексклюзивним досвідом у знищенні підводних вибухонебезпечних предметів володіли національні збройні сили, то сьогодні ці небезпеки разом з ними усувають різні типи (комерційні компанії, неурядові організації, команди центральних та місцевих органів влади тощо) організацій.

Підкреслена необхідність коригування діяльності особового складу невійськових організацій в додаток до тих навичок, які їм надають під час первинного навчання спеціалізовані підрозділи ВМФ. Показано, що процес попередження надзвичайних ситуацій, пов'язаних з підводним розташуванням вибухонебезпечних предметів, необхідно розглядати з урахуванням суттєвих відмінностей діяльності водолазів-саперів ДСНС від діяльності водолазів-саперів ВМС Збройних сил України. Одночасно, отримані висновки можуть відрізнятись за результатами аналізу діяльності міжнародних благодійних та некомерційних організацій, що займаються знешкодженням вибухонебезпечних предметів, які можуть становити небезпеку для цивільних осіб.

Віктор СТРІЛЕЦЬ, д.т.н., проф.
ORCID: 0000-0001-5992-1195
E-mail: vstrelec1956@ukr.net
Сергій СТЕПАНЧУК
НУЦЗУ
ORCID: 0000-0002-6618-4119
E-mail: stepanchukdsns@gmail.com

ПРОБЛЕМНІ ПИТАННЯ ГУМАНІТАРНОГО РОЗМІНУВАННЯ В РАДІАЦІЙНО-ЗАБРУДНЕНІЙ МІСЦЕВОСТІ

На цей час понад 95% території зони відчуження Чорнобильської АЕС, в першу чергу в лісистій місцевості, заміновано. Не є виключеним і мінування Запорізької АЕС або застосування російськими окупантами тактичної ядерної зброї. В доповіді показано, що важливою та нерозв'язаною частиною проблеми гуманітарного розмінування є відсутність закономірностей оперативної діяльності саперів ДСНС в умовах радіаційного забруднення.

Враховуючи унікальність такої ситуації (ніде в світі вона ніколи не розглядалась), яка є притаманною тільки Україні, коли сапер ДСНС повинен застосовувати як засоби бронезахисту, такі засоби індивідуального захисту органів дихання та шкіри, були проведені експериментальні дослідження щодо визначення закономірностей гуманітарного розмінування в умовах радіаційного забруднення в залежності від захисного спорядження. У якості контрольної вправи було обрано "здьоргування вибухонебезпечного предмету". Її вибір

пояснюється тим, що практика розмінування забрудненої вибухонебезпечними предметами місцевості після її звільнення від російських окупантів показала, що навіть на мирних територіях вони використовують підлу практику подвійного мінування, коли основна міна додатково мінується міною-ловушкою.

Робоча гіпотеза полягала в тому, що отримання закономірностей виконання типових операцій гуманітарного розмінування в умовах радіаційного забруднення саперами ДСНС у вигляді функцій розподілу часу їх виконання дозволить здійснити їх порівняльний кількісний аналіз з урахуванням обраного комплексу засобів індивідуального захисту особового складу. Реалізація запропонованого способу порівняльного аналізу закономірностей виконання типових операцій гуманітарного розмінування в умовах радіаційного забруднення саперами ДСНС здійснюється шляхом порівняння часу реалізації способу здьоргування протитанкової міни ПТМ, яка знаходиться на відстані 50 м від укриття, де розміщується сапер під час виконання найбільш небезпечної етапу, в трьох різних варіантах використання комплексу засобів індивідуального захисту піротехніками ДСНС за різних умов можливого радіаційного впливу: варіант 1 – комбінація захисного костюма Л-1, бронезахисту типу захисний бронежилет IV рівня захисту, захисний бронешолом III-А рівня захисту та респіратору типу 3М 6200 ffp3; варіант 2 – комбінація захисного костюма Л-1, бронезахисту типу захисний бронежилет IV рівня захисту, захисний бронешолом III-А рівня захисту та фільтрувального протигазу типу ГП-5; варіант 3 – комбінація захисного костюма Л-1, бронезахисту типу захисний бронежилет IV рівня захисту, захисний бронешолом III-А рівня захисту та апарата на стисненому повітрі типу Dräger 7000.

Порівняльний аналіз закономірностей гуманітарного розмінування в умовах радіаційного забруднення в залежності від захисного спорядження саперів ДСНС показав, що якщо, час виконання типових операцій в комплекті захисного спорядження, до якого входить ізолюючий апарат захисту органів дихання, суттєво (із рівнем значимості α=0,05) відрізняється від їх виконання в комплекті, до якого входить фільтрувальний протигаз, то час виконання в комплекті із респіратором класу ffp3 практично не відрізняється (на рівні значимості α=0,05) від часу виконання в комплекті із фільтрувальним протигазом.

Сильною стороною отриманих результатів є визначення достовірних показників (з рівнем значимості α=0,05), які можуть бути основою для обґрунтування конкретних пропозицій щодо організації робіт з гуманітарного розмінування в умовах радіаційного забруднення, вибору засобів індивідуального захисту, обґрунтування тактико-технічних вимог до них як на етапі створення, так і на етапі придбання, визначення особливостей підготовки саперів. Так, видно, що не має сенсу займатись подальшими дослідженнями особливостей відповідної діяльності саперів в респіраторах класу ffp3, оскільки кожний з них має індивідуально закріплений фільтрувальний. З урахуванням виконання більшості

робіт з гуманітарного розмінування в умовах радіаційного впливу на відкритій місцевості, основну увагу під час подальших досліджень доцільно приділити визначенню оперативно-технічних рекомендацій щодо підвищення ефективності відповідної оперативної діяльності в комплексах індивідуального захисту сапера, до складу яких входять фільтрувальні протигази.

Одночасно необхідно відмітити, що застосування обраного підходу в практичній діяльності супроводжується трудомісткістю проведення експериментальних досліджень, результати яких є основою для науково-обґрунтованих рішень щодо підвищення ефективності дій особового складу піротехнічних підрозділів в радіаційно-забрудненій місцевості, оскільки для здійснення цього процесу необхідно залучити висококваліфікованих спеціалістів, які одночасно мають знання та навички як в практиці розмінування та іншої оперативної діяльності в умовах радіаційного забруднення, так і в організації експериментальних досліджень таким чином, щоб були отримані статистично значимі результати, які стануть основою відповідних пропозицій.

Валерій СТРІЛЕЦЬ, к.т.н.
HALO Trust
ORCID: 0000-0003-1913-7878
E-mail: valerii.strilets@haloukraine.org
Віктор СТРІЛЕЦЬ, д.т.н., проф.
НУЦЗУ
ORCID: 0000-0001-5992-1195
E-mail: vstrelec1956@ukr.net

ОСОБЛИВОСТІ ПРОВЕДЕННЯ ДОСЛІДЖЕНЬ З ВІДКРИТИМ КОДОМ ЗАРАЖЕННЯ УКРАЇНИ ВИБУХОВИМИ БОЄПРИПАСАМИ (НА ПРИКЛАДІ HALO TRUST В УКРАЇНІ)

Повномасштабне вторгнення Росії в Україну, яке почалося в лютому 2022 року, стало “першою війною з відкритим кодом”, де майже кожен аспект конфлікту на землі має онлайн-еквівалент.

У відповідності до [1] в доповіді відмічено, що по мірі розвитку конфлікту та переміщення лінії фронту фахівці HALO Trust складають карту конфлікту та його руйнівних наслідків для України, включно з вибуховими боєприпасами, що залишилися в районах, де бойові дії припинилися. Розслідування HALO очолює цю роботу та змогло нанести на карту зараження вибухонебезпечними предметами по всій Україні. Це дозволяє їх оцінити та у відповідності до отриманих показників підвищити ефективність планування як операцій по

очищенню забрудненої території, так і по проведенню інформування та навчанню мирного населення ризикам (EORE) по всій країні.

В доповіді відмічено, що HALO почало працювати в Україні з кінця 2015 року на підконтрольних уряду територіях Донецької та Луганської областей. Протягом семи років команди HALO проводили нетехнічне обстеження (NTS), розмінування та навчання ризикам у цьому регіоні, зокрема вздовж лінії зіткнення, яка існувала до лютого 2022 року.

Повномасштабне вторгнення Росії 24 лютого 2022 року тимчасово призвело до того, що роботи щодо обстеження та розмінування зупинилися. В той час персонал зосередився на перевезенні сімей у безпечне місце на заході країни та допомагав у розподілі допомоги, навчанню щодо зниження рівня впливу можливих ризиків, а також навчанню з надання першої допомоги. Виведення військ росії з Київської, Чернігівської та Сумської областей на початку квітня 2022 року забезпечило вікно для безпечного відновлення операцій. HALO перемістила свою діяльність на базу поблизу Києва, щоб мати можливість працювати в цих трьох регіонах. Незважаючи на невизначеність на початкових етапах війни перед частковим виходом росії, HALO хотіла бути повністю готовою до майбутніх операцій і почала використовувати "дистанційний" підхід, щоб зрозуміти тип використовуваних вибухонебезпечних предметів, а також масштаб і вплив забруднення ними в Україні.

HALO розглядає дослідження з відкритим кодом як процес збору та аналізу законно зібраної інформації лише з загальнодоступних джерел, без використання таємних методів збору та без інформації з приватних чи секретних джерел. З початку Громадянської війни в Сирії в 2011 році та війни на сході України в 2014 році, дослідження з відкритим кодом стали константою сучасної війни, допомагаючи розвіяти туман війни [1]. Багато глобальних організацій використовують інформацію з відкритих джерел, зокрема ООН, для підтримки миротворчих операцій і планування доставки допомоги під час кризи чи стихійного лиха.

Раніше HALO використовувала дослідження з відкритим кодом для невеликого проекту в Тріполі (Лівія), де дослідники зосереджувалися на публікаціях у соціальних мережах, які публікували фотографії та відео, вказуючи на наявність протипіхотних мін і вдосконалених вибухових пристроїв. Потім точні місця виявлення забруднення були розміщені на карті поряд з лінією фронту битви за Тріполі в 2018 році. Визначення місць розташування боєприпасів, що не розірвалися, і фронтів бойових дій дозволило HALO підготуватися до NTS – процесу ідентифікації та позначення підозрюваних і підтверджених небезпечних зон – і визначити пріоритетні території з високим рівнем забруднення та високим рівнем людської діяльності.

З березня 2022 року цей підхід успішно застосовано та розширено в контексті України. Війна в Україні є, безумовно, найактивнішим з усіх часів конфліктом,

який знайшов найактивніше відображення у соціальних мережах. Це дозволяє HALO використовувати великий обсяг інформації, використовуючи дослідження з відкритих джерел для збору та аналізу даних про забруднення вибухонебезпечними предметами в Україні. Це, у свою чергу, дозволило HALO краще планувати та проводити операції, а також здійснювати діяльність щодо інформування про можливі ризики і доцільну поведінку мирного населення ефективніше та результативніше. Це включає визначення пріоритетів для розгортання груп нетехнічного обстеження і груп очищення, інформування керівництво HALO про закупівлю найбільш відповідного обладнання для зниження рівня очікуваної загрози.

Поточна методологія дослідження відкритого коду HALO включає п’ять основних етапів:

1. Визначення кінцевих цілей і спрямованості дослідження.
2. Визначення джерел.
3. Пошук в Інтернеті.
4. Перевірка/геолокація подій.
5. Картографування, порівняння та аналіз даних.

На цей момент HALO зібрав і перевірив більше ніж двадцять тисяч унікальних подій у тринадцяти категоріях.

Дослідження HALO виявили 400 унікальних типів вибухових боєприпасів, які використовувалися під час конфлікту, переважно боєприпаси російського чи радянського виробництва, а також багато західних зразків. Наразі HALO не відстежує різні види стрілецької зброї та легкої зброї (SA/LW).

Однією з головних проблем є неможливість зібрати всю інформацію про забруднення вибуховими речовинами по всій Україні. Хоча рівень деталізації у висвітленні конфлікту є величезним (до такого рівня, що це створює проблему інформаційного перевантаження), можна очікувати наявність вибухових подій, про які не повідомлятимуть через туман війни та величезний масштаб війни в Україні.

В доповіді показано, що існуючу методологію дослідження відкритого коду HALO доцільно вдосконалити з урахуваннями існуючих наукових підходів в Україні. В першу чергу, для вибору місць розмінування використовувати результати статистичного аналізу отриманих даних: оцінок співвідношення між відкритою початковою інформацією та реальними результатами після розмінування; оцінок розподілів часу розмінування в залежності від різноманітних вихідних даних (географічних та кліматичних умов, оснащення демінерів, рівня їх підготовленості тощо); оцінок зв’язку між параметрами розподілів часу розмінування з інформацією, яка була у відкритих джерелах.

Крім того, результати дослідження відкритого коду HALO в Україні повинні використовуватись у якості вихідних даних для дослідження особливостей використання демінерами роботизованої техніки розмінування з тим, щоб:

– поряд із визначенням компетенцій щодо знань та вмінь щодо користування нею обґрунтувати компетенції щодо навичок (як показник цього можна використати час виконання як окремих операцій, так і закінчених процесів виконання робіт з розмінування на полігоні);

– визначити типові помилки та статистичні оцінки часу виконання окремих операцій та закінчених процесів під час полігонних випробувань, підготовки операторів-демінерів, їх тренувань;

– оцінки ефективності підконтрольної експлуатації роботизованої техніки;

– визначення особливостей використання засобів захисту демінерів (як засобів індивідуального захисту від різних виробників, так і оцінки засобів групового захисту).

Таким чином, результати дослідження відкритого коду HALO в Україні повинні використовуватись не тільки для конкретизації місць проведення гуманітарного розмінування, але й для визначення відповідних оперативно-тактичних рекомендацій щодо використання сучасної техніки під час гуманітарного розмінування та обґрунтування тактико-технічних вимог до нових зразків техніки.

Список використаних джерел:

1. Mathewson, Andro (2022) “Open-Source Research and Mapping of Explosive Ordnance Contamination in Ukraine,” *The Journal of Conventional Weapons Destruction*: Vol. 26: Iss. 1, Article 3. Available at: https://commons.lib.jmu.edu/cisr-journal/vol26/iss1/3.

Тарас ТЛУМАК
НУОУ
ORCID 0009-0004-8900-2279
E-mail tarastlumak07@gmail.com

АНАЛІЗ ЗМІСТУ ЗАХОДІВ БЕЗПЕКИ ОПЕРАЦІЙ, ЯКІ ЗАСТОСОВУЮТЬСЯ В ІНТЕРЕСАХ ВІЙСЬК (СИЛ)

Безпека операцій являю собою спроможність, що визначає та контролює критично важливу інформацію, індикатори діяльності військ (сил), що відносяться до операцій і включає контрзаходи для зниження ризику використання противником вразливих місць.

Аналіз джерел [1-3] показує, що термін “безпека операцій” вперше був введений в армії США під час війни у В’єтнамі під час проведення комплексу

спеціальних заходів (операції) “Purple Dragon”[2]. Метою цієї операції була протидія отриманню розвідкою Північного В’єтнаму і Національного фронту визволення Південного В’єтнаму (в’єт. – Việt cộng) інформації про застосування ВПС США. Вона передбачала дослідження прогалин у ході повітряних операції “Arc Light” і “Rolling Thunder”, коли військове командування США дійшло висновку, що противник якимсь чином постійно уникав ураження у ході застосування авіації США та їх союзників. Бомбардувальні місії в 1966 році не мали значного впливу на В’єтконг і Північну В’єтнамську армію. Розвідувальна інформація та оцінка вогневого ураження цілей, по яких було застосовувалися бомбардувальники B-52, показали менші втрати ворога в людях і матеріальних ресурсах, ніж очікувалося. Інфільтрація людей та ресурсів Північного В’єтнаму до Південного В’єтнаму не була зупинена. Навіть після року бомбардувань, бойовий дух противника залишався високим, а військова та промислова діяльність Північного В’єтнаму не здавалася сильно порушеною. Розглядалося дві версії, перша – недостовірність розвідки США щодо місцезнаходження та сили противника, і друга, загрозливіша, – чи не передається інформація про вильоти авіації наперед, надаючи В’єтконгу та Північній В’єтнамській армії можливість уникнути її ударів. Противник не міг розшифрувати захищену систему комунікацій ЗС США і не мав достатньої кількості шпигунів у Південному В’єтнамі, щоб відслідковувати кожен виліт авіації США в Південно-Східній Азії. Тому було зроблено припущення, що американські війська якимось чином самі ненавмисно розголошують інформацію.

Тому метою тез є повести аналіз змісту заходів безпеки операцій, які застосовуються в інтересах військ (сил) для визначення основних підходів, щодо їх класифікації.

Процес безпеки операцій – це систематичний метод, який використовується для виявлення, контролю та захисту важливої інформації та подальшого аналізу діяльності, пов’язаних із військовими операціями, щоб:

визначити ті дії, які можуть бути виявлені розвідувальними системами противника;

визначити, які конкретні ознаки можуть бути зібраними, проаналізованими та інтерпретованими для своєчасного отримання важливої інформації, яка стане корисною для противника;

обрати контрзаходи, які усувають або зменшують уразливість або знижують виявлення та використання індикаторів, а саме:

уникати різких змін по мірі впровадження контрзаходів безпеки операцій. Зміни в процедурах можуть дати свідчення противнику про початок операції або навчання;

запобігати витоку (виявленню) або можливості збору важливої інформації, особливо під час підготовки та проведення реальних операцій;

уникати сталих моделей (шаблонів) поведінки, у всіх випадках коли це можливо, щоб виключити можливість побудови розвідкою противника точної моделі;

захищати цикл прийняття рішень командиром і забезпечити варіативність (гнучкість) військових дій.

Безпека операцій – це помножувач сил, який може максимізувати оперативну ефективність, економити людські та матеріальні ресурси при інтеграції в операції, заходи, плани, навчання, підготовку та спроможності.

Безпека операцій в НАТО визначається як "процес, що забезпечує військовим операціям або навчанням належну безпеку, використовуючи пасивні або активні засоби, для недопущення отримання противником основних елементів дружньої інформації або їх індикаторів.

Безпека операцій в США має деякі відмінності від підходу НАТО він складається із п'яти кроків:

ідентифікація критичної інформації;

аналіз загроз;

аналіз вразливостей;

оцінка ризику;

проведення відповідних заходів протидії безпеці операцій противника.

Таким чином, аналіз змісту заходів безпеки операцій, які застосовуються в інтересах військ (сил) показав, що в їх основі є послідовність результатів запланованих повторюваних процедур в яких досягається певна мета.

Список використаних джерел

1. Christopher Paul, Jessica Yeats, Colin P. Clarke, Miriam Matthews, Lauren Skrabala. Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade. Handbook for Practitioners. Santa Monica, California: The RAND National Defense Research Institute, 2015. 108 p. URL: http:// www.rand.org/pubs/research_reports/RR809z2.html.

2. Kofman M., Migacheva K., Nichiporuk B., Radin A., Tkacheva O., Oberholtzer J. Lessons from Russia's Operations in Crimea and Eastern Ukraine, Santa Monica, California: The RAND National Defense Research Institute, 2017.

3. Матеріали дослідження збройних сил США "Hierarchy of Psychological Effects Model: an Application of Communicative and Influence Theories Towards a Military Information Support Operations Framework".

Юрій ЯКИМЕНКО, к.військ.н., доцент
ORCID: 0000-0002-6848-852X
E-mail: yakum14@ukr.net
Михайло ЗАПОРОЖЧЕНКО
ДУІКТ
ORCID: 0000-0003-0182-9497
E-mail: zaporozhchenkomm@gmail.com

ОСНОВИ ПСИХОЛОГІЧНОГО ЗАХИСТУ ВІД СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Соціальна інженерія – це спосіб впливу на людину з метою отримання від неї конфіденційної інформації або спонукання її до реалізації певних дій, які в подальшому можуть допомогти зловмиснику в плануванні та скоєнні кіберзлочинів.

Одними з основних цілей соціальної інженерії є проникнення в інформаційні системи компаній в обхід систем безпеки, крадіжка логінів та паролів користувачів та адміністраторів, отримання номерів та PIN-кодів від кредитних карток та іншої важливої інформації.

Для того, щоб подолати корпоративну систему захисту, зловмиснику необхідно витратити час для того, щоб знайти вразливості в інформаційній системі, знайти чи написати власний експлойт та визначитися зі способом його доставки, реалізації та закріплення. Зазвичай це доволі тривалий процес, який вимагає ретельної підготовки, протягом якої зловмисник паралельно шукає будь-яку інформацію про персонал цільової організації, яка може допомогти йому при реалізації атаки. Оскільки у працівників організації вже є відповідні права доступу, зловмиснику легше експлуатувати людський фактор, ніж долати багато шарів технічного та програмного захисту. Неналежно підготовлений персонал або персонал, діяльність якого напряму не пов’язана з інформаційною безпекою, в більшості випадків стане причиною інциденту, про що свідчать численні звіти з описом актуальних інформаційних загроз, в яких соціальна інженерія та, зокрема, фішинг, протягом кількох останніх років входять до рейтингу найнебезпечніших та найрозповсюдженіших загроз.

Якщо говорити не про співробітників організацій, а про звичайних користувачів, то їх ввести в оману ще легше: можна зробити це за допомогою звичайного листування чи дзвінка, використовуючи різноманітні психологічні маніпуляції, і на відміну від організацій, в цьому випадку зловмисник необов’язково має володіти глибокими технічними знаннями та навичками.

Часто одним з психологічних прийомів, які використовують соціальні інженери, є завоювання довіри жертви. Завоювання довіри передбачає пошук інформації про жертву, допомогти у якому можуть куплені бази з даними про користувачів, пошукові системи або пости в різноманітних соцмережах, особливо

якщо жертва активно веде їх. Після того, як була зібрана достатня кількість інформації, зловмисники можуть написати листа чи подзвонити жертві і представитися особами, від яких мало хто буде чекати обману, наприклад, родичами або близькими знайомими жертви, навіть голос яких можна скопіювати за допомогою штучного інтелекту [1], або ж представниками офіційних установ: банків, поліції, аж до організації, в якій працює жертва чи школи, в якій навчаються її діти. Внаслідок завоювання довіри зловмисник може змусити жертву перейти на сайт-підробку для введення своїх банківських даних, розкрити свої персональні дані, перевести гроші, відключити захист на пристрої і багато іншого, що може допомогти йому у реалізації кібератаки.

Однією з характерних особливостей соціоінженерних атак є акцентування уваги на терміновості, внаслідок якої у жертви складається відчуття невідкладності і вона не має часу адекватно оцінити ситуацію, і тому приймає рішення швидко і під тиском, і ці рішення, як правило, виявляються необґрунтованими і невірними. Для цього соціальні інженери можуть застосовувати погрози, обман, маніпуляції та інші методи – все, що може змусити жертву діяти швидко.

Наприклад, працівнику організації може прийти повідомлення про те, що на його робочому місці виявлено підозрілу активність або здійснюється витік даних, і для блокування цієї активності необхідно якомога швидше виконати певні інструкції. В такому випадку поєднуються фактори – терміновості та страху: працівник боїться понести відповідальність за те, що він став причиною інциденту, і в додаток до цього в нього є можливість все швидко виправити, поки ніхто не дізнався. Якщо говорити про звичайних користувачів, розповсюдженими прикладами прояву терміновості є повідомлення про зараження пристрою вірусами, блокування облікових записів, банківських карток та інші.

Наступні фактори стосуються скоріше звичайних користувачів: перший з них можна описати як страх втратити гроші. Типовим сценарієм атаки з використанням такого прийому може слугувати така ситуація: жертва отримує дзвінок від зловмисника, який представляється співробітником банку, в якому обслуговується клієнт, і повідомляє, що з його картки прямо зараз здійснюється переказ коштів на інший нетиповий рахунок, або ж проводиться онлайн-оплата на значну суму, і якщо ініціатор цієї оплати не він, то необхідно її заблокувати чи скасувати, повідомивши “співробітнику банку” CVV2 / CVC2 код картки. При цьому дуже часто зловмисник спілкується впевнено та грамотно, що присипляє пильність жертви, і він навіть може володіти інформацією про номер картки та персональні дані жертви. Страх втратити гроші у сукупності з фактором терміновості та довірою до представника банку можуть призвести до того, що зловмисник отримає доступ до банківського рахунку жертви і потенційна втрата коштів для неї стане реальною.

Також одним із поширених методів соціальної інженерії є заманювання цільової аудиторії вигідними пропозиціями чи обіцянками легких грошей. Ці обманні методи ґрунтуються на психологічних механізмах, таких як бажання

отримати щось безкоштовно, прагнення до збагачення та стимулювання цікавості. Дуже часто такі прийоми застосовуються у контексті криптовалют. Наприклад, в травні 2021 року на платформі YouTube зловмисники одночасно вели декілька трансляцій від імені Ілона Маска, в яких було сказано, що він виділив 500 млн. DOGE, які будуть роздані всім власникам даної криптовалюти. Для цього всім бажаючим необхідно було перейти за прикріпленим до трансляції посиланням, відкривши яке пропонувалося відправити Dogecoin на блокчейн-адресу і отримати у 2 рази більше. В результаті було викрадено криптовалюти приблизно на 5 млн. американських доларів. Як не дивно, але подібні методи досі працюють в силу того, що люди люблять отримати грошові винагороди, залишатися у виграші за виконання простих дій [2].

Особливістю соціальної інженерії та її істотною відмінністю від інших типів кібератак є той факт, що жертва самостійно переходить за шкідливим посиланням, завантажує на свій пристрій шкідливе програмне забезпечення, надає зловмиснику інформацію чи пересилає кошти. Тобто чи буде вона обманута, чи ні, залежить тільки від неї. Розуміння механізмів психологічного впливу для проведення соціоінженерних атак може допомогти звичайним користувачам та організаціям виявити, яким чином вони піддаються маніпуляції, та на основі цих знань вжити відповідних заходів для захисту своїх конфіденційних даних.

Не стати жертвою соціальних інженерів допоможе дотримання дуже простих правил, перше з яких – не довіряти незнайомцям. Якщо телефонують з установи, до якої людина останнім часом не зверталася, та пропонують вирішити якісь проблеми, уточнити дані, рекламують якісь ексклюзивні пропозиції, доцільніше буде не спілкуватися з ними, а за необхідності передзвонити за телефоном, вказаним на офіційному сайті. Також варто пам’ятати, що ймовірність того, що велика організація телефонуватиме своєму клієнту через будь-який з месенджерів, дуже мала. Зі знайомими та родичами така сама ситуація: якщо зміст повідомлення чи дзвінка викликає підозри, то краще скинути та передзвонити самостійно.

При розмові чи листуванні варто звертати увагу на певні деталі, які можуть бути притаманні зловмиснику, наприклад, з очевидного – невідома пошта чи телефон. Потрібно звертати увагу і на ім’я пошти, і на домен: скоріш за все, у великій організації не будуть використовуватися безкоштовні поштові домени та безглузді імена. Також необхідно помічати, коли співрозмовник намагається привернути увагу чи нагнітає обстановку, наприклад, повідомляє про злом чи блокування облікового запису жертви, про помилковий переказ коштів, пропонує взяти участь в акції, обіцяє грошову компенсацію і при цьому чинить тиск на жертву, змушуючи її поспішати, щоб не дати можливість адекватно оцінити обстановку. Зловмисники, які доставляють листи електронною поштою, часто допускають помилки, щоб обійти спам-фільтри, тому на це також слід звертати увагу і ставитися до таких листів з особливою уважністю. В тому разі, якщо на пошту було надіслано посилання без супровідного тексту, нехай навіть від

знайомого відправника, є ймовірність того, що його обліковий запис було скомпрометовано, тому необхідно або уточнити в нього факт відправки та зміст даного посилання, або ж перевірити його за допомогою спеціальних сервісів [3].

Якщо говорити про соціоінженерні атаки, пов'язані з терміновістю, ключовим завданням в таких випадках є збереження холоднокровності та здорового глузду у критичних ситуаціях. Необхідно враховувати, що зловмисники використовують терміновість для того, щоб змусити жертву діяти швидко, не замислюючись над наслідками її дій, оскільки роздуми та аналіз ситуації можуть допомогти уникнути помилок. Для захисту від подібних атак доцільно буде спокійно оцінити ситуацію, визначити, наскільки невідкладними насправді є дії, ні в якому разі не піддаватися на провокації та погрози від зловмисника, ретельно перевіряти інформацію, перш ніж вживати будь-яких заходів, не довіряти невідомим відправникам, використовувати антивірусні програми та складні паролі.

Для корпоративних користувачів необхідно регулярно проводити навчання та тренінги з питань інформаційної безпеки, розглядати існуючі на даний момент та актуальні для сфери діяльності, в якій функціонує організація, загрози та ризики інформаційної безпеки, в тому числі методи соціальної інженерії, їх особливості та способи протидії. Доцільно також буде проводити аудит інформаційної безпеки, зокрема із застосуванням методів соціальної інженерії для виявлення вразливостей в інформаційній системі та недоліків в програмі навчання співробітників та на основі результатів перевірки вдосконалювати їх. І, звісно, не можна нехтувати інструментами для захисту співробітників від взаємодії зі зловмисниками та захисту даних компанії: мають бути впроваджені DLP-системи для попередження витоку конфіденційної інформації за мережевий периметр відділу чи організації, “пісочниці” для захисту від невідомих загроз, захист електронної пошти від спаму та фішингу, мережеві та хостові антивіруси, які здатні виявляти шифрувальників та троянів у повідомленнях, налаштування URL-фільтрації, сервіси операторів зв’язку для блокування зловмисників на основі репутаційних баз і багато інших заходів та засобів захисту.

Соціальна інженерія залишається актуальною загрозою для великої кількості корпоративних та звичайних користувачів. Варто пам’ятати, що в мережі знаходяться величезні об’єми даних, серед яких наявна інформація, яка може бути застосована відносно конкретної особи чи організації для підготовки правдоподібного сценарію соціоінженерної атаки, ціллю якої може стати кожен. Власне тому розуміння принципів та механізмів маніпуляції, яка здійснюється зловмисниками, вкрай важливе для захисту від подібних атак.

Список використаних джерел:

1. Elad Rapaport. VALL-E – The Future of Text to Speech? 2023. URL: https://towardsdatascience.com/vall-e-the-future-of-text-to-speech-d090b6ede07b.

2. Saturday Night Scam: How scammers exploited Elon Musk and SNL to reap millions in cryptocurrency. 2021. URL: https://www.trmlabs.com/post/dogecoin-elon-musk-snl-scam.

3. Тетяна Савчук. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті. 2018. URL: https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html.

Роман ЯРЕМКО, к.психол.н.
ЛДУ БЖД
ORCID: 0000-0002-2781-7788
E-mail: r.yaremko@ldubgd.edu.ua

МОТИВАЦІЯ МАЙБУТНІХ ФАХІВЦІВ З ПОЖЕЖНОЇ БЕЗПЕКИ ДО ЗДІЙСНЕННЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В ОСОБЛИВИХ УМОВАХ

Розуміння особливостей обраної професії, процесу навчання та професійної діяльності вимагає врахування того, що для особистості набувають значення професійні цілі, зміст діяльності та професійно-етичні стандарти. Однак бажання стати професіоналом і сам процес становлення особистості як фахівця в багатьох відношеннях залежать від професійної мотивації.

На основі теоретичного аналізу поняття мотивації можна розглядати в двох аспектах: Мотивація як комплекс психологічних факторів, які спонукають працівника до виконання певних дій або конкретних моделей поведінки, включаючи потреби, наміри, прагнення, мотиви та цілі. Мотивація як механізм управління, який спонукує працівника до певної діяльності та спрямовує його на досягнення відповідного результату [1].

Мотивація визначає стан професійної діяльності особистості і залежить від співвідношення різних мотивів які постійно змінюються, включаючи мотиваційну сферу. До цих мотивів входять: професійне покликання, професійні наміри, потреба у професійній діяльності, ціннісні орієнтації у професійній діяльності та мотиви, пов'язані з професійною діяльністю [2].

Для визначення професійної мотивації майбутніх рятувальників необхідно звернути увагу на особливості їх майбутньої діяльності. Оскільки рятувальники працюють у складних та ризикованих умовах, де завдання можуть бути пов'язані із загрозою для життя та здоров'я як для рятувальників, так і для потерпілих. Ця професія також вимагає високого рівня відповідальності за професійні помилки і може призвести до нанесення шкоди колегам і постраждалим під час виконання службових завдань.

Здійснивши аналіз особливостей діяльності працівників аварійно-рятувальних підрозділів можна стверджувати, що професійна мотивація майбутніх рятувальників представляє собою процес і результат формування значущих мотивів, які виникають з усвідомлення цінності їхньої майбутньої професії, визначення основних аспектів службової діяльності та виконання службових обов'язків. Оскільки мова йде про майбутніх рятувальників – здобувачів вищої освіти, де передбачені специфічні умови навчання, то важливо відзначити, що відповідальність за створення сприятливої мотивації до служби та усвідомлення особливостей майбутньої діяльності значною мірою залежить від професорсько-викладацького складу.

Зважаючи на те, що професійна мотивація майбутніх рятувальників залежить від розвитку важливих професійних мотивів, можна констатувати, що в процесі вибору цієї професії різні мотиви переважають для різних осіб. Для деяких, ці мотиви включають суспільне визнання, бажання досягти власного самовдосконалення та альтруїстичні наміри, в той час як для інших важливими є висока та стабільна заробітна плата та можливість встановлення впливових соціальних зв'язків.

Щодо систематизації професійних мотивів осіб, які обирають ризиковані професії, можна відзначити, що найбільш докладною є класифікація, представлена О.В. Тимченко. У цій класифікації виділено п'ять основних типів професійних мотивів, а саме:

адекватний тип, де ціннісні установки та пов'язані з ними професійні мотиви повністю відповідають соціальному поведінці конкретної особистості;

ситуативний тип, пов'язаний із привабливістю професії в романтичному аспекті або з матеріальними інтересами;

конформістський тип, характерний для осіб, які обрали професію під впливом своєї референтної групи;

компенсаторний тип, який проявляється у тих, хто прагне компенсувати свої власні слабкі сторони через вибір конкретної діяльності;

кримінальний тип, який характеризується антисоціальною спрямованістю та бажанням використовувати свою професію в особистих цілях [3; 4].

Підсумовуючи, можна стверджувати, що мотивація у професійній діяльності є динамічним процесом, який змінюється відповідно до різних етапів професійного розвитку фахівця. Для здобувачів вищої освіти із специфічними умовами навчання, професійна мотивація є важливим фактором успішної реалізації в майбутній професійній діяльності. Таким чином, під поняттям "професійна мотивація майбутніх рятувальників" маємо на увазі динамічну систему психологічних характеристик, які будуть регулювати та стимулювати поведінку майбутніх рятувальників у нестантдартних та особливих умовах діяльності.

Список використаних джерел:

1. Вавринів О.С. Професійна мотивація майбутніх рятувальників до діяльності в особливих умовах. *Психологічні засади забезпечення службової діяльності працівників правоохоронних органів:* матеріали І Всеукраїнської науково-практичної конф. (Кривий Ріг 15 лютого 2018 р.). Кривий Ріг 2018. С.

2. Ковальчук О.П. Теоретичні аспекти дослідження мотивації професійної діяльності військовослужбовців / О.П. Ковальчук // Вісник Національного університету оборони України. - 2011. - № 21. - С. 135–139.

3. Тімченко О.В. Професійний стрес працівників органів внутрішніх справ України (концептуалізація, прогнозування, діагностика та корекція): дис. доктора психол. наук: 19.00.06 / Тімченко Олександр Володимирович. - Харків, 2003. – 427 с.

4. Vavryniv, O.S., Yaremko, R.Ya. Empathy as a factor in the development of personal components of future rescuers' professional self-realization. Insight: the psychological dimensions of society, 2022, 8, 56-69. DOI: 10.32999/2663-970X/2022-8-5.

Наукове видання

СТРАТЕГІЧНІ КОМУНІКАЦІЇ У СФЕРІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ: ПРОБЛЕМИ, ДОСВІД, ПЕРСПЕКТИВИ

IV МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

Тези доповідей

Матеріали подано в авторській редакції.
Відповідальність за достовірність фактів, цитат, власних імен та інших даних несуть автори

Комп’ютерна верстка: Ярослав ЛАШИН