НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ УКРАЇНИ
ІМЕНІ ІВАНА ЧЕРНЯХОВСЬКОГО


# МАТЕРІАЛИ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

# ІНФОРМАЦІЙНИЙ ВИМІР ГІБРИДНОЇ ВІЙНИ: ДОСВІД УКРАЇНИ

Київ-2017

Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. – Київ: НУОУ, 2017. – 104 с.

Під час роботи конференції були обговоренні актуальні проблеми забезпечення інформаційної безпеки держави в умовах гібридної війни, визначено сутність та змісту інформаційної політики держави.

Учасники конференції обговорювали питання правил протидії гібридній агресії Російської Федерації проти України, форми та засоби ведення гібридної війни Російської Федерації проти України. Інформаційні загрози національній безпеці держави та наслідки їх реалізації, провели аналіз інформаційної кампанії Російської Федерації проти України з початку 2014 по теперішній час, розглянули досвід провідних країн світу щодо реалізації інформаційної політики держави в умовах воєнних конфліктів, шляхи вдосконалення інформаційної політики України. Також розглянуті проблемні питання узгодження заходів реалізації інформаційної політики держави з інформаційними та психологічними операціями Збройних Сил України, підготовки та ведення інформаційних та психологічних операцій Збройних Сил України, організації системи міжнародного співробітництва щодо спільної протидії російській інформаційній агресії.

Співорганізаторами конференції виступили Управління інформаційних технологій Міністерства оборони України, Національний інститут стратегічних досліджень, Центр інформації та документації НАТО в Україні.

## ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

| | |
|---|---|
| Голова: | САВЧЕНКО В.А., доктор технічних наук, старший науковий співробітник. |
| Заступник голови: | ДЗЮБА Т.М., кандидат технічних наук, доцент. |
| Члени оргкомітету: | СОЛОННІКОВ В.Г., доктор технічних наук, професор. |
| | БИЧЕНОК М.М., доктор технічних наук, старший науковий співробітник. |
| | КАЦАЛАП В.О., кандидат військових наук. |
| Секретар: | ПРИЙМАК М.В. |

Затверджено протоколом засідання кафедри застосування інформаційних технологій та інформаційної безпеки № 14 від 12 травня 2017 року

Відповідальність за зміст поданих матеріалів несуть автори

Тимчасово виконуючий обов’язки начальника Національного університету оборони України імені Івана Черняховського
генерал-майор ЩИПАНСЬКИЙ Павло Володимирович

Шановні учасники конференції!

Щиро вітаю Вас у стінах Національного університету оборони України імені Івана Черняховського.

Минуло вже три роки, як ми знаходимося у стані неоголошеної гібридної війни з Російською Федерацією. Інформаційна складова гібридної війни стала однією з ключових у російській агресії проти України.

Спираючись на потужну багаторічну інформаційно-психологічну обробку громадян, Росії на перших етапах її агресії вдалося істотно дезорганізувати населення України.

Крім того, в ході проведення антитерористичної операції неодноразово зафіксовано випадки:

застосування противником засобів радіоелектронної боротьби;

захоплення телекомунікаційних об’єктів;

здійснення кібератак проти державних органів та об’єктів критичної інфраструктури України.

Російська агресія змусила нас переглянути підходи щодо інформаційної політики держави, застосування Збройних Сил України та використання кіберпростору в нових умовах.

Виконуючи завдання Президента України – Верховного Головнокомандувача Збройних Сил України щодо нарощування обороноздатності держави, в Україні було затверджено Концепцію розвитку сектору безпеки і оборони України, нові редакції Стратегічного оборонного бюлетеня України та Воєнної доктрини України, а також Державну цільову оборонну програму розвитку озброєння та військової техніки і Державну програму розвитку Збройних Сил України на період до 2020 року, в яких, відповідно до світових тенденцій, базовим є акцент на розвиток спроможностей

сектору безпеки та оборони держави, у тому числі і щодо дій в інформаційному просторі.

Разом з тим, вжиті заходи навряд чи можна вважати достатніми для подолання складної ситуації у сфері інформаційного протиборства. Агресор постійно удосконалює форми і способи інформаційного впливу, застосовує сучасні технологічні підходи, розширює географію та залучає нові цільові аудиторії.

Відтак, нагальним завданням сьогодення є визначення концептуальних, теоретичних і практичних підходів щодо протидії російській агресії в інформаційному просторі сучасної України, у тому числі за досвідом країн-членів НАТО. Це і є основним лейтмотивом нашої конференції.

У роботі конференції беруть участь представники 27 організацій та установ. Таке широке наукове представництво дає можливість якісно і ефективно провести обговорення проблем за тематикою конференції.

Хочу подякувати всім за те, що знайшли час і можливість взяти участь у роботі конференції.

Запрошую до конструктивної та плідної праці.

**Зміст**

д-р техн. наук Андрощук О. С.
канд. психолог. наук Андрощук О. Ю.

# ПІДХОДИ ЩОДО ДОБУВАННЯ ТА АНАЛІЗУ ІНФОРМАЦІЇ В ОПЕРАТИВНО-РОЗШУКОВІЙ ТА РОЗВІДУВАЛЬНІЙ ДІЯЛЬНОСТІ

В останній час спостерігається поява нових та посилення традиційних загроз національній безпеці. Це вимагає інтенсифікації різних напрямків діяльності військових формувань і правоохоронних органів, у тому числі оперативно-розшукової та розвідувальної діяльності (далі – ОРД). Потреба в нових методах управління оперативно-розшуковими підрозділами особливо проявляється під час кримінального аналізу – відносно нового напрямку діяльності, про що свідчить мала кількість наукових публікацій. Кримінальний аналіз дозволяє суттєво підвищити якість та результативність діяльності слідчих та оперативних працівників, а останнім часом, ураховуючи досвід АТО, – і розвідників. Актуальним завданням є розробка підходів щодо добування та аналізу інформації, яка є вихідною для кримінального аналізу.

У роботі було запропоновано модель та методику кримінального аналізу у підрозділах ДПСУ на підставі нечіткої логіки. Як вхідні змінні вибрано ознаки правопорушення на ділянці ДК. Вихідна змінна є показником ступеня можливості використання ділянки для здійснення правопорушення у сфері безпеки ДК.

Цей підхід виявився достатньо новим на відміну від впровадженого у системі «Analyst’s Notebook». Аналіз її застосування свідчить, що відпрацьовано питання автоматизації виявлення та візуалізації зв’язків особи, що причетна до незаконної діяльності (в основному на підставі телефонних дзвінків).

Здійснення кримінального аналізу та інших видів оперативно-розвідувальної діяльності передбачає наявність інформації, яку необхідно отримати (добути) і проаналізувати.

Витяг з документальних носіїв нових знань про осіб, обізнаних про злочинну діяльність, про факти та події, що стосуються сфери та інфраструктури соціально-аномального та ворожого середовища, передбачає: пошук даних, що стосуються контрольного переліку потреб в інформації оперативно-розшукового характеру; визначення кола джерел, що її містять; специфічну інтелектуальну роботу з вивчення добутої інформації з метою встановлення ознак і напрямів злочинних діянь, осіб, які намагаються скоїти або скоїли злочинні діяння, формулювання результатів цієї роботи для вироблення адекватних оперативно-розшукових та профілактичних заходів.

Ураховуючи викладене, процес добування і аналізу (аналітичного пошуку) слід розуміти як таку, що має цільову спрямованість відповідно до оперативно-розшукового процесу, планомірну, упорядковану в часі і регламентовану законодавчими та іншими правовими актами сукупність етапів добування і подальшого аналізу за допомогою певних методик оперативних даних, зафіксованих на матеріальних носіях.

Основними складовими добування і аналізу є:

а) пошук відомостей кримінального характеру, що містяться в конфіденційних і відкритих документальних джерелах, базах та банках даних;

б) подальше дослідження зібраної та систематизованої інформації, розробка рекомендацій щодо її реалізації;

Добування та аналіз передують різним видам кримінального аналізу, для якого міжнародна практика оперативно-розшукової та розвідувальної діяльності виробила такі основні форми:

Crime pattern analysis (аналіз кримінальної обстановки) – дослідження злочинності у специфічній області та/або певному інтервалі часу (приблизно відповідає кримінологічному регіональному аналізу);

Generalprofile analysis (аналіз загального профілю) – вивчення специфіки вчинення злочинів певної категорії;

Methods analysis (аналіз методів) – вивчення та оцінка методів контролю, стримування та іммобілізації злочинності;

Case analysis (аналіз конкретного розслідування) – криміналістичний аналіз справи з урахуванням напрямів розслідування, що виходять за межі даної справи;

Comparativ analysis (порівняльний аналіз) – вивчення «почерку» злочинця;

Offender group analysis (аналіз групової злочинності) – виявлення напрямків злочинної діяльності та системи, зв’язків осіб стосовно групи, спільноти осіб, об’єднаних загальним злочинним задумом;

Specific profile analysis (аналіз особливостей профілю) злочинця – складання профілю злочинця в межах конкретного розслідування з метою його персоніфікації (визначення віку, морфологічних, інтелектуальних і психологічних особливостей, регіонів проживання та здійснення протиправних діянь тощо);

Investigation analysis (аналіз розслідування (оперативних і слідчих дій) – вивчення проведеного кримінальною структурою розслідування в межах конкретного випадку перед передачею справи в суд.

Отже, наведені вище форми кримінального аналізу мають досить чітко окреслені предметні області. Добування та аналіз інформації орієнтовані на оперативно-розшуковий процес, будучи ключовим елементом першої стадії кримінального аналізу, що забезпечує виявлення, а потім припинення і розкриття таємної з елементами маскування протиправної діяльності і, отже, може використовувати елементи будь-якого з видів дослідної роботи для виявлення даних, що цікавлять оперативний та розвідувальний апарат.

Інформаційно-аналітична робота оперативного підрозділу має на меті збір, зберігання, аналіз, оцінку і реалізацію не лише оперативної, а й іншої корисної інформації, що стосується діяльності оперативного підрозділу. Тому добування і аналіз можна розглядати і як один із специфічних елементів інформаційно-аналітичної роботи опер(розвід)апарату в цілому.

Одним із шляхів аналітичного пошуку є побудова та дослідження математичних моделей, що відображають закономірності пошукових процедур

і дозволяють встановити причинно-наслідкові відносини між умовами виконання пошуку та його результатами. Проблемний пошук передбачає максимально широке охоплення джерел даних, що стосуються мети пошуку.

Розглянемо основні фази процесу аналітичного пошуку.

Оцінка даних. Після того як дані зібрано, необхідно визначити, якою мірою вони є корисними для оперативно-розшукової діяльності.

Етап оцінки відомостей містить у себе: вивчення змісту добутої інформації з погляду її достовірності та інформативності документа-носія, надійності джерела; визначення потреби подальшого опрацювання отриманої інформації силами операпарату або за допомогою інших формувань та (або) з'ясування необхідності обмежитися внесенням даних в інформаційні системи; перегляд і вивчення інформації спеціальним суб'єктом-керівником оперативного підрозділу.

У цьому сенсі етап оцінки спрямовано на отримання такої характеристики інформації, як корисність. В аналітичному пошуку значення корисності доцільно оцінити конкретною величиною, яка визначається на основі таких показників: надійність джерела інформації (Н); достовірність даних (Д); інформативність даних (І). У Державній прикордонній службі України цей етап здійснюється методом 4×4. Оціночна частина розвідувального циклу повинна проводитися в обмежений час, щоб уникнути старіння інформації та її маскування великим обсягом інших первинних («сирих») відомостей.

Отже, подано методологічний апарат добування та аналізу інформації, яка є вихідною для кримінального аналізу що здійснюється на підставі методів теорії нечіткої логіки. Застосування цих підходів додатково до існуючих надає можливість: використання якісних показників; урахування неточної, приблизної інформації про значення ознак; використання знань фахівців – експертів, які подаються у вигляді нечітких правил виводу; отримання більш якісної оцінки об'єкта, що досліджується під час кримінального аналізу.

Антоненко С. І.

## ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ УПРАВЛІННЯ ЗБРОЙНИМИ СИЛАМИ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Протягом 2014-2017 років відбулися істотні зміни в безпековому середовищі Східної Європи, пов'язані передусім з активною дестабілізуючою політикою Російської Федерації щодо сусідніх держав, збройною агресією і порушенням територіальної цілісності України (тимчасовою окупацією Російською Федерацією Автономної Республіки Крим, міста Севастополя та військовою агресією в окремих районах Донецької та Луганської областей). Агресія Російської Федерації проти України показала, що попри інтенсивне використання в ній багатьох різнорідних несилових засобів (політико-дипломатичних, економічних, інформаційних тощо) головна роль належить силовим, насамперед військовим і спеціальним засобам.

Завдання щодо забезпечення протидії широкому колу згаданих військових і спеціальних засобів, притаманних російській гібридній агресії, зумовили необхідність створення в Україні системи управління силами оборони – якісно нової форми об’єднання зусиль її військових формувань, правоохоронних органів і спеціальних служб.

Проведене в рамках комплексного огляду сектору безпеки і оборони України оцінювання стану воєнної безпеки держави виявило низку проблем в управлінні силами оборони України:

відсутність об’єднаного керівництва силами оборони, яке здійснювалося б відповідно до принципів і стандартів, прийнятих державами – членами НАТО;

відсутність чіткого розподілу відповідальності за формування та застосування сил оборони, що негативно позначається на здатності керівництва держави ефективно управляти сферою оборони;

низьку ефективність системи оперативного (бойового) управління, зв’язку, розвідки та спостереження;

надмірність обсягів та неактуальність нормативно-правової бази у сфері оборони;

відсутність автоматизованої системи управління матеріально-технічним забезпеченням;

незавершеність процесу побудови ефективної системи управління ресурсами у кризових ситуаціях, що загрожують національній безпеці;

недосконала система планування та спільного застосування військ (сил) та засобів, їх підготовки та забезпечення;

недосконала і неефективна взаємодія між центральними та місцевими органами державної влади, насамперед з питань запобігання і боротьби з тероризмом;

недостатня ефективність діяльності суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, розвідувального, кримінального, терористичного та іншого характеру.

Крім того, досвід застосування Збройних Сил України в антитерористичній операції вказує на наявність низки проблем в організації управління та функціонування міжвідомчого угруповання військ (сил). Це пов’язано насамперед з тим, що система управління силами оборони держави, у тому числі Збройними Силами України, не достатньою мірою відповідає особливостям їх застосування в сучасних воєнних конфліктах, тенденціям розвитку збройної боротьби, зокрема формам та способам ведення гібридної війни і не повною мірою забезпечує максимальну реалізацію їх потенційних бойових можливостей.

З огляду на зазначені проблеми система управління Збройними Силами України має відповідати умовам новітнього конфлікту, насамперед з ознаками гібридної війни, а її реформа сприяти зміцненню спроможностей сил оборони, підвищенню їх готовності до виконання завдань за призначенням та участі у проведенні спільних бойових дій (операцій) з підрозділами НАТО.

На цей час РФ продовжує вести проти України гібридну війну, що є комбінацією різноманітних динамічних дій підконтрольних незаконних збройних формувань та регулярних сил РФ, які взаємодіють зі злочинними озброєними угрупованнями та кримінальними елементами, активно застосовують засоби пропаганди, саботажу, навмисного завдавання шкоди, вчиняють диверсії і терористичні акти, цілеспрямовані інформаційні (інформаційно-психологічні) та кібернетичні впливи (атаки).

Ця діяльність повністю вписується у погляди провідних експертів на способи ведення гібридної війни, а саме: застосування нерегулярних формувань, вчинення терористичних актів, у тому числі насильства й примусу, а також створення кримінального безладу. Ці мультимодальні дії можуть вчиняти окремі формування або одне й те ж формування, оперативно й тактично керовані і координовані в межах основного бойового простору для досягнення синергетичних ефектів.

Аналіз поглядів провідних військових науковців та реальних подій навколо України дає змогу окреслити основні її ознаки та умови гібридної війни:

існування єдиного центру, який планує, організовує і контролює ведення протиборства в усіх сферах;

поєднання конвенційних і неконвенційних воєнних дій та широкого спектру учасників війни (збройних сил, терористів, найманців, партизанів, ополченців, бандформувань, спецпідрозділів, відповідальність за дії яких не бере жодна держава, а також журналістів, дипломатів, економістів тощо);

зосередженість на боротьбі за свідомість людей, тобто інформаційній боротьбі, де основними є не військові суб’єкти, а цивільні – ЗМІ, телебачення, Інтернет, інші засоби масової комунікації;

ведення протиборства в усіх сферах життєдіяльності людини, суспільства і держави.

Характерними особливостями ведення гібридної війни є:

активне застосування сил спеціальних операцій, сил розвідки, військових частин спеціального призначення;

залучення або використання в цілях держави – агресора окремих осіб, груп, організацій та партій, їх можливостей, шляхом відкритого та/або прихованого маніпулювання їх поглядами і переконаннями;

розгортання та ведення широкої інформаційної війни для психологічної та ідеологічної підготовки свого населення, населення й особового складу збройних сил країни, проти якої готують і ведуть гібридну війну, світового суспільства з метою введення в оману стосовно істинних намірів агресора;

створення сепаратистських рухів у державі, що є об’єктом гібридної війни на політичному, етнічному, або релігійному підґрунті;

проникнення розвідки в усі сфери діяльності держави-жертви (як військової, так і державної), розгортання широкої агентурної мережі, підкуп державних службовців та окремих політичних діячів;

вплив на фінансову систему, енергосистему, об’єкти промисловості (особливо воєнно-промисловий комплекс) для їх дестабілізації та припинення розвитку;

ведення торгівельних війн шляхом припинення транзиту, встановлення підвищених мит або заборони на ввезення товарів і недопущення їх на свої ринки з держави, з якою сплановано проведення гібридної війни;

розповсюдження зброї і боєприпасів в районах із сепаратистськими настроями населення;

створення або використання сприятливої політичної ситуації, в ході якої можливо розпочати приховані бойові дії і захоплення частини території суміжної держави з найменшими втратами;

централізоване управління діями збройних сил, сил спеціальних операцій, незаконних збройних формувань, сепаратистів, терористів, бойовиків, диверсійно-розвідувальних груп;

організація проведення плебісциту або референдуму в районах, спланованих до захоплення, для обґрунтування “етнічної” агресії з псевдометою захисту інтересів окремих груп населення (іншої національності або віросповідання);

блокування або порушення комунікацій;

створення загрози застосування угруповань збройних сил та захоплення певних районів території держави;

вивезення з окупованої (підконтрольної) території матеріальних цінностей, сировини й енергоносіїв;

встановлення на окупованій території підконтрольних державі-агресору органів державного управління;

використання політичного, дипломатичного, економічного, інформаційного, конфесійного та інших видів невоєнного потенціалу країни-агресора в усіх сферах життєдіяльності людини, суспільства та країни – жертви агресії.

При цьому тенденція до конвергенції у сучасних конфліктах, яка виявляється у зближенні та взаємному проникненні (поєднанні) вищезгаданих аспектів війни, на думку військового аналітика, теоретика гібридної війни Ф. Гоффмана є принципово новою характеристикою сучасних збройних конфліктів. Конвергенція, що охоплює регулярні мілітарні і проксі-угруповання, стирає межу між державними і недержавними суб’єктами бойових дій, а також їх неоднаковими збройними потенціалами. Ця тенденція змінює форми (модальності) ведення війни, а традиційні категоріальні розрізнення між тероризмом, конвенціальними військовими діями, криміналом, іррегулярними війнами втрачають своє практичне значення.

З огляду на наведене можна зробити висновок, що оперативним середовищем гібридної війни є сукупність тісно пов’язаних сфер протиборства: військової, економічної, соціальної, інформаційної, дипломатичної, торговельної, науково-технічної тощо. Зважаючи на те, що держава – суб’єкт гібридної війни веде її з єдиного центру і дії в усіх сферах протиборства

підпорядковуються єдиній меті, то й протидія держави – об’єкта має бути так само централізованою в усіх сферах.

Таким чином, для протидії гібридній війні має бути створена система управління, спроможна керувати різнорідними (різновідомчими) силами і засобами в усіх сферах зазначених вище.

Саме з огляду на якісно нові умови гібридної війни та для підвищення ефективності управління силами оборони України в нових умовах оновлено низку стратегічних і програмних документів. Так, Указами Президента України затверджено нову редакцію Стратегії національної безпеки України, Воєнну доктрину України, Концепцію розвитку сектору безпеки і оборони України, Стратегічний оборонний бюлетень. У цих концептуальних документах містяться засадничі положення щодо реформування вітчизняного сектору безпеки і оборони, спрямовані на формування його нової якості, у тому числі оборонної складової адекватної гібридним загрозам.

Головним напрямом досягнення такої якості визначено підвищення ефективності управління силами оборони.

Відповідно до Концепції розвитку сектору безпеки і оборони України для вдосконалення державного управління сектором безпеки і оборони, своєчасного виявлення загроз національній безпеці України передбачено:

створити Об’єднаний оперативний штаб як орган управління міжвидовими та міжвідомчими угрупованнями військ (сил);

удосконалити Єдину автоматизовану систему управління Збройними Силами України для роботи в єдиній системі управління сектором безпеки і оборони;

підвищити рівень стратегічного управління у сфері забезпечення національної безпеки створенням мережі ситуаційних центрів, які взаємодіятимуть між собою та з Головним ситуаційним центром України.

У Концепції розвитку сектору безпеки і оборони України визначено Перелік кризових ситуацій та Розподіл відповідальності складових сектору безпеки і оборони за організацію планування, реагування на загрози та під час виконання завдань за призначенням.

Згідно із зазначеним Розподілом Міністерство оборони України та Збройні Сили України несуть головну відповідальність за планування, реагування та застосування сил і засобів для протидії кризовій ситуації із ознаками гібридної війни (ситуація 1.2), а саме застосуванню іншою державою проти України окремих військових підрозділів та/або частин, вогневих ударів сукупно із невоєнними засобами, а також узгодженим діям не передбачених законом воєнізованих та/або збройних формувань, приватних військових компаній для досягнення рішучих воєнно-політичних цілей, окупації України або її окремих територій, примушення воєнно-політичного керівництва України до певних воєнно-політичних рішень, встановлення прямого або опосередкованого контролю над Україною. Решта складових сектору безпеки і оборони у разі виникнення такої ситуації або беруть безпосередню участь у виконанні завдань, або виконують допоміжну роль.

При цьому питання управління складовими сектору безпеки і оборони у кризовій ситуації з ознаками гібридної війни розкрито не достатньо чітко.

Водночас концептуально наголошено на вдосконаленні державного управління сектором безпеки і оборони, одним із напрямів якого є утворення Об'єднаного оперативного штабу як органу управління міжвидовими та міжвідомчими угрупованнями військ (сил).

У Стратегічному оборонному бюлетені деталізовано ці погляди на розвиток системи управління складовими сектору безпеки і оборони, їх взаємодії та контролю за ними. У документі першою стратегічною ціллю Матриці досягнення стратегічних цілей і виконання основних завдань оборонної реформи передбачене створення Об'єднаного керівництва силами оборони відповідно до принципів і стандартів, прийнятих у державах – членах НАТО. Для цього оперативною ціллю 1.3 визначене удосконалення системи військового управління силами оборони через розмежування питань формування, підготовки військ (сил) та їх застосування: так повноваження щодо планування оборони держави та стратегічного планування застосування визначене Генеральному штабу Збройних Сил України; формування та підготовка військ (сил) Командуванням видів (окремих родів військ (сил) Збройних Сил України; застосування військ (сил) Об'єднаному оперативному штабу.

При цьому питання за рахунок чого підвищиться ефективність управління силами оборони, зокрема Збройними Силами України, за умов розмежування питань формування і підготовки військ (сил) та їх застосування, залишається відкритим.

На сьогодні у системі управління Збройними Силами України створено Об'єднаний оперативний штаб Збройних Сил України, який по суті не є органом управління для сил оборони України. Очільник Об'єднаного оперативного штабу Збройних Сил України не має повноважень з управління міжвідомчими угрупованнями військ (сил), оскільки нормативно – правова база з цього питання потребує вдосконалення.

Передбачуване введення посади Командувача об'єднаних сил, який буде підпорядковуватися Головнокомандувачу Збройних Сил України та через Об'єднаний оперативний штаб Збройних Сил України плануватиме застосування та безпосередньо керуватиме об'єднаними силами і засобами Збройних Сил України, переданими в його підпорядкування, а також іншими складовими сил оборони, на сьогоднішній день не має механізму імплементації і потребує внесення змін до Законів України "Про оборону України" та "Про Збройні Сили України".

Крім того, Концепцією розвитку сектору безпеки і оборони України передбачене узгодження концепцій, стратегій і програм реформування та розвитку складових сектору безпеки і оборони та оборонно-промислового комплексу. Водночас, протягом січня 2017 року, Кабінет Міністрів України схвалив Концепцію розвитку Національної гвардії України на період до 2020 року і Стратегію реформування системи Державної служби України з надзвичайних ситуацій, в яких питання формування сектору безпеки і оборони

як цілісного функціонального об'єднання, керованого з єдиного центру, створеного на основі уніфікованої системи планування для досягнення спільних спроможностей розкрито недостатньо, особливо в частині взаємодії із Збройними Силами України.

Системний аналіз особливостей інших заходів для досягнення стратегічних та оперативних цілей відповідно до Матриці досягнення стратегічних цілей і виконання основних завдань оборонної реформи свідчить, що наукове обґрунтування змісту, форм і способів функціонування системи управління Збройними Силами України та розроблення методики оцінювання відповідності системи управління Збройними Силами України умовам гібридної війни є надзвичайно актуальним науковим завданням. Передусім, це обумовлено необхідністю об’єктивно діагностувати ступінь відповідності системи управління Збройними Силами України умовам гібридної війни та відсутністю науково обґрунтованого інструментарію дослідження, методики оцінювання відповідності системи управління збройними силами, збалансованої системи індикаторів, критеріїв та показників оцінювання відповідності умовам гібридної війни .

Таким чином, зміна характеру сучасного збройного конфлікту та гібридна агресія РФ проти України створили поштовх для прискорення трансформацій й структурних зрушень у секторі безпеки і оборони України. Одним із пріоритетних напрямів оборонної реформи є реінжиніринг (модернізація) системи управління Збройними Силами України з метою приведення її у відповідність до умов сучасних воєнних конфліктів. Створення і повноцінне функціонування системи управління збройними силами яка б відповідала умовам сучасного воєнного конфлікту практично неможливо без наукового аналізу умов гібридної війни та об’єктивного діагностування проблем діяльності існуючої системи управління в умовах ведення антитерористичної операції. Важливість об’єктивного наукового підходу до створення системи управління збройними силами обумовлена критично високою ціною помилок в управлінні на стратегічному рівні та відсутністю часу та ресурсів для експериментів. На сьогодні створення об’єднаного керівництва силами оборони, що здійснюється відповідно до принципів і стандартів, прийнятих державами – членами НАТО, визначено стратегічною ціллю № 1 оборонної реформи і перебуває в стадії започаткування, тому логічно що відповідність системи управління Збройними Силами України умовам гібридної війни має значний потенціал для зростання. Разом з тим, на цей час не розроблено методики оцінювання такої відповідності, що не дає змоги оцінити і спрогнозувати результати рішень щодо удосконалення системи управління.

Вважається за доцільне розроблення методики оцінювання відповідності системи управління Збройними Силами України умовам гібридної війни визначити напрямом подальших наукових досліджень.

канд. техн. наук Басараб О. К.

# ЩОДО СТВОРЕННЯ «ІНТЕЛЕКТУАЛЬНОЇ» СИСТЕМИ ОХОРОНИ ДЕРЖАВНОГО КОРДОНУ

З появою нових видів загроз, зокрема збройного конфлікту в східних регіонах України, активізацією тероризму та загрози його поширення територією України виникла нагальна потреба в розвитку Державної прикордонної служби України, створення та застосування нових підходів до охорони державного кордону, запровадження сучасних технологій у системі охорони кордону.

Стратегією розвитку Державної прикордонної служби України, що схвалена розпорядженням Кабінету Міністрів України від 23.11.2015№ 1189-р (далі – Стартегія), визначено ряд завдань, одним з яких є забезпечення розвитку прикордонної інфраструктури. Розвиток прикордонної інфраструктури передбачає створення «інтелектуальної» системи охорони державного кордону.

Створення сучасної«інтелектуальної» системи охорони державного кордону, у свою чергу, передбачає розгортання:

мережі інтегрованих веж з обладнанням технічного спостереження (радіолокаційні станції, оптико-електронні камери) та засобами передачі даних (для відкритих і рівнинних ділянок);

бездротових систем спостереження, здатних здійснювати фото (відео) зйомку при виявлені руху об’єкта (людина, тварина, автомобіль) в полі зору камери і автоматичну передачу отриманого зображення на мобільний термінал або комп’ютер (для напіввідкритих гірсько-лісистих ділянок);

сигналізаційних комплексів охорони протяжних ділянок українського виробництва на лінійній частині існуючого загороджувального паркану (колишніх сигналізаційних систем або комплексів) – на окремих напрямках;

систем відеоконтролю і сигналізації шляхом встановлення мультиспектральних камер та датчиків на існуючі металеві спостережні вежі;

пересувних комплексів технічного спостереження (на базі позашляховика) з можливістю одночасного здійснення радіолокаційного та оптико-електронного спостереження;

командних центрів на центрах управління службою відділів та прикордонних загонівдля отримання інформації про тривоги від всіх розгорнутих технічних засобів охорони державного кордону і своєчасного реагування на обстановку;

засобів передачі даних (засобів зв’язку) від технічних засобів до командних центрів.

На виконання Стратегії на озброєння Державної прикордонної служби України вже прийнято ряд сучасних технічних засобів:

пересувні бойові модулі «Тритон»;

система раннього попередження, виявлення та розпізнавання корпорації «Аерос» (США);

бездротові системи спостереження «SMARTDEC-869»;

системи відеоконтролю і сигналізації (мультиспектральні камери та датчики, встановлені на існуючих металевих спостережних вежах, паркані та окремих вежах), сейсмічні системи (оптико-волоконний кабель), засоби передачі даних та командні центри (розгорнуті на цусвпс для отримання інформації про тривоги від ТЗОК), які в комплексі передбачають створення інтелектуальної системи контролю;

безпілотні авіаційні комплекси БпАК-МП-1 «Spectator-M».

Таким чином, прийняття новітніх технічних засобів сприяє створенню сучасної«інтелектуальної» системи охорони кордону та нової системи захисту державного кордону в цілому, запровадженню європейських стандартів інтегрованого управління кордонами тощо.

д-р техн. наук Биченок М.М.
канд. військ. наук Войтко О.В.
Чернега В.М.

## ПРО ЕКСПЕРТНЕ ОЦІНЮВАННЯ РИЗИКІВ НЕГАТИВНИХ ІНФОРМАЦІЙНИХ ВПЛИВІВ

Застосування технологій гібридної війни в сучасних війнах та збройних конфліктах перетворило інформаційну сферу на ключову арену протиборства. Використання найновіших інформаційних технологій впливу на свідомість громадян спрямовано на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності держави.

Упереджуючи реагування на небезпеку негативних інформаційних впливів потребує науково-методичного інструментарію для оцінки загроз цих впливів (ризиків інформаційної безпеки) та обґрунтування заходів із запобігання чи мінімізації небажаних наслідків. Застосування такого інструментарію пов’язано, перш за все, з розробкою адекватних математичних моделей ризиків інформаційних впливів.

Наукове дослідження будь-яких об’єктів чи процесів, у тому числі й інформаційних, починається з вимірювання їхніх параметрів за допомогою формалізованого опису. Аналіз науково-методичного апарату оцінювання ризиків інформаційної безпеки свідчить, що їх основу складають певні методологічні засади, нормативно-правові акти або міжнародні стандарти, які визначають вимоги інформаційної безпеки.

Отже, потреба науково-обґрунтованого підходу до безпеки життєдіяльності в інформаційному середовищі зумовлює необхідність формалізації та оцінювання небезпеки негативних інформаційних впливів, тобто ризиків інформаційної безпеки.

Метою дослідження є формалізація та оцінювання ризиків негативних інформаційних впливів методом експертних оцінок.

Головну трудність для математичного моделювання ризиків інформаційній безпеці становить невизначеність просторово-часових

характеристик процесів зародження і прояву джерел негативних інформаційних впливів. У теорії прийняття рішень розрізняються два типи невизначеності: статистичний і нестатистичний. До першого типу відносяться процеси, що можуть спостерігатися достатню кількість разів, зокрема, за допомогою натурних або модельних експериментів. Частота виникнення подій (інформаційних впливів), що характеризують ці процеси, трактується як статистична ймовірність. Якщо досліджувані процеси проявляються недостатню кількість разів, або взагалі припускають реалізацію лише в майбутньому, то вони являють нестатистичний тип невизначеності. У цьому випадку ймовірність трактується не як частота виникнення події, а як ступінь впевненості (міра можливості), що ця подія відбудеться. Нестатистична інтерпретація невизначеності оперує поняттям суб'єктивної ймовірності. Оцінювання суб'єктивних ймовірностей здійснюється за допомогою спеціально організованих експертних процедур на основі декомпозиції складної події на більш прості.

Узагальнена експертна процедура оцінювання ризиків інформаційних впливів включає п'ять основних етапів:

1) *Ідентифікація джерел негативних інформаційних впливів* – виконується збір і аналіз усіх доступних відомостей про випадки прояву і негативні наслідки інформаційних впливів у межах оцінюваної території для отримання відповіді на наступні питання:

- які за ґенезою є джерела негативних інформаційних впливів на даній території?
- де, коли і за яких умов вони проявлялися чи можуть проявитися на даній території?

2) *Визначення стану джерел негативних інформаційних впливів* – проводиться аналіз просторово-часових характеристик виявлених джерел для відповіді на такі питання:

- яка була у минулому чи очікується частота виникнення і тривалість негативних інформаційних впливів від цих джерел на даній території при відсутності запобіжних заходів?
- якими будуть зазначені характеристики при різних варіантах запобіжних заходів?

3) *Оцінка уразливості об'єктів впливу* – за результатами аналізу станів джерел негативних інформаційних впливів визначаються відповіді на питання:

- яка чисельність, склад і уразливість об'єктів впливу у межах даної території від можливих інформаційних загроз певного типу?
- яка чисельність, склад і уразливість об'єктів впливу у межах даної території від можливих інформаційних загроз усіх типів?

4) *Визначення ризиків інформаційній безпеці* – на основі проведеного аналізу стану джерел інформаційних загроз і потенційних об'єктів їх впливу формуються відповіді на питання:

- які можливі сценарії зміни стану різних джерел і відповідні негативні наслідки їх прояву?

- якою може бути уразливість об’єктів впливу від усіх і від окремих типів інформаційних загроз?

- якими будуть відповідні частоти прояву різних джерел інформаційних загроз?

5) *Обґрунтування заходів щодо мінімізації ризиків негативних інформаційних впливів* – з урахуванням економічних і соціальних вимог та можливостей заданого регіону розробляються відповіді на заключні питання:

- який припустимий ризик, тобто припустима частота прояву різних джерел?

- якими стануть сценарії зміни стану джерел інформаційних загроз і відповідні негативні наслідки їх прояву після здійснення варіантів запобіжних заходів?

- який варіант цих заходів забезпечує досягнення припустимого ризику при мінімальних витратах на їхню реалізацію?

Для формалізованого представлення ризику інформаційного впливу R можна використати модель, що пов’язує між собою ймовірність виникнення певних подій (прояву інформаційних джерел) P і відповідних їм наслідків W:

$$R = P \cdot W \qquad (1)$$

Враховуючи, що $0 \le P \le 1$ та нормовані втрати $0 \le W \le 1$, ці показники можна використовувати для кількісного оцінювання ризику інформаційного впливу в характерних ситуаціях:

при $P = 1$, $W = 0$, $R = 0$ частота прояву інформаційної загрози велика, а величина втрат незначна;

при $P = 0$, $W = 1$, $R = 0$ прояв інформаційної загрози відбувається вкрай рідко, а величина втрат велика;

при $P = 0$, $W = 0$, $R = 0$ незначна частота прояву інформаційної загрози і її наслідків;

при $P \neq 0$, $W \neq 0$, $R \neq 0$ відбуваються різні частоти прояву інформаційних загроз і різні наслідки. Ця ситуація може оцінюватися як небезпечна і характеризуватися значною величиною ризику інформаційного впливу.

Для обчислення ймовірностей і, відповідно, оцінювання ризиків існують три основні методологічні підходи :

статистичний – за результатами багаторазових спостережень відповідно закону великих чисел розраховують частоту прояву різних джерел негативних інформаційних впливів;

соціологічний – за допомогою цього методу визначається сприйняття населенням і його окремими групами тих чи інших інформаційних впливів. Проводяться соціологічні опитування, під час яких визначаються оцінки інформаційних ризиків, пов’язані з прийняттям тих чи інших рішень щодо запобіжних заходів;

експертний – при використанні першого підходу часто зустрічаються випадки, коли недостатньо статистичних даних щодо прояву різних джерел негативних інформаційних впливів. Тоді залучаються експерти для суб’єктивної оцінки ймовірності прояву того чи іншого джерела.

Таким чином, на основі аналізу джерел негативних інформаційних впливів в статті розроблено узагальнену експертну процедуру оцінювання ризиків негативних інформаційних впливів. Оцінка ризиків експертними методами має перевагу в умовах відсутності об'єктивних даних про величини ймовірностей виникнення певних негативних інформаційних впливів і відповідних їм наслідкам.

д-р техн. наук Богданович В.Ю.
д-р військ. наук Свида І.Ю.
Прима А.М.

## ІНФОРМАЦІЙНА ПІДТРИМКА КОМПЛЕКСНОГО ВИКОРИСТАННЯ ВІЙСЬКОВИХ І НЕВІЙСЬКОВИХ ІНСТРУМЕНТІВ ПРОТИДІЇ ЗАГРОЗАМ ВОЄННІЙ БЕЗПЕЦІ ДЕРЖАВИ

Захист своїх геополітичних інтересів за допомогою воєн до недавнього часу вівся традиційними збройними засобами з використанням регулярних армій. Специфіка воєн XXI–го століття полягає в тому, що роль традиційних збройних засобів вже не є провідною, а суттєво збільшується роль таких інструментів, як політичні, дипломатичні, економічні, інформаційні, ідеологічні, психологічні, гуманітарні, розвідувальні, котрі часто виявляються ефективнішими і більш руйнівними

Прямі військові зіткнення між державами відбуваються все рідше, поступаючись внутрідержавним конфліктам, громадянським війнам, які, перш за все, обумовлені внутрішніми причинами, але провокуються і підтримуються ззовні. В воєнних діях воєн такого типу все більшу роль відіграють недержавні учасники або актори, які виступають в ролі ключового інструменту і провідника зовнішньої політики держави, що реалізує свої геополітичні інтереси.

Для сучасних воєн, які отримали назву "гібридних", характерним є не використовувані засоби, а цілі, що досягаються, зіставні з цілями, які зазвичай переслідуються в ході традиційних воєн, наприклад, знищення, розграбування, окупація, зміна режиму, занурення в хаос.

Одну з найважливіших відмінностей гібридної війни становить те, що вона відбувається не стільки за володіння територіями і природними ресурсами, скільки з прагненням контролювати настрій громадян країни-опонента завдяки контролю за інформаційним простором і промиванню мізків на захоплених територіях.

Завдяки вживаним технологіям на сучасному етапі зазначені вище цілі можуть бути досягнуті без застосування летальної зброї. Ще одним інструментом для реалізації своїх геополітичних інтересів є примушення країни до збройного конфлікту з вибраним для знищення (ослаблення) супротивником. У цьому разі починає відігравати істотну роль дипломатичний чинник. Останні гібридні конфлікти засвідчили ще один спосіб досягнення геополітичних інтересів, а саме формування та використання страху влади застосовувати збройні сили для реалізації своїх національних інтересів (захисту державного суверенітету,

відновлення територіальної цілісності, відбиття агресії й покарання агресора), що паралізує зовнішню політику, робить її недієздатною й залежною від тих, хто подібного страху не має.

Середовище безпеки в XXI ст., сформоване в умовах глобалізації, виявляється якісно складнішим і вимагає готовності до протидії більш складним загрозам як окремій людині, так і суспільству. До таких загроз відносяться «гібридні» загрози, які поєднують у собі військові і цивільні складові. Їх особливістю є суворо цілеспрямований, адаптивний щодо держави-мішені і конкретної політичної ситуації. Комплекс «гібридних» загроз володіє рядом характеристик, що забезпечують його ефективне застосування на всіх етапах так званої «гібридної» війни. Такий комплекс завдяки унікальній синергетиці несе в собі набагато більшу руйнівну силу, ніж проста сума вхідних в нього загроз. Ця особливість зумовлює їх могутній руйнівний потенціал. Синергетичний ефект від дії загроз цього виду забезпечується реалізацією системи комплексних і взаємозалежних підготовчих і подальших заходів, пов'язаних з координацією діяльності значної кількості учасників, що діють на території країни-мішені та поза її межами. Успіху сприяє ефективне використання чинників, що обумовлюють високу динаміку розвитку обстановки і додання процесам контрольованої спрямованості з використанням як невійськових, так і військових інструментів (рішень).

Цілеспрямований характер і висока динаміка переходу «гібридних» загроз з категорії потенційних до реально діючих вимагають ретельного попереднього опрацьовування на державному рівні заходів з протидії.

Законами України, Воєнною доктриною України та Концепцією розвитку сектору безпеки і оборони (СБОУ) України визначені завдання складових СБОУ у сферах оборони і забезпечення безпеки держави .

У цілому сили безпеки і оборони повинні бути здатними до ведення операцій (бойових дій) різного масштабу із рішучими цілями в умовах інформаційного протиборства, боротьби за панування в повітрі та на морі, застосування противником високоточної зброї та асиметричних дій, ефективно протистояти розвідувально-диверсійним діям противника.

Основні зусилля з розвитку сектору безпеки і оборони передбачається зосередити на поетапному та узгодженому нарощуванні оперативних спроможностей сил безпеки і оборони та рівня їх готовності до невідкладного реагування на виклики й загрози національній безпеці України, зокрема на:

удосконаленні концептуальних та доктринальних засад підготовки та застосування військ (сил) і засобів сектору безпеки і оборони;

централізації управління сектором безпеки і оборони у мирний час, у кризових ситуаціях, що загрожують національній безпеці, та в особливий період, підвищенні рівня міжвідомчої координації і взаємодії;

узгодженні концепцій, стратегій і програм реформування та розвитку складових сектору безпеки і оборони та оборонно-промислового комплексу;

удосконаленні системи державного прогнозування та стратегічного планування, системи планування застосування військ (сил) і засобів сектору безпеки і оборони.

Результати проведених досліджень показують, що досягнення поставлених цілей у сфері забезпечення воєнної безпеки держави практично неможливе без розроблення й послідовного проведення єдиної гнучкої державної політики, інтеграції сил та засобів сектору безпеки і оборони, створення та впровадження в життя єдиної системи взаємоузгоджених і всебічно зважених заходів економічного, політичного, інформаційного й організаційного характеру, адекватних загрозам життєво важливим інтересам суспільства і держави.

Запропонований метод управління інтегрованим потенціалом протидії загрозам воєнного характеру являє собою послідовне виконання визначених процедур, спрямованих на отримання необхідної інформації щодо загроз воєнного характеру та їх характеристик та визначення можливостей (потрібного потенціалу) суб'єктів СБОУ для комплексного застосування у процесі управління протидією цим загрозам, що у підсумку дозволяє обґрунтовувати раціональний склад сил і засобів та їх необхідні спроможності для деескалації виявлених (прогнозованих) загроз у межах виділених, як державою, так і недержавними організаціями, ресурсів. Успішна реалізація даного методу потребує відповідної інформаційної підтримки в ході спеціальних дій по нейтралізації виявлених (прогнозованих) загроз. На жаль, методичний апарат організації такої підтримки на даний час не розроблено. Виходячи із аналізу інформаційних дій у останніх збройних конфліктах, можна сформулювати основні завдання інформаційної підтримки:

забезпечення залучаємих для протидії загрозам суб'єктів необхідною інформацією;

реалізація заходів щодо введення супротивника в оману;

забезпечення оперативної скритності;

проведення психологічних операцій, зокрема з використанням телебачення, радіо, друкованих ЗМІ для підриву морального духу військ та населення супротивної держави;

формування негативного представлення про воєнно-політичне керівництво супротивної держави як про джерело кризи та ймовірного агресора для всього регіону, деструкцію морально-етичних цінностей та нагнітання несприятливого психологічного клімату у відношеннях з іншими державами;

прицільна інформаційна обробка ключових фігур у керівництві супротивної держави на основі врахування їх психологічних особливостей, політичної і іншої орієнтації, пропаганда і впровадження форм суспільної поведінки, що знижує моральний потенціал нації;

активізація діяльності «агентів» впливу, що знаходяться на території супротивної держави;

розрив інформаційних потоків;

встановлення контролю за інформаційним та експертним простором супротивної держави і т. ін.

**Таким чином,** належна інформаційна підтримка військових і невійськових заходів щодо протидії загрозам воєнній безпеці держави дозволить отримати необхідну інформацію щодо загроз воєнного характеру, їх характеристик та визначення можливостей (потрібного потенціалу) суб'єктів

СБОУ для комплексного застосування у процесі управління протидією цим загрозам, що у підсумку дозволяє обґрунтовувати раціональний склад сил і засобів та їх необхідні спроможності для деескалації виявлених (прогнозованих) загроз у межах виділених, як державою, так і недержавними організаціями, ресурсів.

д-р техн. наук Бутвін Б.Л.

## МЕТОДИКА ОЦІНКИ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ НА ОСНОВІ БАГАТОПАРАМЕТРИЧНОГО, НЕЛІНІЙНОГО МЕТА ПІДХОДУ

Доповідь націлена на результатах розробки методики оцінки загроз національній безпеці України на основі складних розрахункових алгоритмах методу групового урахування аргументів.

На сьогодні наша держава вже четвертий рік веде неоголошену інформаційну війну. Одним із завдань ухвалення раціональних рішень на дії у відповідь є адекватна оцінка інформаційних загроз.

Існуючі методичні підходи в основному засновані на спрощених підходах до оцінки цих загроз що вносить істотні помилки до оцінки їх пріоритетного ряду. В основному ці підходи засновані на адитивних (чи мультиплікативних) формах розрахунку інтегрального рівня цих загроз без необхідного теоретичного обґрунтування. Це призводить до значних помилок і як наслідок до неправильних рішень на проведення оптимальних заходів у відповідь, спрямованих на нейтралізацію цих загроз.

Пропонується новий методичний підхід, який заснований на сучасному методі групового обліку аргументів. Він дозволяє побудувати складний метафункционал, який заснований на групових експертно-аналітичних оцінках. Розрахунки показали, що запропонований методичний підхід забезпечує досить високий рівень адекватності експериментальних (експертно-аналітичних) даних і розрахункових даних розрахованих за допомогою метафункционалу.

Васільєва О.О.

## ДОПОВІДЬ НАЦІЛЕНА НА ВИЯВЛЕННЯ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ ІНФОРМАЦІЙНО-ПРОПАГАНДИСТСЬКИХ КАМПАНІЙ РФ З ВИКОРИСТАННЯМ СОЦІАЛЬНИХ МЕРЕЖ

На сьогодні наша держава вже четвертий рік поспіль знаходиться в стані так званої «гібридної війни» з Росією. Інформаційно-пропагандистська війна як складова гібридної війни. Завдання України - давати ефективну і змістовну відповідь на інформаційну агресію проти нашої держави. Підписання указу №47/2017 Про рішення Ради національної безпеки і оборони України від 29

грудня 2016 року «Про Доктрину інформаційної безпеки України». Аналіз положень «Доктрини», основні концептуальні напрямки роботи для реалізації.

Протидія руйнівному інформаційному-психологічному впливу Російської Федерації в умовах розв'язаної нею гібридної війни: виявлення та захист від інформаційно-психологічних впливів – дезінформації, деструктивної пропаганди, виявлення та протидія спеціальним інформаційним операціям.

Основні платформи ведення інформаційно-психологічних операцій. Соціальні медіа (соціальні мережі, блоги, форуми) як основні платформи планування та проведення інформаційних операцій, розповсюдження дезінформації, "чуток", димотиваторів, підбурювання населення до протиправних дій (погроми, заворушення тощо), вербування в лави незаконних збройних формувань (НЗФ) на окупованих територіях України.

Основні методи роботи ворожої сторони. Створення соціальних тематичних груп для поширення контенту. Створення соціальних груп для збору інформації. Створення груп для збору коштів з метою фінансування НЗФ. Створення груп для вербування найманців.

Заходи протидії, які слід проводити для запобігання переваги агресора в інформаційній сфері. Популяризація проукраїнських тем. Виявлення та блокування "ворожого" контенту.

канд. істор. наук Гапеєва О.Л.

## АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДОСВІД ОДКБ

У загальноприйнятому сенсі термін "інформаційна безпека" означає захищеність особистості, суспільства та держави від деструктивних та інших негативних впливів в інформаційному просторі. Отже, проблематика забезпечення інформаційної безпеки, без перебільшення, є актуальним питанням сьогодення та предметом наукових досліджень політологів, соціологів, правознавців та фахівців у галузі інформаційних технологій.

Починаючи з грудня 1991 р. на пострадянському просторі відбувається процес утворення міжнародних регіональних об'єднань: Співдружності Незалежних Держав, Організації Договору про колективну безпеку (далі – ОДКБ), Союзної держави Росії і Білорусії. Аналіз діяльності останніх свідчить, що однимі з пріоритетних напрямів у інформаційній сфері, окрім налагодження інформаційного обміну, стало забезпечення інформаційної безпеки. З цією метою було розроблено й узгоджено низку керівних документів, пов'язаних із формуванням єдиного інформаційного простору Співдружності Незалежних Держав, захистом інформації з обмеженим доступом, співробітництвом у сфері захисту інформаційних ресурсів і наданням взаємної допомоги у запобіганні негативним інформаційним впливам. Зауважимо, що Російська Федерація (далі – РФ), як держава-учасниця кожної з вищеперерахованих організацій, фактично є координатором дій у цій сфері.

У наших попередніх наукових студіях досліджувались питання забезпечення інформаційної безпеки на пострадянському просторі в історичній ретроспективі. На нашу думку, найбільш цікавим для України є досвід ОДКБ у сфері забезпечення інформаційної безпеки, зокрема, проведення спільних операцій у кіберпросторі, а також діяльність Аналітичної Асоціації, утвореної у 2013 р. Слід зауважити, що в Україні відсутні комплексні наукові дослідження щодо діяльності ОДКБ у цьому напрямку. Саме тому основу дослідження складають офіційні документи, які розміщені на інтернет-порталі організації (http://www.odkb-csto.org), матеріали виступів та інтерв'ю керівного складу, аналітичні матеріали державних інформаційних агенцій, матеріали наукових й науково-практичних конференцій та семінарів за тематикою, що вивчається.

Отже, створення власної системи інформаційної безпеки (далі – ІБ) в ОДКБ розпочалось у листопаді 2006 р. Відповідно, було розроблено Програму спільних дій, затверджену Рішенням Ради колективної безпеки. З метою координації співпраці держав-учасниць у сфері ІБ була утворена Робоча група при Комітеті секретарів Ради безпеки з питань інформаційної політики та інформаційної безпеки.

З метою формування інформаційного простору ОДКБ і протидії кримінальним злочинам засобами інформаційних технологій, було розроблено концептуальні й організаційні засади системи ІБ; спланована систему заходів щодо забезпечення ІБ об'єктів міждержавного призначення, організації взаємодії міністерств і відомств держав-учасниць ОДКБ, а також низку заходів кадрового, наукового і фінансового змісту. Так, з метою підготовки, перепідготовки та підвищення кваліфікації фахівців з інформаційної безпеки держав-учасниць ОДКБ було створено базову навчально-методичну структуру, на яку покладено завдання з організаційно-методичного забезпечення підготовки військових фахівців, наукових і педагогічних кадрів. У якості базової організації затверджено Краснодарське вище військове училище (країна дислокації – РФ).

Нагальною проблемою стала й розробка єдиного понятійного апарату з питань ІБ. Так, у Положенні про співробітництво держав-учасниць ОДКБ у сфері забезпечення інформаційної безпеки, затвердженому у грудні 2010 р., вперше було закріплено терміни "інформаційна безпека" та "система інформаційної безпеки". Зокрема, остання – це комплекс заходів правничого, політичного, організаційного, кадрового, фінансового, науково-технічного і спеціального характеру, метою якого є забезпечення ІБ держав-учасниць ОДКБ. У травні 2011 р. було прийнято Програму діяльності Парламентської Асамблеї ОДКБ щодо зближення і гармонізації національного законодавства держав-учасниць на період 2011-2015 рр.

Першим спільним заходом держав-учасниць ОДКБ в інформаційній сфері стало проведення у 2009 р. спеціальної операції "ПРОКСІ". Наступного року було проведено операцію "ПРОКСІ-ПІВДЕНЬ" з метою надання підтримки Киргизькій Республіці у стабілізації соціально-політичної обстановки та недопущення протиправних дій в інформаційному просторі. Як свідчать офіційні джерела, під час операції у національних сегментах держав-учасниць

ОДКБ було виявлено близько 2 тисяч інформаційних ресурсів, що використовувались з метою поширення деструктивної інформації. У грудні 2014 р. “ПРОКСІ” отримала статус операції постійної дії.

Слід зауважити, що підвищена увага до питань інформаційної безпеки у РФ спостерігається після поразки останньої в інформаційній війні під час російсько-грузинського воєнного конфлікту (2008 р.) У монографії “СМИ, пропаганда и информационные войны” російського вченого, доктора політичних наук Ігоря Миколайовича Панаріна (відомого своєю теорією розпаду США на шість окремих держав) головною проблемою “антиросійської” інформаційної кампанії 2008 р. вказано “…несвоєчасні організаційно-управлінські рішення в інформаційній сфері та нездатність еліти ОДКБ вести ефективне інформаційне протиборство в умовах посилення конкуренції у сучасному світі”. За автором, на порядок денний вийшло питання одночасного створення потужних інформаційно-аналітичних та інформаційно-пропагандистських структур ОДКБ .

І.М. Панарін запропонував утворити Комітет інформаційної безпеки ОДКБ, який мав виконувати функції “… розробки нової системи підготовки інформаційної еліти країн ОДКБ, інтеграції зусиль державних інформаційно-розвідувальних структур країн ОДКБ з організації спільних інформаційних операцій (оборонних і наступальних) щодо захисту інформаційно-ідеологічного простору країн ОДКБ”. Він також вказував на необхідність прийняття Доктрини інформаційної безпеки ОДКБ та створення Системи спеціальних структур інформаційного протиборства та залучити до її складу представників органів державної влади й управління, бізнесу, наукових інституцій, ЗМІ. Розглянемо впровадження пропозицій російського вченого у практичну площину.

У березні 2013 р. на засіданні першого семінару-наради з керівниками інформаційно-аналітичних структур держав-учасниць ОДКБ було прийнято рішення про створення Аналітичної Асоціації ОДКБ, яка об’єднала 25 інформаційно-аналітичних і соціологічних структур держав-учасниць Організації. Призначенням Асоціації є розробка скоординованої інформаційної політики, обміну інформацією та здійснення експертного й ситуаційного аналізу. Звісно, її Координатором став І.М. Панарин.

У квітні 2014 р. у м. Єкатеринбурзі за участю Генерального секретаря ОДКБ було підписано Меморандум про створення Університетської ліги ОДКБ, до якої увійшло 30 вишів з усіх держав-учасниць. Влітку 2014 р. на базі Московського державного університету приладобудування і інформатики пройшов триденний навчальний спільний семінар Секретаріату ОДКБ та Університетської ліги на тему: “Інформаційна війна: історія і сучасність”, у якому окрім повноважних представників вищевказаних структур взяли участь співробітники Міністерства закордонних справ РФ, Міністерства оборони та інших силових відомств РФ. У листопаді-грудні цього ж року було проведено цикл навчальних курсів з ІБ в університетах п’яти країн ОДКБ (Вірменія, Казахстан, Білорусь, Таджикистан, Киргизстан). Як свідчить інформація, розміщена у ЗМІ, студенти вивчали методи пропаганди, основи теорії

інформаційної війни; проблематику “кольорових революцій” як форми ведення інформаційної війни; інформаційну війну в соціальних мережах, комп’ютерні психотехнології тощо. Наприкінці 2014 р. підписано документ щодо створення Центру протидії кіберзагрозам у рамках ОДКБ.

Одним з перспективних напрямів діяльності ОДКБ у сфері забезпечення інформаційної безпеки стала активна діяльність у молодіжному середовищі, зокрема, шляхом навчання студентів (журналістів, фахівців з міжнародних відносин та економічних спеціальностей) основам підготовки, ведення та протидії інформаційно-психологічним операціям. Окремо слід вказати про підготовку фахівців із захисту інформації на технічних факультетах цивільних вишів.

канд. психол. наук Горбенко Ю.Л.,
Горбенко А.Ю.
Горбенко О.В.

## КОНСЦІЄНТАЛЬНА ЗБРОЯ: МЕХАНІЗМИ ТА ЗАСОБИ ПРОТИДІЇ

Своєю появою поняття “гібридна війна” завдячує своєму широкому використанню під час Російської агресії проти України. Сутність цього поняття широко представлена у сучасному Українському науковому середовищі та широко використовується у сучасній науковій літературі, зокрема такими авторами як: А. Баровська, М. Варій, К. Кононенко, Г. Почепцов, Л. Смола та інші. У своїй роботі “Гібридна війна: Сутність та структура феномену” Є. Магди зазначає що “гібридну війну можна у найзагальніших рисах визначити як сукупність заздалегідь підготовлених і оперативно реалізованих дій військового, дипломатичного, економічного, інформаційного характеру, спрямованих на досягнення стратегічних цілей. До складових гібридної війни відносяться традиційні та нестандартні загрози, тероризм, підривні дії, коли використовуються новітні чи нешаблонні технології для протидії перевазі супротивника у військовій силі”.

В умовах інформаційного суспільства, вирішення задач війни напряму залежить від можливостей швидкої обробки інформації та використання її у військових цілях. Крім того, широкі можливості засобів масової комунікації, по миттєвій доставці будь-якої інформації у будь-яку частину світу, роблять саму інформацію зброєю.

Спеціально вироблена інформація у відповідності до концепції агресії спрямованої на руйнування духовних засад народу, його ідеології, історії, культури, національної самосвідомості, з метою підкорення волі загарбника.

Такий вид інформаційно-психологічної складової гібридної війни аналітики назвали консцієнтальною війною (від латинського слова conscientia – свідомість або совість).

У буквальному сенсі цього слова – це війна, спрямована на руйнування свідомості та совісті народу, що піддається агресії.

В індустріальному суспільстві вплив слова і мови на можливості керування людиною був нівельований, але і тоді принциповим було положення про те, що перемога чи поразка – це, в першу чергу, перевага ідеї та мотивації над противником, а не чисельний стан військ чи економіки. Б. Поршнєв у своїх фундаментальних працях розкрив закономірності розвитку лінгвістичної компоненти (мови) у історичному процесі та показав механізми підкорення людської свідомості. До основних засобів підкорення (контрконтрсугестії за Б. Поршнєвим) належать: віра або довіра; навіювання; повторення; переконання. При цьому він прогнозував, що у майбутньому основним засобом підкорення буде переконання.

Як формується переконання, як засіб підкорення, у сучасному інформаційному суспільстві? Першим етапом є розмивання поняття совість, другим – формування міфологічного "образу світу".

Якщо особистість приймає, нав'язаний противником, потрібний "образ світу" за основу – вона вже не здатна вийти за рамки простору цього образу і формує свою "картину світу", яка і визначає межі мислення і діяльності індивіду.

Механізмами формування такого "нав'язаного світу" можуть виступати системні впливи на такі компоненти як:

- руйнування релігійних уявлень і переконань;
- руйнування лінгвістичної компоненти свідомості (мови);
- створення соціальних міфів;
- нав'язування стереотипів поведінки;
- формування соціальних установок;
- руйнування історичних архетипів;
- руйнування політичних, культурних традицій.

Руйнування совісті є найважливішою метою засобів масової комунікації, які, по суті, стають замінником "внутрішніх наказів суспільства", що передаються як "заохочення чи покарання батьків" у дитинстві. У подальшому ті ж самі засоби масової комунікації сіють недовіру до керівництва та засобів комунікації опонентів, потім багаторазово повторюють необхідну їм інформацію, навіюють "яскраві образи" та у кінцевому результаті формують потрібний "образ світу".

Якщо двадцять відсотків суспільства сприймає цю інформацію з потрібними (ЗМІ) ідеями адекватно, то ідеї, що поширюються, починають існувати у суспільстві самостійно; якщо ж більше ніж п'ятдесят відсотків суспільства, цю інформацію схвалює – суспільна свідомість починає народжувати лідерів, які втілюють ці ідеї у життя.

Війна на знищення свідомості та совісті, ведеться не гребуючи ніякими засобами, всупереч будь-яким загальнолюдським цінностям. Тому виправданими є будь-яка дія: брехня, міфи, перекручення інформації, підкуп, обстріли цивільного населення та знищення своїх же союзників, недотримання будь-яких домовленостей і тому подібне.

Підсумовуючи наслідки застосування консцієнтальної зброї, В. Карякин відмічає, що "відбувається: зниження загального рівня свідомості людей, що

живуть на певній території; руйнування у них стійкої системи світоглядних цінностей і заміщення їх різними ціннісними симулянтами; як наслідок – знищення родової і культурної пам'яті людей, психотизація і невротизація суспільства, що виникає через це і призводить до появи маніакально-буйних і водночас повністю керованих "шизоїдів"; руйнування традиційних механізмів самоідентифікації і заміщення їх механізмами ідентифікації нового типу через створення різного роду "груп участі"; впровадження в суспільство спеціально сконструйованої матриці цінностей, норм поведінки і реакцій як єдино можливої моделі життєдіяльності населення; знищення здатності ставити глобальні і стратегічні цілі — руйнування суб'єктності цілих етносів і народів; здійснення цивілізаційної перевербовки етносів і народів.

О. Сенченко, з приводу механізмів дії консцієнтальної зброї, зауважує, що вона "вражає усіх, хто не має системи сталих цінностей, властивих певній цивілізації, моральності й моральних принципів, але головними її жертвами стає саме молодь, без життєвого досвіду.

Основу цієї зброї становлять інформаційні бомби, що надходять до супротивника через ЗМІ, телебачення і особливо Інтернет, який набув широкого поширення серед підлітків. І головною небезпекою є нові інформаційні технології, оскільки контролювати поширення інформації в мережі, особливо в соціальних мережах, до яких залучена майже вся молодь, практично неможливо".

Сучасний демократичний світ не готовий до таких викликів і тому не здатний адекватно реагувати на інформаційні атаки, підготовлені у масштабах всього світу. Постає питання: які існують засоби протидії таким атакам?

Чи необхідно спростовувати всю брехню, всі міфи та всі ідеологічні концепції сторони що їх використовує?

Але, по суті, боротися з вірусом шляхом його модифікації – це створювати та поширювати нові віруси.

Якщо керівництво української або будь-якої європейської держави поставить за мету спростовувати все, усю брехню Росії, то вони не зможуть генерувати будь-які свої ідеї, більше того, саме спростовування міфів, ще швидше їх розповсюджує та легітимізує, використовуючи інструменти демократичного суспільства, для поширення брехні.

Д. Золотухін з цього приводу зазначає, що неможливо виграти цю війну "симетричними методами", тобто якщо "Росія вклала $1 млрд. у британський Russia Today, то давайте ми теж створимо кілька телеканалів".

Це буде схоже на гонку озброєнь, яка виснажила колишній Радянський союз, але у даному випадку у якості озброєння буде використовуватись мас-медіа.

У перші роки війни громадські організації "Інформаційний Спротив", Stop Fake, InformNapalm та інші змогли заповнити вакуум, що утворився в інформаційному просторі України. Але, вивчаючи їх діяльність, необхідно зазначити, що самі назви даних організацій вказують про напрямки їх роботи. "Інформаційний спротив", " Stop Fake " показує їх спрямованість на контргру, а

не на ведення власної. В таких умовах нам не здолати формування “структурованого світу”, який нав’язується ззовні.

Перехід до вироблення власної стратегії побудови громадянського суспільства, фундаментом якої повинна стати правда, якою б вона не була є єдиним можливим шляхом протидії інформаційній агресії. Будь то правда про історію нації, про походження мов, про події на фронті, про героїв фронту і волонтерів, про стан суспільства і економіки, про сучасні виклики і можливості їх подолання. Але правда завжди “дорого коштує”, про що дізналися організатори “Інформаційного Спротиву”, Stop Fake, InformNapalm, проте альтернативного засобу боротьби з брехнею крім правди немає.

В даних умовах, державні структури повинні законодавчо закріпити можливість громадським організаціям використовувати суспільну думку та забезпечити квоти на інформаційні програми, спрямовані на формування позитивного іміджу держави та збройних сил, поширення правдивих історичних фактів, повагу до національних символів і традицій та мобілізацію на протистояння зовнішній агресії.

Сьогоднішні власники українських мас-медіа створюють декілька інформаційних просторів: на одних йде війна, на інших – розважальні шоу та інше. Таке положення створює умови, за яких Ідея не спроможна досягти критичних п’ятдесяти відсотків суспільства, а як результат втрачається можливість сформувати нових лідерів цієї нової Ідеї.

Чи може це робиться свідомо, щоб не помінялись еліти?

Тоді у стані війни їх необхідно притягати до відповідальності.

Отже, інтерпретація подій та новин, забезпечується здебільшого тими, хто контролює ці засоби. В українських реаліях це не більше десяти олігархічних кланів. Чи відповідають цінності та інтереси цих кланів інтересам українського громадянського суспільства? Чи може більшість населення, яке знаходиться за межею бідності, мати вплив на мас-медіа? Відповідь очевидна – ні!

Сама війна, розв’язана Росією проти України не змогла би реалізуватися при повазі народу України до своєї історії, державності, традицій та заможному середньому класі, який би цінував свій добробут та землю. Чи кричали би заможні люди: “Путін прийди”? Відсутність власної стратегічної державної політики, відірваність державних структур від потреб громадянського суспільства, відсутність механізмів та організацій, які вибудовували б взаємовідносини суспільства, державних органів та комерційних структур для об’єктивного осмислення соціальних, політичних або економічних процесів являється протидією консцієнтальній зброї, тобто, формуванню єдиної, без перекручень та міфів, системи соціальної комунікації, яка відповідала б потребам і цінностям людей яких вона об’єднує.

У сьогоднішніх реаліях цим займаються волонтерські організації, які об’єднують комерційні організації, суспільство і державні структури, фактично вирішуючи завдання державних органів. Тому, логічно було б віддати їм контролюючі функції з правом висловлювати вотум недовіри органам влади, що не справляються з основними функціями які на них покладені. Вкрай важко

перемогти коли в стані війни перебуває лише Генштаб та активні групи волонтерів.

Як це не дивно, але для перемоги необхідно побудувати стратегічну модель розвитку майбутнього України, показати талановитій молоді перспективи розвитку та забезпечити їх відповідними фінансовими можливостями (грандами, програмами і т.п.), заохочувати переносити в Україну виробництво високотехнологічної продукції, в кінці кінців провести реальну децентралізацію з забезпеченням прозорості управління та звітності для всіх щаблів влади.

Якщо Україна стане вітриною для якості життя пересічного громадянина і росіяни, і німці та французи захочусь переїхати на постійне місце проживання до нас, ніякої пропаганди та боротьби з фейками не буде потрібно, і саме головне - це буде правдою.

Нам необхідно перестати постійно відповідати на виклики, а будувати власну історію та економіку, незалежну від феодальних держав типу Росія.

Гуцуляк Д.М.

## ДОСВІД РОБОТИ МОБІЛЬНИХ ПРЕС-ГРУП МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ В КОНТЕКСТІ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ АГРЕСІЇ РОСІЇ НА ДОНБАСІ

14 квітня 2017 року, минуло три роки від початку Антитерористичної операції на території Луганської та Донецької областей. 14 квітня 2014 року Виконуючий обов’язки Президента України, Голова Верховної Ради України Олександр Турчинов підписав Указ №405/2014 “Про рішення Ради національної безпеки і оборони України від 13 квітня 2014 року “Про невідкладні заходи щодо подолання терористичної загрози і збереження територіальної цілісності України”, який почав антитерористичну операцію на сході України із залученням Збройних Сил України.

“Гібридну війну”, яку розв’язала Російська Федерація проти України ще називають “війною нового покоління”.

“Російська стратегія такої війни спрямована, перш за все, проти слабких місць України і Заходу (США/НАТО), а не проти їх сили. Війна нового покоління відрізняється від більшості експертних поглядів-оцінок на “…гібридний конфлікт тим, що вона поєднує в собі непоказову, приховану підтримку державою-агресором незаконних збройних формувань з її безпосереднім, повноцінним та навіть з елементами хизування втручанням на всіх етапах та у всіх формах”, наводить визначення експертів американського дослідницького фонду “Потомак” у своїй аналітичній статті на УКРІНФОРМ, “Гібридна війна Росії проти України: уроки та висновки” віце-президент Незалежного аналітичного центру геополітичних досліджень “Борисфен Інтел”, кандидат військових наук, доцент, генерал-лейтенант запасу Юрій Радковець. Він підкреслює, що окремі аспекти цієї стратегії появилися раніше в Чечні, Молдові та Грузії, але в Україні цю стратегію Росія одночасно і тестує, і

вдосконалює. Окуповані російськими окупаційними військами (російсько-терористичними силами) український Крим і окремі райони Донбасу фактично перетворені в дослідницький полігон для іспитів та тестування як модернізованих і нових російських озброєнь та військової техніки, так і для перевірки нових концепцій створення та застосування російських військ, в тому числі інформаційних і спеціальних операцій.

Інформаційній агресії Росії, та підтримуваних нею інформресурсів незаконних збройних формувань на території окремих районів Донецької та Луганської областей, активно протидіють представники військових та цивільних українських засобів масової інформації. З початку Антитерористичної операції на сході України через Прес-центр Штабу АТО представники цивільних ЗМІ висвітлюють перебіг цих подій.

З метою посилення інформаційної складової, з 20 лютого 2017 року у зв'язку із загостренням оперативної обстановки в районі проведення АТО на території Донецької та Луганської областей, з метою оперативного та об'єктивного інформування громадськості та міжнародної спільноти про хід проведення АТО, злочинні дії російсько-окупаційних військ, порушення бойовиками режиму припинення вогню, до зони відповідальності ОТУ «Луганськ», «Донецьк» та «Маріуполь» на ротаційній основі відряджаються мобільні прес-групи від Міністерства оборони України.

Згідно з окремим дорученням Державного секретаря Міністерства оборони України, до складу мобільних прес-груп входять досвідчені військові журналісти – представники засобів масової інформації Міністерства оборони України: Центрального друкованого органу МО України «Народна армія», ЦДО МО України журналу "Військо України", Центральної телерадіостудії Міністерства оборони України.

Їх завдання - оперативний збір інформації в зоні відповідальності оперативно-тактичних угруповань "Луганськ", "Донецьк" та "Маріуполь" про ворожі обстріли мирних населених пунктів, фото та відеофіксації злочинної діяльності російсько-окупаційних військ, висвітлення важкої діяльності Збройних Сил України із захисту нашої Батьківщини.

Згідно з дорученням, відповідним посадовим особам в зоні відповідальності ОТУ дано вказівку щодо всебічного сприяння діяльності мобільних прес-груп. Зокрема, щодо організації роботи, доступу на об'єкти, розміщення, технічного обслуговування тощо.

Координація діяльності прес-груп здійснюється через Прес-центр Штабу АТО (м. Краматорськ), Оперативний прес-центр (м. Авдіївка), Об'єднані центри цивільно-військового співробітництва у м. Сєвєродонецьк та Маріуполь.

З метою належної організації роботи прес-груп у місцях виконання творчих (редакційних) завдань на період відрядження, відповідальним за діяльність мобільних прес-груп в районі проведення АТО визначено заступника керівника Антитерористичної операції по зв'язках з громадськістю та засобами масової інформації.

За доповідями офіцерів Центрального друкованого органу Міністерства оборони України «Народна армія», які перебувають у складі мобільних прес-

груп в районі проведення АТО, населення Донецької та Луганської областей продовжує піддаватися негативному впливу російської пропаганди. Це відбувається не в останню чергу через відсутність українських ЗМІ у визначених районах. З огляду на це, керівництво редакції прийняло рішення (за погодженням з керівництвом Управління комунікацій та преси Міноборони України) друкувати додатковий тираж газети (1000 екземплярів) та направляти ці газети в місто Авдіївка Донецької області. Для зменшення руйнівного впливу російської пропаганди та об'єктивного інформування місцевого населення, в цих номерах друкується спеціальний вкладиш (4 сторінки), який вміщує матеріали антипропагандистської тематики та розповідає про ситуацію на лінії розмежування.

Протягом місяця, з початку роботи мобільних прес-груп військовими журналістами здійснено близько 70 виїздів на передові позиції підрозділів Сил Антитерористичної операції, підготовлено та опубліковано понад 200 інформаційних повідомлень на офіційному веб-порталі Міністерства оборони України та веб-сторінці Прес-центр Штабу АТО "Facebook" у мережі Інтернет, підготовлено та розповсюджено понад 100 відеосюжетів на каналі YouTube "Військове телебачення України" та офіційному веб-порталі Міністерства оборони України, які в подальшому використовувалися на інших телевізійних каналах України. Наприклад, відеосюжети, підготовлені військовими кореспондентами в районі бойових дій, використовуються під час підготовки військових телерадіопередач з подальшою трансляцією (щодня) в ефірі практично всіх центральних («5 канал», «УТ-1», «ICTV», «Інтер», «Україна») та кількох зарубіжних телевізійних каналів із позначкою "Відео військового телебачення".

канд. техн. наук Дзюба Т.М.
Литовченко С.М.

## АСПЕКТИ КОМУНІКАЦІЙНОЇ ВЗАЄМОДІЇ МІЖ ІНФОРМАЦІЙНО-МЕДІЙНИМИ СТРУКТУРАМИ ТА ПІДРОЗДІЛАМИ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ ЗБРОЙНИХ СИЛ УКРАЇНИ

Гібридна агресія путінської Росії проти України значною мірою реалізується через пропагандистську комунікаційну технологію. На думку фахівців Російська пропаганда або кремлівська пропаганда сьогодні, це - російська державна інформаційна політика, спеціальні інформаційні заходи ("спецоперації", "політичні технології") та відповідні державні органи і установи, які під виглядом «суспільного інформування» займаються психологічною обробкою населення Російської Федерації, а також населення інших країн – в першу чергу країн пострадянського, російськомовного простору та російської діаспори. Також об'єктом російської пропаганди є іншомовне населення у США, ЄС, арабських країнах, тощо. Загалом російська пропаганда розповсюджується щонайменше 40 мовами світу у 160 країнах.

Левова частина російського інформаційного спаму спрямовується проти України та її Збройних Сил. І тому є закономірністю поява довгоочікуваної нової редакції Доктрини інформаційної безпеки України введеної в дію Указом Президента від 25 лютого 2017 року. У цьому документі нормативно закріплено низку важливих термінологічних визначень, як то стратегічні, урядові, кризові комунікації та поняття – стратегічного наративу.

Також в одному із розділів Доктрині йдеться про механізми її реалізації через відповідні органи державної влади, міністерства і відомства.

Зокрема, Міністерство оборони України має забезпечувати функціонування системи військово-цивільних зв'язків у місцях постійної дислокації та розгортання підрозділів Збройних Сил України, інших військових формувань, а також організовувати і забезпечувати:

зв'язки з українськими та іноземними засобами масової інформації щодо висвітлення ситуації в районі проведення антитерористичної операції в Донецькій та Луганській областях;

протидію спеціальним інформаційним операціям, спрямованим проти Збройних Сил України та інших військових формувань;

супроводження інформаційними засобами виконання завдань оборони України;

донесення достовірної інформації до військовослужбовців Збройних Сил України, інших військових формувань, зокрема через засоби масової інформації Збройних Сил України.

Зазначенні доктринальні положення, на наш погляд, актуалізують аспекти комунікаційної взаємодії між інформаційно-медійними структурами та підрозділами інформаційно-психологічних спеціальних операцій Збройних Сил України, особливо в зоні проведення АТО.

При цьому слід зважати на особливості в діяльності цих структур. Вони полягають в їх підпорядкованості, виробленні специфічного інформаційного контенту що впливає на різні цільові аудиторії, режимно-секретних обмеженнях тощо.

Відомо, що інформаційно-медійні структури сьогодні підпорядковані Управлінню комунікацій та преси Міністерства оборони України та Управлінню зв’язків з громадськістю Збройних Сил України. Це військові засоби масової інформації: газета, журнал, радіо, телебачення та мережа прес-служб видів, родів військ та посади прес-офіцерів в бригадах.

До структури підрозділів інформаційно-психологічних операцій належать Головний, 74, 83 Центри та 16 загін інформаційно-психологічних операцій, які підпорядковані командуванню Сил спеціальних операцій Збройних Сил України.

Слід зазначити на тому, що досвід проведення АТО, рекомендації експертів зі стратегічних комунікацій армій НАТО при Міноборони України (хоча є обґрунтовані сумніви, що саме пропозиції Альянсу повною мірою можуть бути адаптовані в Україні. Адже сама структура Альянсу та виклики з якими він стикається відрізняється від аналогічних параметрів в Україні) свідчать що досягнення інформаційної переваги над противником досягається

через вмілу координацію діяльністю зазначених вище структур за єдиним задумом.

Тому сьогодні важливо:

- досягати консенсусу на оперативно - стратегічному рівні в питаннях формування єдиного наративу для інформаційно-медійних структур та підрозділів інформаційно-психологічних операцій Збройних Сил України (далі – структури);

- активно реагувати на дезінформацію противника, особливо в зоні АТО на оперативно-тактичному рівні, всіма силами і засобами структур;

- розробити спільну матрицю кризових ситуацій і методики їх врегулювання засобами комунікації в зоні АТО та місцях постійної дислокації військових частин (підрозділів);

- проводити систематичні узгоджувальні наради на рівні керівників та їх заступників з метою виключення непорозуміння та інформаційної асиметрії в діях підлеглого особового складу. (Структури ІПсО не можуть підміняти роботу прес-центру в зоні АТО. А фахівці прес-центру не повинні залучатися до проведення операцій з ведення противника в оману підрозділами ІПсО);

- започаткувати спільні командно-штабні навчання за єдиними задумом між фахівцями двох структур;

- синхронізувати та унормувати взаємодію між структурами у відповідних нормативних документах: спільних наказах, директивах, планах і розпорядженнях;

- розвивати міждісциплінарні наукові і навчальні програми за профілем соціальних комунікацій та інформаційно-психологічної безпеки.

До речі, експерти вважають прикладом вдалої комунікаційної взаємодії врегулювання ситуації в Костянтинівці у березні 2015 року. Коли після смертоносного ДТП за участю українських військових загинула дитина і отримала травму жінка й іще одна дитина. Це спровокувало хвилю обурення серед населення. А спецслужби РФ і сепаратисти з їх потужним потенціалом фейкових медіа підбурювали жителів міста на повстання проти влади. Тоді, разом з оперативними співробітниками МВС, Національної гвардії і СБ України, скоординовано спрацювали інформаційні служби силових відомств. У тому числі і інформаційно-медійні структури та підрозділи інформаційно-психологічних операцій Збройних Сил України.

канд. техн. наук Драглюк О.В.
Зінченко М.О.
Мужеський К.К.

## ПІДХІД ДО ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ ПРОВІДНИХ КРАЇН СВІТУ

Інформаційна боротьба ведеться не тільки в ході військового конфлікту, але ж ще задовго до його початку та після завершення. На етапі підготовки до збройної боротьби заходи інформаційної боротьби проводяться в першу чергу

на державному рівні з метою створення бажаних воєнно-політичних та економічних умов для початку агресії. З іншого боку, вона є ефективним засобом запобігання і стримування військових конфліктів. До основних особливостей ведення інформаційної боротьби в цей період можна віднести: обмеженість у використанні сил, способів і засобів інформаційного впливу на противника; дотримання існуючих норм міжнародного права, тісну взаємодію силових відомств та інших державних структур при проведенні заходів інформаційної боротьби. З початком військових (бойових) дій сили і засоби інформаційної боротьби вирішують завдання з використанням їх усього можливого арсеналу, включаючи знищення об'єктів інформаційної інфраструктури противника.

Складність ІБ обумовлена багатогранністю проявів інформації та інформаційних процесів. В збройних силах провідних країн світу інформаційна боротьба трансформується в окремий інтегрований вид стратегічного (оперативного) забезпечення операцій а в подальшому як окремий вид боротьби. Відповідно з'являються нові форми ведення інформаційної боротьби: інформаційна операція, спеціальна інформаційна операція.

Після досягнення воєнно-політичної мети інформаційна боротьба спрямована на: стабілізацію соціально-політичної обстановки в країні противника; нейтралізацію осередків опору; лояльне ставлення до перетворень в країні світової спільноти.

Інформаційна боротьба набуває активного стратегічного характеру, ведеться без обмежень у просторі та часі та характеризується економічною доцільністю, нелетальністю дії та високою ефективністю щодо досягнення воєнно-політичної мети.

Актуальне питання для інформаційної безпеки України це можливе проведення проти неї інформаційної операції. У “Об’єднаній доктрині інформаційних операцій” (*JOINT DOCTRINE FOR INFORMATION OPERATIONS (Joint Pub* 3-13*)*) інформаційна операція складається з:

1. Забезпечення заходів захисту інформації про план операції, про елементи, які суттєво впливають на досягнення успіху, про союзні сили, аби таким чином уповільнити процес прийняття рішення противником.

2. Використання усіх можливих засобів для введення в оману противника стосовно ходу операції, ключових точок місцевості, напрямків основних зусиль, що уповільнює процес прийняття рішення противником через його системи збору і аналізу інформації.

3. Використання засобів РЕБ та РЕР для впливу на противника та захист власних радіосистем.

4. Використання зброї проти визначених цілей для досягнення більшої ефективності інформаційної операції.

5. Атаки на комп’ютерні мережі.

6. Проведення психологічних операцій для забезпечення умов для відновлення порядку, підтримку дружньо налаштованого населення. Вплив на противника та нейтралізація психологічного впливу з його боку.

7. Впливи на суспільство - інформування власної і іноземної аудиторії про свої цілі, дружні війська, хід операції.

8. Цівільні впливи - встановлення військовим командуванням дружніх стосунків з місцевими органами управління, населенням, місцевим лідерами в районі своїх інтересів.

У мирний час, в умовах обмежень у використанні сил, способів і засобів кількість складових інформаційної операції зменшується до чотирьох. Це атаки на комп'ютерні мережі, психологічні операції, впливи на суспільні та цивільні відносини. Це ті види інформаційного впливу, які несуть постійну загрозу інформаційній безпеці України. З них найбільш небезпечні - це атаки на комп'ютерні мережі та психологічні операції.

Як видно з складових інформаційних операцій, вони, в основному, не підпадають під класичні правила ведення бойових дій. Ведення інформаційних операцій не потребують визначених театрів бойових дій, залучення значних людських та матеріально-технічих ресурсів, а отже потребують розробки нових нормативних актів про види та способи ведення саме інформаційної боротьби. Крім того, необхідним для такого роду боротьби є залученням фахівців різних напрямків та спеціальностей.

Зінченко М.О.
Плугова О.Б.
канд. техн. наук Драглюк О.В.

## ІНФОРМАЦІЙНА ВІЙНА, ЗАСОБИ РЕАЛІЗАЦІЇ ТА ПРОТИДІЇ

В останній час ефективно використовуються методи та засоби інформаційної боротьби, які можуть призвести до таких трагічних наслідків, як: зміна суспільного ладу та політичного устрою; розпад держави; втрата армії; розвал економічної системи в країні; втрата національної ідеї та духовних цінностей; загибель людей тощо. В інформаційному просторі України йде безперервна боротьба за управління ресурсами, вплив і контроль на території нашої держави. Події які сталися в кінці 2013 року та на початку 2014 року стали драматичними для України. Внаслідок дестабілізації внутрішньої політичної ситуації, анексії Криму та початку гібридної війни на сході України змінилася геополітична ситуація не лише в Європі, а й в усьому світі.

Слід відзначити, що впродовж останніх років, інформаційні впливи, які здійснювались російськими медіатехнологами на території Криму, південних та східних регіонах України, часто не розглядались, як загроза національній безпеці, а попит частини населення України на російські теле- та радіопрограми не викликав побоювань української влади у тому, що їх перегляд (прослуховування) з часом призведе до деструктивного і дестабілізуючого впливу на свідомість громадян, а через їхню свідомість – до зміни ставлення до самої держави.

І дійсно, агресор не шкодує фінансів на інформаційну війну, подає інформацію, що держава розвалюється, що Україною керують "радикали,

фашисти, бандерівці, нацисти, хунта", які чинять масовий безлад, вандалізм, вбивають людей на вулицях, спалюють будинки комуністів (регіоналів) та російськомовних громадян.

Канали країни агресора подають відомості про те, що біженці покидають Україну та шукають притулку в Росії, показуючи при цьому картинки з українсько-польського кордону. І хоча Росія перші плани які були ними заплановані провалила, це лише розлютило агресора та інформаційна війна набрала шалених обертів, яку Україна поки що програє. Росія влаштовує своїм глядачам повноцінне шоу «про жахіття та беззаконня в Україні, на яке не шкодують великих грошей – захоплюючий сценарій, вишукана акторська гра, відповідна музика, спеціальні ефекти, шокуючі відео.

Основними напрямами та способами маніпулятивних психоінформаційних технологій агресора відносно України були (та й залишаються надалі):

– поступове зниження міжнародного іміджу України з метою послаблення її геополітичного значення;

– відповідне дозування та спотворення інформації з метою дестабілізації ситуації в державі та впровадження власної політики;

– формування стереотипу меншовартості та вторинності українців, а також відповідне руйнування почуття нації та народу;

– домінування російської мови, культури та традицій для утвердження самоідентифікації при одночасному витісненні української мови та культури.

Подання інформації у вітчизняних ЗМІ значно програє російській стороні. Так, при висвітленні подій, пов'язаних з АТО на сході країни, цілком не варто було на початках операції повідомляти дані про кількість та дислокацію українських військових підрозділів, перелік та якість озброєння, номерні знаки, що нанесені на військову техніку, кількість убитих і поранених, виведення з ладу озброєння (наявність такої інформації дає змогу аналітикам терористів зіставити і обґрунтувати наведені цифри). Необхідно досить делікатно підходити до показів на телеекранах похоронів загиблих. Неперевірена чи сенсаційна інформація аж ніяк не слугує підняттю бойового духу в сучасних умовах ведення антитерористичної операції на Сході України та може провокувати нові інформаційні загрози. Недопустимо, щоб випуски новин виглядали ніби повідомлення з фронту, в них більше присутньою повинна бути влада, яка може не лише щось коментувати, але й вдаватися до конкретних дій. Суспільству важливо почути не лише про наші поточні негаразди, але й довідатися про шляхи і напрями реформування державного будівництва, формування України як нової політичної нації, прояви солідарності на сході та заході держави. Тобто достатніх меседжів від влади про те, що робиться або що планується робити.

Для захисту інформаційного простору та національної безпеки України необхідним є:

-зміна інформаційної політики з доповненням законодавчої та нормативно-правової бази, яка відповідала б нормам міжнародного права;

- здійснення захисту національної інформаційної сфери;

-просування української інформації на територію агресора, використовуючи при цьому сучасні технології;

-зменшення впливу олігархів на ЗМІ;

-формування та захист сприятливого образу України за допомогою сучасних технологій;

-створення та підтримка національного бренду, розвиток конкурентоспроможності на міжнародній арені;

- здійснення політики для збереження єдиної української політичної нації, на зближення політичних поглядів населення Сходу та Заходу України;

- здійснення обмеження російської інформації, яка впливає на населення Півдня та Сходу України;

- сприяння розвитку вітчизняних інтернетресурсів, які просувають іномовлення;

- здійснення діяльності в інформаційному та віртуальному просторі у національних інтересах нашої держави, поширення позитивної інформації про Україну.

Таким чином, щодо України здійснюється неймовірно потужна інформаційна війна, але українська влада ніколи не здійснює контрнаступальних дій, а обмежується лише обороною. Наша держава повинна не лише оборонятися в інформаційній війні, а й вести наступальні дії по відношенню до агресора.

Крім того, необхідним є вироблення стратегії та тактики ведення боротьби в інформаційному полі та утворити структуру, яка буде займатися аналізом та збором необхідної інформації для боротьби в інформаційній війні з агресором.

Коваль П.О.
канд. військ. наук Кацалап В.О.

## РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ОРГАНІЗАЦІЇ ТА ПРОВЕДЕННЯ ДІЙ З ПСИХОЛОГІЧНОГО ВПЛИВУ В ІНТЕРЕСАХ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ

Події на півдні та сході України показали важливість та актуальність питань інформаційно-психологічного впливу на сучасному етапі розвитку суспільства.

Перед державними і військовими органами управління країни постало завдання розробки ефективних заходів нейтралізації негативного інформаційного-психологічного впливу Російської Федерації та протидії його подальшому розгортанню.

Доктрина інформаційної безпеки є новим підходом до вирішення завдань інформаційного-психологічного протиборства. Це зумовлено зростанням ролі інформаційного-психологічного протиборства у сучасних воєнних конфліктах, перетворення психологічного впливу на одну із основних сфер бойових дій, а

також необхідністю застосування асиметричних засобів боротьби в ході протидії заходам “гібридної війни” РФ проти нашої держави.

Набуває важливості питання зменшення часу на організацію та проведення інформаційних заходів. Це питання може бути вирішене формалізацією зазначених процесів, тобто розробкою методики організації інформаційних заходів з чіткою послідовністю стандартизованих процедур.

Розробка рекомендації дає змогу в повному обсязі використовувати стандартизовані процедури планування заходів психологічного впливу, організацію діяльності сил і засобів, які залучаються до їх проведення, налагодження між ними чіткої взаємодії, а також для оперативної оцінки ефективності роботи психологічного впливу з метою вчасного і якісного корегування. Крім того, результати можуть бути використані в інтересах удосконалення навчального процесу у вищих військових навчальних закладах (за відповідною тематикою) та при проведенні наукових досліджень.

Кондратенко А.В.

## ДОСВІД ІНФОРМАЦІЙНИХ СТРУКТУР МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ В ІНФОРМАЦІЙНОМУ ПРОТИСТОЯННІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Реалізацію державної інформаційної політики в Міноборони та Збройних Силах України, ведення інформаційно-розяснювальної роботи з питань підвищення престижу військової служби, формування в українському суспільстві позитивної громадської думки щодо Збройних Сил та висвітлення їх діяльності, виконання завдань в інформаційній сфері, забезпечення ефективної діяльності системи інформування громадськості та взаємодії зі ЗМІ покладено на Управління комунікацій та преси Міністерства оборони України.

Забезпечення інформаційної діяльності Міністерства оборони України та Збройних Сил України здійснюють підпорядковані структури:

1 газета — Центральний друкований орган Міністерства оборони України «Народна армія» (м. Київ);

1 журнал — Центральний друкований орган Міністерства оборони України «Військо України» (м. Київ);

2 телерадіоорганізації — Центральна телерадіостудія Міністерства оборони України (м. Київ), Телерадіокомпанія Міністерства оборони України «Бриз» (м. Одеса).

З початку 2017 року головні зусилля Управління спрямовуються на інформування суспільства про реформування Міністерства оборони України та Збройних Сил України, їх життєдіяльність та виконання ними завдань забезпечення оборони держави, захисту її суверенітету та територіальної цілісності, зокрема, в ході антитерористичної операції на території Донецької та Луганської областей, створення позитивного іміджу ЗС України у суспільстві.

Інформаційна діяльність Міністерства оборони України спрямована на:

- своєчасне, об'єктивне та вичерпне інформування особового складу та громадськості про життєдіяльність Збройних Сил України, зокрема, в контексті останніх подій, які відбуваються в державі;

- підтримання на високому рівні морально-психологічного стану особового складу з використанням відпрацьованих форм інформаційної діяльності;

- формування психологічної стійкості, мотивації військовослужбовців до виконання найважливіших завдань щодо підтримання високої обороноздатності держави;

- створення умов для формування у Збройних Силах України розвинутого інформаційного середовища як елемента прозорого, демократичного цивільного контролю над військовими формуваннями;

- оприлюднення офіційної позиції Міністерства оборони України, забезпечення підтримки урядових рішень та вільного доступу до інформації.

Основою інформаційної діяльності Міністерства оборони України є доведення керівництвом Міністерства оборони України, Генерального штабу Збройних Сил України до громадськості відомостей про діяльність Міністерства оборони України як органу виконавчої влади та Збройних Сил України як інституту збройного захисту держави.

Основні форми поширення інформації:

- брифінги, прес-конференції та інтерв'ю керівного складу Міністерства оборони України та Генерального штабу Збройних Сил України для засобів масової інформації;

- підготовка публікацій для друкованих та електронних засобів масової інформації та ін.

Найефективнішими шляхами проведення інформаційно-роз'яснювальної роботи стали:

- постійне інформування суспільства про життєдіяльність Міністерства оборони України та Збройних Сил України шляхом оприлюднення інформаційних повідомлень на офіційному веб-порталі Міністерства оборони України у мережі Інтернет, підготовки публікацій у друкованих ЗМІ, трансляції відповідної інформації у теле- та радіоефірі;

- збільшення присутності Міністерства оборони України в мережі Інтернет та популяризація офіційного веб-порталу Міністерства оборони України шляхом розсилки інформаційних повідомлень та відео матеріалів з посиланнями на веб-портал.

З метою нейтралізації існуючих загроз в інформаційній сфері, проведення попереджувальних заходів додаткові зусилля військових ЗМІ в інформаційній сфері зосереджено на використанні всесвітньої мережі Інтернет.

З початку року Управлінням підготовлено, направлено до вітчизняних засобів масової інформації та оприлюднено через офіційний веб-портал Міністерства оборони України в мережі Інтернет близько 1600 інформаційних повідомлень і прес-релізів. Матеріали поширювалися серед вітчизняних та іноземних ЗМІ (понад 500 адресатів).

Постійно діє англомовна версія стрічки новин офіційного веб-порталу Міністерства оборони України та офіційної сторінки Міністерства оборони України у соціальної мережі «Facebook».

Постійно здійснюється цілодобовий моніторинг центральних та регіональних ЗМІ. Щоденно готуються огляди новин (тричі на добу на 8.00, 13.00 та 21.00) та дайджести газетних матеріалів з оборонної тематики.

У зв'язку з активним інформуванням громадян України про поточну суспільно-політичну ситуацію на Сході України та пов'язаним з цим надзвичайним ростом престижу військової служби у Збройних Силах України, офіційний веб-портал Міністерства оборони України відвідало понад 350 тисяч користувачів.

Найпопулярніші публікації на сторінках Міністерства оборони України у соціальних мережах поширюються за допомогою перепостів, коментування читачів, а також публікацій у засобах масової інформації.

На щоденне отримання новин від Мінооборони у соціальній мережі «Facebook» підписано 182 тисячі 495 осіб.

Кількість переглядів відеоматеріалів каналу Міністерства оборони на Інтернет-каналі «Youtube» становить 2 мільйона 887 тисяч 636 осіб. На канал підписано 4 тисячі 675 осіб.

Сторінка Міністерства оборони в соціальній мережі мікроблогів Twitter на сьогодні має 25 тисяч 815 читачів.

Найпопулярніші публікації на сторінках Міністерства оборони України у соціальних мережах активно поширюються за допомогою перепостів, коментування читачів, а також публікацій в засобах масової інформації.

З метою інформування суспільства про заходи реформування і розвитку Збройних Сил України Управлінням організовано, проведено та забезпечено інформаційне супроводження наступних найважливіших заходів за участю посадових осіб Міністерства оборони та Генерального штабу ЗС України:

за участю керівного складу Міністерства оборони та Збройних Сил України та інших посадових осіб:

- 5 брифінгів та прес-конференцій;
- участь у 7 теле-, радіопрограмах;
- 43 інтервю та коментарів вітчизняним та зарубіжним ЗМІ.

забезпечено підготовку та інформаційне супроводження участі керівництва Мінооборони у прямій телефонній лінії Кабінету Міністрів України та брифінгу для представників ЗМІ перед початком її проведення (20 січня).

На виконання рішення Міністра оборони України, з метою об'єктивного та оперативного висвітлення питань діяльності Міністерства оборони України та Збройних Сил України проводяться:

брифінги в Українському кризовому медіа-центрі речників Міністерства оборони України (двічі на тиждень);

брифінги речників Міністерства оборони України з питань АТО в Українському кризовому медіа-центрі (щодня);

брифінги англомовного речника Міністерства оборони України в Українському кризовому медіа-центрі з питань українсько-російського військового конфлікту для іноземних засобів масової інформації (щопонеділка).

Зазначені заходи дозволили значно знизити стурбованість і напругу в суспільстві щодо нагальних питань діяльності Міністерства оборони України, забезпечення військовослужбовців в зоні АТО необхідним речовим та медичним майном, піклування про них з боку держави.

Забезпечено постійне оперативне наповнення достовірною інформацією з актуальних питань державної політики (в межах компетенції) Українського національного інформаційного агентства «Укрінформ».

Також забезпечено висвітлення у засобах масової інформації заходів міжнародного співробітництва в Україні та за кордоном, участі Міністерства оборони України, Збройних Сил України у загальнодержавних заходах з нагоди державних свят та пам'ятних дат, робочих поїздок Міністра оборони України та начальника Генерального штабу – Головнокомандувача ЗС України у військові гарнізони та райони проведення Антитерористичної операції, участі Збройних Сил України у міжнародних навчаннях, тактичних навчаннях на всій території України.

канд. військ. наук Косогов О. М.
Сірик А. О.

## ОСНОВНІ ПРОБЛЕМНІ ПИТАННЯ ТА НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

В умовах триваючого геополітичного протистояння інформаційна політика РФ набула рис агресивного характеру і стала однією з найбільш ефективних для реалізації зовнішньополітичних цілей невоєнними способами.

Так, Росія тенденційно застосовує інформаційно-пропагандистські заходи для створення нових джерел нестабільності за кордоном**,** підтримує значну кількість веб-сайтів медіа-партнерства, а також інформаційних агентств в усьому світі. Також, активізувалися заходи РФ у кібернетичному просторі, які спрямовані на всіх її потенційних противників. Наприклад, необхідно відмітити кібератаки хакерських угруповань, які підтримувалися спецслужбами РФ, у 2016 року на головний офіс Демократичної партії США, що призвели до витоку тисяч електронних листів, призначених для внутрішнього користування. Американські спецслужби і досі не поставили крапку у розслідуванні "таємної операції" Росії з втручання у президентські вибори США (за заявами The Washington Post з посиланням на високопоставлені джерела).

Україна за останні три роки ведення гібридної війни з РФ найчастіше ставала жертвою негативного інформаційно-психологічного впливу та шпигунських кібератак з її боку і в таких умовах вона потребує створення адекватної системи безпеки у світі, що трансформується, де виклики національній безпеці все частіше набувають рис гібридних загроз. Ситуація у

вітчизняній інформаційній сфері в таких умовах залишається складною та характеризується наступними проблемами.

По-перше, в Україні не в повному обсязі відпрацьовано системні нормативно-правові документи, які формували б цілісну державну політику з інформаційної безпеки (насамперед, в стратегічних документах немає чіткого розподілу функцій та завдань між суб'єктами забезпечення такої безпеки) та недостатньо сформовано цілісну термінологічну систему, яка б визначала єдиний понятійний апарат у зазначеній сфері. Цю проблему розглянемо в сегменті кібербезпеки.

Необхідно відзначити, що в 2016 році Верховна Рада України попередньо схвалила законопроект "Про основні засади забезпечення кібербезпеки України" але, робота з його прийняття до кінця проведена не була. У Законі України "Про основи національної безпеки" є лише поняття "комп'ютерний тероризм" та "комп'ютерна злочинність" (без пояснень).

У Стратегії національної безпеки України використовуються терміни "кіберпростір", "кіберзагрози", "кібербезпека", "кібератака", "кіберрозвідка", "кіберзлочин", але не дається їх тлумачення. Також визначено загрози кібербезпеці і безпеці інформаційних ресурсів та пріоритетні напрями забезпечення кібербезпеки і безпеки інформаційних ресурсів.

У Стратегії кібербезпеки України, що є базовим документом у сфері кібербезпеки, взагалі не дається понятійно-категорійний апарат.

Все це призводить до того, що навіть спеціальні підрозділи силових відомств, у назві яких міститься поняття "кіберзлочинність", "кібербезпека", не забезпечені відповідними нормативними документами для визначення предмета своєї роботи.

По-друге, з початком російської агресії, відсутність в Україні загальнонаціонального міжвідомчого координаційного органу (який би узгоджував та координував діяльність різних державних та недержавних структур в інформаційному, в тому числі кібернетичному просторі), а також розпорошення зусиль між такими структурами при проведенні інформаційних заходів призвело до неспроможності вчасно та ефективно протидіяти інформаційним та кібернетичним загрозам державі.

По-третє, відсутність відповідних фахівців у системі забезпечення кібербезпеки України. Незважаючи на те, що ряд вищих навчальних закладів (військових, цивільних або відомчих) здійснюють підготовку фахівців за різноманітними спеціальностями, що можуть бути віднесені до сфери кібербезпеки, якість їх підготовки в багатьох аспектах бажає бути кращою.

Крім того, не вистачає поліпрофільних науково-дослідних інститутів, які б комплексно досліджували питання кібербезпеки (не лише проблеми обмеження доступу до інформації чи забезпечення технологічної безпеки, а й соціально-гуманітарної складової і особливо – їх поєднання).

По-четверте, широке впровадження західних програмних продуктів (зокрема, фірми Microsoft) та використання апаратних засобів зарубіжного виробництва. Пошук можливих "закладок" у цій продукції практично

неможливий, а залежність нашої держави від згаданих продуктів становить загрозливий рівень для національної безпеки.

ВИСНОВКИ

В умовах проведенням РФ деструктивного інформаційного впливу як щодо України, так і інших держав світу необхідно організовувати та здійснювати заходи протидії за такими основними напрямами [5].

– розроблення нормативно-правової бази стосовно засад державної політики у сфері інформаційної безпеки, яка б визначала взаємодію спеціалістів силових структур України з місцевими органами самоврядування, державними (недержавними) установами, громадсько-політичними організаціями, ЗМІ тощо;

створення єдиного міжвідомчого органу, який здійснюватиме керівництво, координацію та контроль заходів інформаційної безпеки (наприклад, міжвідомча комісія при РНБО);

завершення формування Національної системи забезпечення інформаційної, зокрема кібернетичної безпеки та її складових в МО України, МВС України, СБУ та інших відомствах;

визначення об’єктів критичної інфраструктури держави, виведення з ладу, знищення яких призведе до вагомих наслідків та матеріальних втрат, зокрема у воєнній сфері;

узаконення діяльності, використання за єдиним замислом патріотичного ресурсу (працівників недержавних установ, звичайних громадян України – хакерів-любителів) для виконання завдань протидії інформаційним та кібернетичним заходам;

нарощування суб’єктів, що генерують інформацію, а також присутність технічних можливостей для її поширення не тільки в інформаційному просторі України, а й за її межами;

розроблення регламентуючих документів щодо ведення інформаційної боротьби (керівництво, настанова, положення);

завершення створення збалансованої системи забезпечення інформаційної безпеки Міністерства оборони та Збройних Сил України.

підвищення ефективності роботи штабів стратегічного та оперативного рівнів ЗС України щодо підготовки та проведення інформаційних (кібернетичних) заходів, зокрема в кіберпросторі;

кадрове забезпечення та удосконалення (відновлення) належної підготовки фахівців ІПсО, в тому числі кіберфахівців;

забезпечення специфічними засобами, які б сприяли на сучасному рівні розвитку інформаційних технологій вирішенню завдання захисту об’єктів інформаційної інфраструктури держави та здійснення превентивних заходів у кіберпросторі;

удосконалення системи наукових досліджень у сфері інформаційної (кібернетичної) безпеки.

д-р військ. наук Купрієнко Д. А.

# МОДЕЛЬ СИСТЕМИ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ПРИКОРДОННОЇ БЕЗПЕКИ НА МІСЦЕВОМУ РІВНІ В УМОВАХ ВЕДЕННЯ ПРОТИВНИКОМ ВІЙН МЕТОДАМИ СУЧАСНИХ КОНЦЕПЦІЙ

*Мета доповіді* – висвітлення результатів а) аналізу доцільності запровадження стратегічних комунікацій (далі – СК) як важливого інструменту інформаційно-психологічного впливу на формування відношення місцевого населення щодо процесу забезпечення (гарантування) прикордонної безпеки (далі – ЗПБ) в умовах ведення противником війн методами сучасних концепцій; б) побудови моделі системи стратегічних комунікацій у контексті ЗПБ на місцевому рівні в умовах ведення противником війн методами сучасних концепцій.

Загалом, актуальність СК у контексті ЗПБ обумовлена особливим характером впливу соціокультурних відносин у межах прикордонних територій (феномену прикордоння) на сферу прикордонної безпеки (далі – ПБ). Так, розглядаючи екстремальні випадки, прикордоння може слугувати або «потужним щитом» на захисті національних та регіональних інтересів (у т. ч. за рахунок створення та функціонування громадських організацій з охорони правопорядку та державного кордону (далі – ДК), мережі гласних та негласних агентів тощо), або навпаки – бути джерелом зародження та розповсюдження злочинності (зокрема, контрабандної діяльності, сепаратизму, повстанських рухів, екстремізму, радикалізму, іредентизму, тероризму, розкраданню національних багатств та ін.), пособницькою базою для транснаціональної і транскордонної злочинної діяльності, не мати належної стійкості щодо інформаційно-психологічних впливів при веденні противником війн методами сучасних концепцій (гібридної, преемптивної, консцієнтальної, мереже-центричної та ін.) тощо.

Побудову сучасних стратегічних комунікацій регламентовано вимогами нормативно-правових актів України стратегічного значення, зокрема:

Воєнної доктрини України (схвалено Указом Президента України від 24.09.2015 № 555/2015);

Концепції розвитку сектору безпеки і оборони України (затверджено Указом Президента України від 14.03.2016 № 92/2016) ;

Концепції інтегрованого управління кордонами (схвалено розпорядженням КМУ від 28.10.2015 № 1149-р);

Стратегії розвитку Державної прикордонної служби (схвалено розпорядженням КМУ від 23 листопада 2015 р. № 1189-р).

Так, Воєнна доктрина України (далі – ВДУ) є системою поглядів на причини виникнення, сутність і характер сучасних воєнних конфліктів, принципи і шляхи запобігання їх виникненню, підготовку держави до можливого воєнного конфлікту, а також на застосування воєнної сили для захисту державного суверенітету, територіальної цілісності, інших життєво

важливих національних інтересів. У ній визначено, що найвищий ступінь небезпеки має загроза державному суверенітету та територіальній цілісності України, яка є ймовірною з боку Російської Федерації. Усунення (мінімізація) цієї загрози, забезпечення відсічі збройній агресії та створення умов для відновлення територіальної цілісності України потребує мобілізації всіх політичних, економічних, воєнних та соціальних можливостей держави і суспільства, що передбачає комплексне планування дій, централізоване керівництво та координацію зусиль усіх складових сектору безпеки і оборони України (далі – СБОУ), державних і громадських організацій, об'єднаних спільними цілями.

Як зазначено у ВДУ, з метою досягнення переваги над воєнним противником мають бути посилені заходи з реалізації державної інформаційної політики на тимчасово окупованій противником території і міжнародній арені. Забезпечення інформаційної складової безпеки здійснюватиметься шляхом запровадження ефективної системи заходів *стратегічних комунікацій* у діяльність суб'єктів СБОУ. У ВДУ під *СК тлумачиться 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*. Створення та впровадження системи СК є одним із напрямів розвитку СБОУ щодо інтеграції до європейських та євроатлантичних безпекових структур. А це, у свою чергу, згідно Концепції розвитку СБОУ, вимагає проведення відповідних демократичних перетворень національних безпекових інституцій.

Крім того, у Концепції розвитку СБОУ подано розподіл відповідальності складових цього сектору за організацію планування, реагування на загрози та під час виконання завдань за призначенням. Зокрема, Державна прикордонна служба України (далі – ДПСУ) приймає безпосередню участь у припиненні збройного конфлікту на ДК, у боротьбі з тероризмом, а також є головним виконавцем щодо припинення збройних та ін. провокацій на ДК, охорони ДК та суверенних прав України у її виключній (морській) економічній зоні. Згідно Закону про ДПСУ (у редакції від 28.12.2015), однією з її основних функцій є координація діяльності військових формувань та відповідних правоохоронних органів, пов'язаної із захистом ДК та пропуском до тимчасово окупованої території (далі – ТОТ) і з неї, а також діяльності державних органів, що здійснюють різні види контролю при перетинанні ДК та пропуску до ТОТ і з неї або беруть участь у забезпеченні режиму ДК, прикордонного режиму і режиму в пунктах пропуску через ДК та в контрольних пунктах в'їзду-виїзду. Отже, ДПСУ здійснює координацію зазначених суб'єктів СБОУ та ін. державних органів щодо консолідації їх потенціалів у векторі ЗПБ.

Тому, окрім ВДУ, завдання формування сталих ефективних комунікацій з населенням та інститутами громадянського суспільства, використання їх потенціалу в реалізації державної політики у сфері безпеки ДК регламентовано Концепцією інтегрованого управління кордонами, яка спрямована на підвищення ефективності реалізації державної політики у сфері безпеки ДК та імплементацію відповідних європейських стандартів з урахуванням складного

та динамічного безпекового середовища довкола України, узятих нею зобов'язань в рамках виконання Плану дій щодо лібералізації ЄС візового режиму для України та Порядку денного асоціації між Україною та ЄС. Згідно цієї Концепції суб'єктами інтегрованого управління кордонами є МВС, МЗС, Мінінфраструктури, Міноборони, СБУ, Адміністрація Держприкордонслужби, ДФС, ДМС, Національна поліція, Національна гвардія та ін. компетентні органи державної влади.

Завдання формування ефективного механізму комунікації з громадськістю та використання її потенціалу для реалізації державної політики у сфері охорони ДК, поставлені і у Стратегії розвитку ДПСУ на період до 2020 р.

З урахуванням особливостей українського прикордоння та світового досвіду забезпечення правопорядку у населених пунктах, профілактики утворення повстанських та ін. деструктивних рухів та формувань, результативним для побудови «сильного прикордоння», яке консолідоване в інтересах національної та регіональної безпеки, може вважатися тільки комплексний вплив на місцеве населення з урахуванням задоволення життєво-важливих інтересів громадян та суспільства, невід'ємною складовою якого мають бути СК.

З урахуванням зазначеного, пропонована нами модель системи стратегічних комунікацій у контексті ЗПБ на місцевому рівні в умовах ведення противником війн методами сучасних концепцій включає: а) формування належних умов для реалізації життєво-важливих інтересів населення (забезпечення сталого розвитку прикордонних територій); б) формування довіри населення до суб'єктів забезпечення ПБ; в) активізація участі населення у забезпеченні ПБ; г) нейтралізація/зменшення впливу нелегітимних (злочинних) організацій, що діють у прикордонні.

Найбільший ефект може бути отриманий, якщо позиції (а)-(в) реалізуються послідовно, а (г) – паралельно з ними. У такому разі, «сильне прикордоння» буде закономірним наслідком дії об'єктивних чинників взаємодії громадян, суспільства та держави.

Набір інструментів для реалізації пропонованого підходу не може бути універсальним, адже кожне прикордоння має свої іманентні особливості. Тому, план заходів має розроблятися на основі воєнної, прикордонної, внутрішньої, регіональної, зовнішньої та соціальної державної політики з урахуванням конкретного безпекового середовища.

При обґрунтуванні плану заходів корисним буде врахувати потенціал синергії взаємодії органів влади, бізнесу та громадянського суспільства, що визначено у Стратегії сталого розвитку «Україна – 2020» та рекомендовано у сучасних дослідженнях, присвячених територіальному розвитку. Крім того, заслуговує на увагу досвід НАТО, що викладений у «Керівництві для командира роти (взводу, відділення) з питань боротьби з повстанцями (незаконними збройними формуваннями)» (2006 р.). Зазначені у ньому прийоми та процедури уособлюють «найкращу практику», отриману з американських, австралійських та британських джерел.

Отже, у доповіді висвітлено результати аналізу доцільності запровадження стратегічних комунікацій як важливого інструменту інформаційно-психологічного впливу на формування відношення місцевого населення щодо процесу забезпечення прикордонної безпеки, а також запропоновано модель системи стратегічних комунікацій в умовах ведення противником війн методами сучасних концепцій.

Литовченко С.М.

## ОРГАНІЗАЦІЯ ПРОВЕДЕННЯ ЗАХОДІВ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГОВПЛИВУ СПОЛУЧЕНИМИ ШТАТАМИ АМЕРИКИ В РОКИ ДРУГОЇ СВІТОВОЇ ВІЙНИ

Незважаючи на вступ США у Другу світову війну 7 грудня 1942 року здійснення спроб проведення заходів інформаційно-психологічного впливу (далі – ІПсВ) було відмічене лише з січня 1942 року. Спочатку США не змогли у повному обсязі впливати на морально-психологічний стан ворога, особливо морально стійких японців. Основними причинами були низький рівень навченості та недостатня фахова підготовка особового складу залученого до проведення заходів, недостатні знання та вивчення національно-психологічних особливостей противника, низька якість матеріалів ІПсВ та непорозуміння військовим командуванням США важливості та ролі проведення заходів ІПсВ під час підготовки та безпосередньої участі у воєнних діях, відсутності ефективності їх проведення.

Робота з організації проведення заходів ІПсВ здійснювалась, зокрема у сухопутних військах, на фронтовому рівні. Безпосередньо задання були покладені на відділи психологічної війни (далі – ПсВ) фронтів. Найпотужніший було створено при штабі союзних військ в Північній Африці в листопаді 1942 року за наказом генерала Д.Ейзенхауера, в тому ж році розроблено першу настанову щодо ведення ПсВ. В подальшому на базі відділу в 1944 році було сформовано управління ПсВ при Верховному головнокомандуванні союзних експедиційних сил, яке визначало ПсВ «як розповсюдження пропагандистських матеріалів, які призначені для деморалізації ворога й придушення його волі до опору, а також підвищення морального духу союзників».

Зміни поглядів та відношення військового командування США відбулися під час проведення кампанії по захопленню Тунісу в травні 1943 року. В той час в експедиційному корпусі союзників у Північній Африці налічувалось 4,6 тис. осіб, які залучались до проведення заходів ІПсВ. За останні 10 днів кампанії було розроблено та розповсюджено близько 9,5 млн листівок. Після проведеної кампанії та встановлення факту деморалізації військ противника, якими командував німецький генерал Фон Арнім, чималим попитом перед завоюванням Тунісу на листівки-перепустки серед солдатів-італійців, за які вони навіть погоджувались платити 600 франків, погляди військового командування США різко змінилися.

Після підрахунку американськими експертами вартості листівок виготовлених за 5 років ведення воєнних дій в перерахунку на одного жителя складала близько однієї рейхсмарки, що не можливо порівняти із загальними витратами на війну.

Відчувши «смак» перемоги у ПсВ американці розпочинають розвивати напрямок її ведення. Як приклад можливо висвітлити розгортання ПсВ проти Японії, яка розпочалася навесні 1945 року.

Посилаючись на дані розвідки, на той час в Японії політична обстановка була така, що сприяла згоді правлячих кіл на беззастережну капітуляцію.

Проаналізувавши розвідувальні дані американцями було розроблено стратегічний план, основою якого було здійснення тиску військовими і політичними засобами на японських керівників з вимогою прийняти умови капітуляції без проведення висадки військ у складі морського десанту.

В плані ПсВ завдання капітуляції Японії мирним шляхом було викладено в чотирьох пунктах:

переконати військове і політичне керівництво в безнадійності опору та зазначити, що альтернатива капітуляції – повне знищення збройних сил та пригноблення населення;

пояснити переваги беззастережної капітуляції;

створити суперечності, заворушення й опозицію серед тих військових керівників, хто залишався непохитним у своєму опорі.

У цьому контексті на початку 1945 року було відпрацьовано план з переорієнтації свідомості населення Японії після її капітуляції (2 вересня 1945 року), в якому зазначались наступні заходи:

випуску інформаційних бюлетенів в яких висвітлювалось становище в країні;

доведенні підготовленої першої «об’єктивної» історії Японії;

керівництва службами суспільної інформації Японії;

підтримки діяльності лояльних громадських організацій, популяризація прогресивних національних традицій;

пропаганди демократичних перетворень у США та Великій Британії;

проведенні «чисток» в органах правопорядку, формування громадської думки, що засуджує військових злочинців, придушення небажаних мілітаристських рухів;

формуванні громадської думки щодо необхідності прийняття Японії до міжнародної економічної співдружності;

підтриманні діяльності, яка відволікає увагу японців від відродження колишніх порядків, популяризуючи міжнародні традиції, розваги, активну політичну участь у масових муніципальних заходах, створенні профспілок з метою запевнення японців в щирості американців;

пропагуванні громадських свобод і підготовки до остаточного перегляду репресивної політичної системи;

психологічній підготовці до проведення промислових, аграрних та інших економічних перетворень;

створенні умов для вільної преси;

доведенні до японців істинного значення поразки й зобов'язань з метою недопущення зустрічних звинувачень і реваншу;

припиненні діяльності анархічно-політичних рухів;

пропаганди проти мілітаризму й агресії;

поясненні демократичних ідей та тенденцій у японський культурі та історії, приведенні їх у відповідність до стандартів американської демократії;

поєднанні західних (православних) та японських етичних принципів;

підготовки до прийняття Японії в сім'ю народів на рівній соціальній та економічній основі, за умови повного викорінення ідей мілітаризму, морської могутності й експансіонізму;

відмови від наявної в США суспільної думки про японську расову неповноцінність.

Підводячи підсумок можна зазначити, що США одними з перших, ще з часів Другої світової війни визначились із організацією та порядком проведення заходів ІПсВ, хоча в подальшому багато запозичили з практичного досвіду діяльності радянських структур у Німеччині.

канд. істор. наук Луник О. О.
канд. військ. наук Корчев В. Б.

## ДЕЯКІ ПИТАННЯ ІНФОРМАЦІЙНОГО СУПРОВОДУ ЦИВІЛЬНО-ВІЙСЬКОВОГО СПІВРОБІТНИЦТВА СТРУКТУР СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ У ПРОТИДІЇ ГІБРИДНІЙ АГРЕСІЇ

Цивільно-військове співробітництво (далі – ЦВС), як одна з функцій військової компоненти структур сектору безпеки і оборони, є невід'ємною частиною сучасних багатовимірних операцій, охоплює усі співпрацюючі сторони, задіяні у вирішенні конфлікту, та сприяє взаємодії цивільних та військових структур. Визнання ЦВС важливим елементом підтримки бойових дій – стала практика провідних країн світу.

Успішний досвід українських військовослужбовців задіяних у міжнародних миротворчих операціях не став поштовхом для створення структур ЦВС. До початку проведення антитерористичної операції (далі – АТО) в окремих районах Донецької та Луганської областей це питання не було вирішено. Блокування пересування військових колон, перешкоджання виконанню завдань, передача розвідувальної інформації протиборчій стороні – це лише деякі видимі наслідки відсутності належного ЦВС та його інформаційного забезпечення. Як наслідок, ряд службово-бойових завдань підрозділами не були виконані, що призвело до неповоротних втрат серед військовослужбовців.

Серед військових ці підрозділи називають коротко – «сіміки» (від англійського CIMIC – civil military cooperation). Перший підрозділ ЦВС у зоні проведення АТО з'явився у травні 2014 року. Тоді він налічував лише 14 офіцерів Збройних сил України (далі – ЗСУ), які мали досвід участі в миротворчих місіях у Косові та Іраку. До пілотного проекту залучалися дві

групи: в районі відповідальності сектору «Б» та на кордоні з окупованим Кримом. Командування ЗСУ у січні 2015 року ухвалило рішення про створення Управління цивільно-військового співробітництва. На нову структуру покладені три основні функції: організація взаємодії, підтримка бойових підрозділів, допомога місцевим органам влади та населенню. Оскільки під час проведення АТО виникає чимало інших невирішених питань, підрозділи ЦВС займаються, зокрема, пошуком та ексгумацією тіл загиблих на окупованій території, їхнім транспортуванням, а також сприяють обміну полоненими або незаконно утримуваними військовослужбовцями на території окремих районів Донбасу. А з недавнього часу ці підрозділи здійснюють інформаційне та психологічне супроводження сімей безвісти зниклих та загиблих військовослужбовців. Такі структури мають всі країни НАТО. На жаль, у нас необхідні структури з'являються після виникнення критичної ситуації. Ось і про іракський досвід ЦВС згадали лише з початком АТО.

Особливості участі підрозділів Збройних сил України, Національної гвардії України, Міністерства внутрішніх справ, Служби безпеки України, Державної прикордонної служби України в АТО, інших бойових і спеціальних діях на сході та півдні України, окреслили суттєві проблеми в організації взаємодії між командирами підрозділів військових формувань та місцевими органами самоврядування й населенням у районах виконання завдань. Постало нагальне питання щодо налагодження цивільно-військової взаємодії структур сектору безпеки і оборони у зоні конфлікту, інформаційного супроводу цих процесів.

Як відомо, інформаційний вплив на групи населення здійснюється різними формами і методами та за допомогою різних комунікативних засобів. Досвід проведення військових та миротворчих операцій НАТО, США та інших держав реалізувався в базові положення концепції ЦВС. Цікавим для нас є положення про інформаційне забезпечення діяльності підрозділів НАТО, концепцію якого для кожної операції на окремих територіях готують фахівці ЦВС перед її проведенням.

Загальновизнана практика проведення інформаційного впливу, достатнього для отримання підтримки у місцевого населення (в залежності від специфіки регіону), дозволяє окреслити термін впливу – від трьох до чотирьох місяців. Інформаційний вплив на місцеве населення здійснюється через засоби масової комунікації (ТБ, Інтернет, радіо, друковані видання), а також шляхом розповсюдження інформації через ключових суб'єктів комунікації – осіб, які мають вплив на місцеве населення (представники органів місцевої влади, політики, бізнесмени, формальні та неформальні лідери).

На початковому етапі проведення антитерористичної операції, на віддаленні 30-40 км від лінії зіткнення, супротивник мав абсолютну перевагу у питаннях інформаційного впливу. Найбільш слабкі місця забезпечення інформаційної підтримки дій бойових підрозділів полягали у неспроможності здійснення превентивних заходів.

Специфіка роботи груп ЦВС полягає утому, що вони працюють на території своєї держави. Це дозволяє уникнути мовного, ментального,

релігійного бар'єрів, полегшує можливості впливу на місцеве населення в районі проведення бойових дій. Разом з тим недостатність правового, фінансового та методологічного забезпечення значною мірою утруднює їх функціонування. Однак, на відміну від багатьох інших суб'єктів інформаційної політики, групи ЦВС щоденно і цілеспрямовано здійснюють прозору діяльність з метою зміцнення рівня інформаційної безпеки в районах проведення АТО.

Структурні підрозділи ЗСУ: Управління цивільно-військового співробітництва, 14 оперативних груп і три центри ЦВС у Маріуполі, Сєвєродонецьку, Краматорську – щоденно готують підґрунтя для створення повноцінного інформаційного впливу на місцеве населення. У інших військових формуваннях структур сектору безпеки і оборони, на жаль, немає навіть і цих перших кроків.

Для виявлення місць (районів) проведення диверсійно-розвідувальних і терористичних операцій використовується інформація, яка надходить від різних джерел інформації (підрозділи, бази даних, взаємодіючі структури сектору безпеки і оборони, органи виконавчої влади держави й інше). Така інформація має різні інформаційні компоненти та різні значення показників достовірності і повноти інформації, що ускладнює її сумісне використовування для виявлення місця та часу можливих протиправних дій.

Необхідно зазначити, що оцінка ймовірності проведення супротивником диверсійно-розвідувальних і терористичних операцій необхідна для своєчасного прийняття рішень щодо дії підрозділів сектору безпеки і оборони у прикордонні та на лінії зіткнення.

Успішна протидія диверсійно-розвідувальним і терористичним операціям можлива за умови своєчасного виявлення інформаційних ознак місць ймовірного проведення об'єктами спостереження протиправних дій та передачі якісної (достовірної та повної) інформації у систему управління. На підставі цих даних здійснюється підготовка адекватних управлінських рішень.

Основні інформаційні ознаки типових місць (районів) можливого проведення диверсійно-розвідувальних і терористичних операцій складають: наявність позитивних агентурних даних; наявність позитивних результатів прогнозу можливих варіантів розвитку подій на національному або релігійному підґрунті в районах (місцях) прикордоння; наявність інформації, одержаної від затриманих агентів іноземних спецслужб, терористів, контрабандистів, представників опозиційних сил тощо; проведення демонстрацій з антидержавницькими вимогами; активізація діяльності спецслужб на ділянці державного кордону; наявність населених пунктів у прикордонні, жителі яких схильні до демонстративних протиправних дій; наявність підприємств промисловості, пошкодження (руйнування) яких призведе до масового зараження (іншої шкоди) цивільного населення; наявність релігійних пам'ятних місць, руйнування яких може призвести до національних та (або) релігійних конфліктів на території держави; вияви діяльності екстремістських організацій; проведення широкомасштабних масових безчинств місцевим населенням; наявність інформації, отриманої від взаємодіючих структур сектору безпеки і оборони.

Отже, для виявлення ймовірних місць проведення диверсійно-розвідувальних і терористичних операцій необхідно організувати збір даних інформаційних ознак про типові місця можливого їх проведення, визначити об’єкти впливу і планомірно здійснювати тиск на них, налагоджувати комунікації та обмін інформацією з ключовими гравцями цивільного компоненту, координувати діяльність військового компоненту. Структури ЦВС військових формувань сектору безпеки і оборони у взаємодії між собою повинні забезпечити успішне виконання цих завдань.

канд. військ. наук Ляшенко І.О.
д-р. техн. наук Солонніков В.Г.

## ОБГРУНТУВАННЯ FITNESS-ФУНКЦІЇ ДЛЯ ОЦІНКИ ЖИВУЧОСТІ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Поняття живучості відоме в техніці давно і практично використовується при створенні технічних систем різного призначення, але до цих пір не створено розвинутої теорії, яка містила б, як і теорія надійності, загальнотехнічні результати, що дозволяють досліджувати цю властивість, оцінювати її кількісно та розробляти практичні рекомендації проектувальникам складних систем по забезпеченню живучості.

Не дивно, що останніми роками спостерігається значне підвищення інтересу до цієї характеристики як в теоретичному, так і в практичному відношенні. Це можна пояснити, мабуть, наступними обставинами. По-перше, зростання масштабів і вартості систем призводить до значного зростання збитків від тривалого відключення навіть частини системи, збільшенню частки технологічно пов'язаних порушень працездатності, а отже, масштабів “ураження” системи. По-друге, у великих системах зростає складність і трудомісткість відновлюваних операцій. Тому прагнення до зменшення розмірів “ураження” системи одночасно є прагненням до створення сприятливіших умов для відновлення необхідного рівня її функціонування. По-третє, унаслідок розвинених зв'язків між різними системами і підсистемами по різних каналах (інформаційних, матеріальних і енергетичних) значну роль можуть відігравати вторинні наслідки порушень працездатності елементів системи. Збиток від вторинних наслідків може стати значно вищим, ніж від первинних наслідків, аж до повного припинення функціонування або загибелі системи. Тому виникає проблема усунення або обмеження вторинних наслідків. Нарешті, існує проблема швидкого і оптимального включення ресурсів, що збереглися в системі, на користь виконання життєво важливих функцій системи після сильного впливу на неї. Ясно,

що вирішення цієї проблеми вимагає від системи нових якостей, яких вона може і не мати в своєму розпорядженні, якщо спроектована для роботи тільки в нормальних умовах експлуатації.

Необхідно оцінити здібності системи продовжувати нормально функціонувати в умовах постійних деструктивних впливів і протистояти їм, адаптувати алгоритми функціонування до нових умов й організовувати функціональне відновлення або забезпечити функціонування в процесі деградації, можливо без втрати найбільш значимих «критичних» інформаційних функцій; необхідний перехід від аналізу і оцінки надійності до аналізу й оцінки живучості.

Окрім можливості «внутрішнього» відновлення системи після деструктивних впливів, живучість системи характеризується також можливістю впливу на зовнішнє середовище, в якому ця система функціонує. Ця можливість особливо чітко проглядається якраз в інформаційних системах.

При аналізі живучості функціонування інформаційна система характеризується:

- метою функціонування (інформування, дезінформування, інформаційний вплив і т.п.);

- множиною завдань, що виконуються нею $Z = \{z_1, z_2, z_3, ..., z_n\}$;

- множиною компонент (інформаційних ресурсів) – складових цієї системи $K = \{k_1, k_2, k_3, ..., k_m\}$;

- множиною структурних компонент системи $S = \{s_1, s_2, s_3, ..., s_l\}$ та зв'язків між ними $R = \{r_1, r_2, r_3, ..., r_j\}$.

При чому множина функцій системи не може бути змінена, повинні застосовуватись усі функції, можливо з меншою ефективністю або з погіршенням якості, тобто повинна виконуватися умова:

$$\prod_{i \in Z} x(f_i) = 1, \quad x(f_i) = \begin{cases} 1, \textit{ якщо } f_i \textit{ виконується;} \\ 0, \textit{ якщо } f_i \textit{ не виконується.} \end{cases}$$

У будь-якому випадку складається з $K = \{k_1, k_2, k_3, ..., k_m\}$ повинно виконуватися деяка підмножина функцій $F^*$, які реалізують мету функціонування інформаційної системи, тобто

$$\prod_{f_i \in F^*} x(f_i) = 1.$$

Множина функцій $F^*$ залежить від стану системи та заданих умов до живучості.

Малхазов Є.С.

# ДІЯЛЬНІСТЬ УПРАВЛІННЯ КОМУНІКАЦІЙ ТА ПРЕСИ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ ЩОДО ВИСВІТЛЕННЯ У ЗМІ УЧАСТІ ЗС УКРАЇНИ У АНТИТЕРОРИСТИЧНІЙ ОПЕРАЦІЇ

Під час агресії Російської Федерації проти України Управління комунікацій та преси Міністерства оборони України здійснює оперативне та всебічне інформування особового складу Збройних Сил України та громадськості шляхом використання наявної системи забезпечення інформаційної діяльності Міністерства оборони та Збройних Сил України.

При цьому діяльність Управління координується Адміністрацією Президента України, Міністерством інформаційної політики та профільним структурним підрозділом Кабінету Міністрів.

На виконання Розпорядження Президента України № 862/2014-рп «Про заходи щодо забезпечення інформування громадськості про антитерористичну операцію» до складу прес-центру штабу АТЦ на ротаційній основі відряджаються речник та військові журналісти з усіх підпорядкованих Міністерству оборони України військових засобів масової інформації.

Крім того, військові журналісти залучені до роботи у складі штабів оперативно-тактичних управлінь в зоні АТО, груп цивільно-військового співробітництва тощо.

Відповідно до рішення Міністра оборони України з 6 лютого 2017 року відкрито Оперативний прес-центр АТО в Авдіївці, а з 10 березня 2017 року – у Маріуполі та Сєвєродонецьку.

Основні зусилля прес-центру штабу АТО та прес-офіцерів ОТУ «Маріуполь», «Луганськ» і «Донецьк» спрямовуються на інформування громадськості про стан обстановки на лінії розмежування, проведення цільової роботи щодо формування суспільної та міжнародної думки з приводу порушення російсько-окупаційними військами Мінських домовленостей, а також на висвітлення подій, що відбуваються в районі Авдіївської промзони та безпосередньо у населеному пункті Авдіївка.

З цією метою, за інформацією прес-центру штабу АТО починаючи з 1 січня забезпечено регулярне надходження інформаційних повідомлень (у середньому 4-5 за добу) через Прес-центр штабу АТО у ЗМІ, а також своєчасне опрацювання відповідних матеріалів, які ставали основою для проведення брифінгів речників Міністерства оборони, КМУ та Адміністрації Президента України. А саме організовано:

роботу понад 500 груп вітчизняних та закордонних ЗМІ;

щоденні інформаційні повідомлення та коментарі речника АТО для вітчизняних та закордонних ЗМІ (прямі включення);

щоденні ранкові і вечірні відеоповідомлення щодо подій в районі проведення АТО (на сторінці Прес-центру штабу АТО у Фейсбуці);

щоденні текстові інформаційні повідомлення щодо подій в районі проведення АТО (на сторінці Прес-центру штабу АТО у Фейсбуці);

інформаційні повідомлення про виконання службових (бойових) завдань військовослужбовцями органів управління, військових частин і підрозділів ЗС України в районі проведення АТО (на сторінці Прес-центру штабу АТО в Фейсбуці);

спростування неправдивих інформаційних повідомлень, поширених ЗМІ.

Прес-центром штабу АТО систематично здійснюється інформування суспільства щодо поточної ситуації в регіоні, висвітлюються брифінги керівника Спільного центру з контролю та координації питань припинення вогню та стабілізації лінії розмежування сторін щодо роботи центру, надається інформація про роботу спостережної місії ОБСЄ, проводяться брифінги та прес-конференції щодо ситуації в районі проведення АТО.

Крім того з метою об'єктивного інформування громадськості про ситуацію в зоні проведення антитерористичної операції у Донецькій та Луганській областях, відеофіксації доказів присутності військовослужбовців Російської Федерації на території України, знищення ворожої військової техніки особовим складом військових частин і підрозділів Збройних Сил України та інших наслідків ведення бойових дій, командирам військових частин і підрозділів в зоні АТО керівництвом Міністерства оборони України та Генерального штабу Збройних Сил України доручено забезпечити проведення відеофіксації фактів знищення особового складу та військової техніки ЗС РФ, а також інших фактів, які підтверджують присутність збройних сил РФ на території України.

У разі, якщо на місце фіксації не можуть вчасно дістатися знімальні групи прес-центру штабу АТО, зйомки доручено проводити безпосередньо силами особового складу підрозділів, які виконують завдання в даній місцевості, після чого зафіксовані дані оперативно передаватимуться до прес-центру штабу АТО.

Окрім того, Управлінням започатковано Курси підвищення медійної компетенції для українських журналістів з питань висвітлення проблематики АТО, з метою подальшого запровадження дворівневої акредитації в зоні АТО та змін до правил відвідування журналістами військових частин Збройних Сил України, які виконують бойові завдання безпосередньо на лінії зіткнення.

Павлюк М.Л.

## ОРГАНІЗАЦІЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ В ІНТЕРЕСАХ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ

Україна, яка є мішенню РФ у «гібридній» 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.

Стратегічні комунікації є тим інструментом, що відповідає всім зазначеним вимогам, а також застосовується в сучасній практиці провідних акторів міжнародного простору. З огляду на специфічний стан неоголошеної війни в Україні для застосування нашою державою інструменту стратегічних комунікацій вважаємо за доцільне звернутися передусім до досвіду НАТО.

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.

Стратегічні комунікації в інтересах антитерористичної операції передусім мають бути спрямовані на підрив і делегітимізацію 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.

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.

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 (overarching strategic objectives);

в) визнання того, що всі операції і види діяльності є важливими компонентами процесу комунікації, оскільки все, що говорить і робить НАТО або не спромігся сказати й зробити 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.

канд. техн. наук Панченко В.М.

# ПЕРСПЕКТИВИ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ СФЕРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У НАЦІОНАЛЬНІЙ АКАДЕМІЇ СБ УКРАЇНИ

До 2016 року підготовка фахівців для сфери інформаційної безпеки в Україні здійснювалася у понад десяти вищих навчальних закладах за спеціальностями галузі знань «Інформаційна безпека», у тому числі в Національній академії СБ України, Національному авіаційному університеті, Національному технічному університеті України «КПІ імені І. Сікорського». Після запровадження Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29 квітня 2015 року № 266 (далі – Постанова-266), спеціальності галузі знань «Інформаційна безпека» стали складовою підготовки фахівців за спеціальністю «125 Кібербезпека» галузі знань «12 Інформаційні технології», а спеціальність «Організація захисту інформації з обмеженим доступом» із галузі знань ««Військові науки, національна безпека, безпека державного кордону» увійшла до спеціальності «073 Менеджмент» (наказ МОН України від 06.11.2015 року № 1151).

Внаслідок зазначених змін, у системі підготовки кадрів для сфери інформаційної безпеки держави було втрачено два напрямки: інформаційно-психологічної безпеки та охорони державної таємниці, що є абсолютно неприпустимим в умовах зовнішньої агресії з боку РФ.

Так, діяльність фахівця з інформаційно-психологічної безпеки полягає у протидії розвідувально-підривній діяльності іноземних спецслужб, що здійснюється через суб'єктів інформаційної діяльності, веденні заходів інформаційного протиборства в інтересах України, протидії інформаційним операціям проти України та маніпулюванню суспільною свідомістю тощо. Основним завданням такого фахівця є уміння розпізнавати та протидіяти інформаційним операціям, які сьогодні активно проводяться російськими спецслужбами проти України.

Діяльність фахівця з організації захисту інформації з обмеженим доступом пов'язана, насамперед, із захистом державної таємниці. Відповідно до Закону України «Про державну таємницю» спеціальним уповноваженим органом державної влади у сфері охорони державної таємниці є Служба безпеки України. Відтак, найбільш підготовлені за цією спеціальністю випускники проходять військову службу (працюють) в органах СБ України. Проте підготовка фахівців з організації захисту інформації з обмеженим доступом здійснювалася не лише для потреб спецслужби. На сьогодні в Україні діяльність, пов'язану із державною таємницею, провадять понад 5 тис. режимно-секретних органів підприємств установ, організацій різних форм власності, які спільно з СБ України беруть участь у забезпеченні державної безпеки. Зокрема, це підрозділи Міністерства оборони України, Служби зовнішньої розвідки України, Державної прикордонної служби України,

Управління державної охорони України, Національної гвардії України, недержавних установ та організацій.

З огляду на зазначене, з метою створення належних умов для функціонування системи підготовки кадрів для сфери забезпечення інформаційної безпеки, у тому числі охорони державної таємниці, Службою безпеки України у 2016 році внесено до Міністерства освіти і науки України письмові пропозиції про включення до галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» Постанови-266 нової спеціальності 256 «Інформаційна безпека (спеціалізації за видами діяльності державних органів у сфері забезпечення інформаційної безпеки)».

Зважаючи на агресію РФ проти України, зростання ролі інформаційних засобів у цьому протистоянні, а також клопотання безпекових відомств, зокрема і зазначені вище від Служби безпеки України, постановою Кабінету Міністрів України від 01 лютого 2017 року № 53 (далі – Постанова-53) у галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» Постанови-266 введено нову спеціальність 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)». При цьому відповідно до вимог Постанови-53 для нової спеціальності 256 «Національна безпека» вид (види) діяльності затверджуються відповідним державним органом, який забезпечує виконання завдань у сфері національної безпеки, за погодженням з Міністерством освіти і науки України.

Керуючись положеннями статті 7 Закону України «Про основи національної безпеки України», статті 2 Закону України «Про Службу безпеки України», статті 5 Закону України «Про державну таємницю», Доктрини інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № 47, та виходячи з компетенції Служби безпеки України з протидії загрозам національній безпеці України в інформаційній сфері, на сьогодні Національною академією СБ України здійснюються заходи щодо затвердження в установленому порядку в рамках нової спеціальності 256 «Національна безпека» окремого виду діяльності – «забезпечення державної безпеки в інформаційній сфері».

Зауважимо, що Національна академія СБ України здійснює підготовку фахівців для сфери інформаційної безпеки з 2003 року, а з 2012 року - підготовку офіцерів запасу за військово-обліковими спеціальностями «Організація психологічної боротьби», «Організація та ведення інформаційної боротьби», «Захист від інформаційно-психологічного впливу», «Організація та ведення інформаційної боротьби в кібернетичному просторі», «Захист інформації», «Організація режиму секретності, секретного діловодства та архівна справа». В рамках заходів співпраці Україна-НАТО з 2003 року на базі Навчально-наукового інституту інформаційної безпеки Національної академії СБ України щорічно проводиться семінар підвищення кваліфікації працівників державних органів, підприємств, установ і організацій України, які працюють з інформацією НАТО з обмеженим доступом. Крім цього, Національна академія СБ України - єдиний у державі навчальний заклад, який має ліцензію Міністерства освіти та науки України на проведення підвищення кваліфікації

фахівців режимно-секретних підрозділів державних органів, органів місцевого самоврядування, підприємств, установ та організацій України, що провадять діяльність, пов’язану з державною таємницею.

Таким чином, підготовку фахівців для сфери інформаційної безпеки держави у Національній академії СБ України у подальшому планується здійснювати за спеціальністю 256 «Національна безпека (забезпечення державної безпеки в інформаційній сфері)». До основних складових навчальної програми за цією спеціальністю пропонується включити питання:

– безпеки інформаційних ресурсів (захисту інформації з обмеженим доступом);

– безпеки інформаційно-телекомунікаційної інфраструктури (кібербезпеки);

– безпеки інформаційного простору (протидія інформаційним операціям, стратегічні комунікації).

канд. техн. наук Пащенко Т.П.

## ГІБРИДНА ВІЙНА ТА СОЦІАЛЬНІ МЕРЕЖІ

Поняття гібридна війна вперше з’явилося у військових документах США і Великобританії. Думки спеціалістів щодо визначення поняття “гібридна війна” є неоднозначними. Взагалі воно означає підпорядкування певній території за допомогою інформаційних, електронних, кібернетичних операцій у поєднанні з діями озброєних сил, спеціальних служб і інтенсивним економічним тиском. Основним інструментом гібридної війни є створення державою-агресором в державі, обраній для агресії, внутрішніх протиріч та конфліктів з подальшим їх використанням для досягнення політичних цілей агресії.

Експерти називають гібридну війну типом конфлікту, який все частіше буде застосовуватися у XXI столітті. Гібридна війна, яку розв’язано проти України, ведеться одразу на декількох рівнях та напрямах, одним з яких є інформаційний. На думку Євгена Магди, одного із провідних в Україні політичних експертів*:* “Гібридна війна впливає перш за все на свідомість людей”.

Хоча військова складова конфлікту об’єктивно залишається основним чинником його розгортання, однак масштаби застосування інформаційної складової стають дедалі більшими. Про масштаби інформаційної війни, розгорнуті Росією проти України, найточніше сказав колишній головнокомандувач об'єднаних Збройних сил НАТО в Європі Ф. Брідлав: “Це найбільш дивовижний інформаційний бліцкриг, який ми коли-небудь бачили в історії інформаційних воєн”.

Інформаційна складова гібридної війни на всіх її етапах несе в собі функції забезпечення. На першому етапі інформаційна складова створює умови для виникнення конфліктної ситуації. На другому етапі – привід для опосередкованого втручання держави-агресора у внутрішні справи атакованої

країни. На третьому етапі – створює відповідний медійний простір для легітимізації дій агресора. У такому разі цільовими групами для інформаційних атак є:

цивільне населення, що перебуває в зоні конфлікту;

цивільне населення атакованої країни в цілому;

цивільне населення країни-агресора;

представники світової спільноти.

За змістом інформаційна складова гібридної війни має вигляд війни смислів (сенсів) із застосуванням інтернет-технологій та соціальних он-лайн мереж. На сьогоднішній день соціальні он-лайн мережі відіграють важливу роль у процесі поширення інформації, створюючи умови для над швидкого поширення інформаційних повідомлень.

На думку професора Г. Почепцова, відомого фахівця в галузі інформаційної війни, сьогоднішній конфлікт між Україною та Росією представляє собою “першу смислову війну в світі”. Смислова війна є довготривалою і зайнята не так фактами, скільки зміною інтерпретацій фактів, щоб опонент прийняв потрібне для атакуючої сторони рішення. У смисловій війні саме образ та візуалізація вмикають світ емоцій, де немає місця раціональним міркуванням.

Поняття інформаційна он-лайн мережева війна визначає комплекс інформаційних впливів між соціальними системами (групами), що орієнтовані на отримання певних переваг у економічних, військових, політичних, культурних та громадських протистояннях.

Головним завданням мережевих он-лайн проектів у рамках гібридної війни є створення певної віртуальної реальності, тобто образів, яких не існує в природі (симулякрів). За допомогою таких дій формується потрібне атакуючій стороні бачення ситуації конкретними цільовими групами, які є об’єктами інформаційно-психологічної агресії. У соціальних мережах поширюються великі обсяги недостовірної інформації: неперевірені “фотофакти”, “відео очевидців”, “коментарі учасників” тощо. Прикладами симулякрів є: “фашисти в Києві”, “звірства каральних батальйонів”, “розіп’яті хлопчики”.

Активна фаза військового протистояння в зоні проведення антитерористичній операції, що розпочалася з кінця лютого – початку березня 2014 р., супроводжувалася тактичною інформаційною підтримкою, яка так само використовувала прийоми побудови й експлуатації симулякрів. Україні вдалося досить швидко адаптуватися і частково відреагувати на цей виклик.

Однією з головних функцій соціальних он-лайн мереж є можливість координації інформаційних потоків, що розгортаються навколо реальних військових дій. Особливої ваги набуває завдання встановлення контролю над інформаційним простором країни, проти якої здійснюється агресія, а також тих країн, які можуть якимось чином впливати на перебіг конфлікту.

Як допоміжний засіб використовують діяльність різноманітних громадських структур – благодійних фондів, аналітичних центрів, культурних товариств тощо.

У контексті останнього особливого значення набувають технології web 2.0, які надають атакуючій стороні – країні-агресору необмежені можливості у здійсненні впливу на населення країни, проти якої здійснюється агресія.

Ефективним засобом посилення власних можливостей щодо координації інформаційних потоків може стати залучення до активної співпраці волонтерів. Волонтерський рух в середовищі он-лайн мереж як інструмент протидії інформаційній агресії або для здійснення аналогічних атак на інформаційне поле супротивника став одним із засобів протидії російській агресії проти України. Серед українських волонтерських проектів, які діють як допоміжні віртуальні ресурси в інформаційно-психологічній війні з російськими агресорами та сепаратистськими рухами, можна назвати такі: Inform Napalm, "Інформаційний спротив", центр "Миротворець".

В умовах сучасних військових конфліктів, важливе значення має система доступу до інформації, що надходить із зони бойових дій. А головним завданням будь-якої профільної військової структури є обмеження доступу до джерел інформації сторонніх осіб і поширення інформації у вигідному для себе контексті.

Соціальні он-лайн мережі є джерелом для збирання розвідувальної інформації. Події на південному сході України переконливо продемонстрували, що інформація з соціальних мереж при правильному аналізі може дати розвідці значно більше достовірних даних, чим донесення від агентурної мережі.

Розвідка відкритих джерел OSINT (Open Source Intelligence) здійснюється шляхом збору, обробки та передачі цільовому адресату інформації з загально доступних відкритих джерел з метою вирішення конкретних завдань розвідки. До відкритих джерел відносять: традиційні ЗМІ (газети, журнали, радіо, телебачення); інтернет-видання (новинні сайти та портали, інтернет-ресурси профільних структур); акаунти та віртуальні майданчики у соціальних он-лайн мережах; офіційні звіти державних структур; публічні заяви політиків та держслужбовців; спостереження – радіомоніторинг, використання загальнодоступних даних, аерофотозйомок (наприклад, Google Earth); професійні та академічні звіти, конференції, доповіді, статті; звіти та виступи в ЗМІ окремих незалежних експертів та експертних груп. За результатами різних експертних оцінок, американські розвідувальні служби з відкритих джерел добувають від 35 % до 95 % розвідданих.

У провідних країнах світу система OSINT є важливим інструментом захисту національних інтересів та основною складовою в діяльності профільних силових відомств. Зокрема, в США та країнах НАТО існують окремі мережі центрів, що займаються збиранням та обробкою інформації з подальшим формуванням відповідних баз даних та практичним їх застосуванням для прийняття необхідних рішень.

З початком розгортання повномасштабних військових дій на Донбасі, волонтери групи Inform Napalm, використовуючи методи OSINT-розвідки, не тільки розповсюджували в інтернеті отриману інформацію, а також почали складати аналітичні звіти, в яких вказували загрозливі напрямки, загрозу

утворення котлів, проривів сил терористів. Аналітики групи перші спрогнозували можливість катастрофи в секторі Д (Іловайський котел), підтверджуючи свою аналітику картами.

Таким чином, у системі сучасних економічних, політичних та військових протистоянь інформаційно-смислові війни в соціальних он-лайн мережах посідають провідне місце, як один з ключових супроводжувальних процесів. Головне призначення таких процесів – шляхом концентрації зусиль на певних ключових ланках, забезпечувати суттєві переваги в рамках комплексного протиборства сторін.

кандидат наук з державного управління Петрик В.М.

## ЩОДО ПРОВЕДЕННЯ ВСЕУКРАЇНСЬКОЇ СТУДЕНТСЬКОЇ ОЛІМПІАДИ «ШЛЯХИ ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ ВІД ШКІДЛИВИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ

1-2 квітня 2017 року була проведена **ІІІ Всеукраїнська студентська олімпіада** «Шляхи та механізми захисту інформаційного простору України від шкідливих інформаційно-психологічних впливів» в Інституті спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» (м. Київ, вул. Верхньоключова, 4).

На Олімпіаді багато уваги приділялося аналізу інформаційної агресії РФ проти України. В олімпіаді прийняло участь 15 команд (три команди від ІСЗЗІ КПІ ім. Ігоря Сікорського: «Камікадзе», «Політехнік+», «Бандерівці», керівник Петрик В.М.) із 9 ВУЗів України.

Мета олімпіади:

1. Розгляд широкого спектру реальних та потенційних загроз інформаційно-психологічній безпеці держави, суспільства і окремої особи.

2.Формування критичного мислення у студентів і курсантів.

3. Розробка рекомендацій щодо вдосконалення освітнього процесу для підготовки фахівців із захисту інформаційного простору України.

4. Визначення ролі й місця вищих навчальних та науково-дослідних закладів у забезпеченні інформаційно-психологічної безпеки держави.

І Всеукраїнська студентська олімпіада «Шляхи та механізми захисту інформаційного простору України від шкідливих інформаційно-психологічних впливів» (далі Олімпіада) відбулася в Інституті спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», ІІ Олімпіада в Національному авіаційному університеті, а IV Олімпіаду планується провести у Київському національному університеті будівництва і архітектури в березні 2018 року.

Якщо є бажаючі провести V Олімпіаду в 2019 році, звертайтеся до організатора 067-246-29-10

Сподіваюся на подальшу плідну співпрацю.

Потьомкін О.С.

# ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО СТРАТЕГІЇ ВИЗНАЧЕННЯ ДІЙ ПРЕДСТАВНИКІВ ВІЙСЬКОВИХ ПРЕС-ЦЕНТРІВ У КРИЗОВИХ УМОВАХ ЗА ДОСВІДОМ ПРОВЕДЕННЯ АТО НА ТЕРИТОРІЇ ДОНЕЦЬКОЇ ТА ЛУГАНСЬКОЇ ОБЛАСТЕЙ

В умовах агресії Російської Федерації по відношенню до України, ведення нею збройної, інформаційної та ідеологічної боротьби проти Українського народу та його культурної спадщини, існує нагальна потреба детального та поетапного вивчення питання управління військовим прес-центром в кризових умовах.

Військовослужбовці стикаються з унікальною проблемою катастроф або аварійних ситуацій. Такі фактори сприяють негайному підвищенню суспільної уваги кожен раз, коли певна обставина, або непорозуміння обумовлюють кризову ситуацію. В результаті цього перед військовим фахівцем зв'язків з громадськістю виникають непрості завдання унаслідок високої чутливості всіх прошарків суспільства і його відповідальності за надання розголосу інформації такого роду.

Саме в таких умовах особливого значення набувають питання визначення конкретних дій представників військових прес-центрів у кризових умовах та особливо в умовах проведення АТО.

Отже визначимо основні постулати для представників військових прес-центрів у кризових умовах, та коротко їх пояснимо:

1. Оприлюднення всієї інформації щодо кризового питання без затримок.

Відшукуйте можливості як всередині організації, так і поза її межами, щоб представити громадській думці вашу версію розвитку подій.

2. Формування порядку денного.

Всі події фіксуються, особливо на початковому етапі розвитку кризи. Слід повідомляти спочатку про свої пріоритети, а вже потім давати відповідь на питання представників засобів масової інформації.

3. Значимість (актуальність).

В першу чергу роз'ясніть в період кризи важливість проблеми, яка стала причиною настання кризової ситуації. Не дозволяйте ставити під сумнів важливість зробленого вами заяви.

4. Юридичні обмеження.

Негайно звертайтеся за порадою до свого юрисконсульта; у будь-якому випадку, його рекомендації повинні чинити так само оперативно, як і питання, що задаються представниками засобів масової інформації.

5. Юридичні наслідки, пов'язані з культурологічним контекстом.

Посадова особа, що займається вирішенням кризової ситуації, зобов'язаний усвідомлювати юридичні наслідки, а також уявляти собі практику правозастосування.

6. Координація інформаційних випусків.

Переконайтеся, що всі, хто має відношення до процесу координації, обізнані про хід розвитку кризової ситуації і не поширюють суперечливої інформації.

7. Думка громадськості.

Як відреагує громадськість на кризу? Виступіть з обігом як до внутрішньої, так і зовнішньої аудиторії з метою з'ясування характеру інформації про кризової ситуації, яку від вас хочуть почути.

8. Оперативність у наданні інформації.

Своєчасне реагування та задоволення прохань про надання інформації, а також відомостей про причини виникнення кризової ситуації.

9. Розповсюдження повідомлень.

Переконайтеся, що по всім обставинам справи надана належна інформація, особливо на початковому етапі розвитку кризової ситуації.

10. Облік культурологічних особливостей.

Знання культурологічних та етнічних особливостей і тонкощів мови та промови в районі виконання завдань за призначенням.

11. Офіційне представництво в особі однієї людини.

Призначте, навчіть і забезпечте усіма необхідними матеріалами одного представника організації для відповідей на внутрішні і зовнішні запити, що стосуються вашої ролі в кризовій ситуації. Цю роль може виконати командир бригади, прес-офіцер, або посадова особа, яка займає рівнозначну посаду.

12. Пожежна команда.

Особа або група осіб, що аналізують виниклі внаслідок кризи питання, які можуть ще більше роздмухати пожежу та/або ще більше погіршити ситуацію.

Отже, підбиваючи короткі підсумки, зауважимо, що аналіз питань, що стосуються антикризової комунікації, має велике значення для фахівців зв’язків з громадськістю, оскільки багатьом з них доводиться ліквідовувати наслідки кризових ситуацій на тлі їх можливого неправильного розуміння населенням Донецької та Луганської областей. Збройні сили являють собою строго формалізовану і жорстку організацію, яку громадськість не завжди вірно розуміє.

Збройні Сили мають власну історію вирішення проблем унікальною складності у зв'язку з катастрофами та аварійними ситуаціями. Незалежно від того, якою незначною може виявитися проблема, характер її сприйняття громадськістю не буде таким же, як субординація, прийнята в Збройних Силах. Тому, дуже важливо, щоб офіцер зі зв’язків з громадськістю займався вивченням кризових ситуацій, що мали місце в минулому і не очікував настання кризової обстановки на своєму об'єкті, щоб вжити відповідних заходів.

канд. техн. наук Присяжнюк М.М.

# ІНФОРМАЦІЙНА СКЛАДОВА СУЧАСНИХ ГІБРИДНИХ ВОЄН

Світові події останніх років, зокрема, революційні зміни влади та збройні конфлікти в Північній Африці, на Близькому Сході та колишньому СРСР свідчать про появу нових форм і методів досягнення провідними державами зовнішньополітичних цілей і владнання міждержавних розбіжностей.

На заміну класичним військовим агресіям приходять так звані «гібридні війни», що мають прихований характер та ведуться, переважно, у політичній, економічній, інформаційній і соціальній сферах. Збройні сили для вирішення окремих завдань залучається в невеликій кількості. Центр зусиль зміщується з фізичного знищення супротивника в рамках масштабної війни до вживання засобів «м'якої сили» проти країни-супротивника з метою дезінтеграції та зміни її керівництва, включення до сфери свого впливу.

Тема «гібридної війни» є сьогодні актуальною та потребує детального дослідження її суті, складових, форм і способів ведення.

Прикладом такої війни є агресія Росії проти України, яка стала довгостроковим чинником впливу на українську політичну, економічну, військову та соціальну сферу. Внаслідок дій Росії впродовж 2014 року деформовано систему глобальної та регіональної безпеки, а також чинну систему міжнародного права. Міжнародні гарантії безпеки для України (зокрема й Будапештський меморандум) виявилися недієздатними в умовах, коли агресором виступив один із її гарантів – Російська Федерація.

Росія застосувала проти України концепцію «гібридної війни», яка багато в чому є унікальною зі структурно-функціонального погляду: за формою вона «гібридна», а за змістом – «асиметрична». Так характер нового типу війни продемонстрували спочатку анексія Криму навесні 2014 року, потім – підтримка місцевих радикальних елементів та повномасштабне вторгнення російських підрозділів до східних областей України.

За словами генерал-майора у відставці Франка ван Каппена, члена верхньої палати парламенту Нідерландів: «Держава, яка веде гібридну війну, укладає оборудку з недержавними виконавцями – бойовиками, групами місцевого населення, організаціями, зв'язок із якими формально повністю заперечується. Ці виконавці можуть робити такі речі, які сама держава робити не може, тому що будь-яка держава зобов'язана дотримуватися Женевської та Гаазької конвенцій про закони сухопутної війни, домовленості з іншими країнами». Всю брудну роботу можна перекласти на плечі недержавних формувань. При цьому країна-агресор залишається публічно непричетною до розв'язаного конфлікту.

Варто розкрити причин виникнення самої концепції «гібридних війн».

Головною з таких причин є наявність потужних видів зброї (у т. ч. масового знищення), що робить класичні війни вкрай небезпечними, як для самого агресора, так і для всього світу. Адже це призведе до масових жертв

серед мирного населення, з'являться масштабні потоки біженців, руйнуватимуться транспортні та промислові інфраструктури, розірвуться існуючі торгівельно-економічні зв'язки тощо.

Важливим чинником є також бажання агресора применшити свою роль у розв'язанні конфліктів задля уникнення міжнародних санкцій і недопущення втрати свого авторитету та позицій на світовій арені.

Ще однією причиною є намагання встановити контроль (політичний, економічний тощо) над об'єктами агресії без надмірних збитків нападників.

В агресивних діях Росії проти України ключового значення набула психологічна обробка. Цьому чиннику Кремль приділяє першочергову увагу, адже правильно спланована акція психологічного тиску на місцеве населення позбавляє від потреби відкритого використання збройних сил.

Серед засобів психологічного впливу варто виділити такі, що спрямовані на зовнішнього користувача, на внутрішню російську аудиторію та на населення територій, де відбувається військова агресія.

Інформаційна складова гібридної війни РФ спрямована на всі три цільові аудиторії. Для зовнішнього користувача складається образ «легітимності» дій РФ в Україні – «воз'єднання Криму і міста російської слави Севастополя з матінкою Росією» та аргументи хрущовської доби щодо «несправедливості приєднання Криму до УРСР у 1954 р.», навмисно забуваючи факт, що з приєднанням Криму до УРСР до РСФСР відійшли українські етнічні землі Бєлгородської, Воронежської, Курської, Брянської та Ростовської областей. Ці ж аргументи є абсолютно валідними для російської аудиторії, стимулюючи громадську думку у вірному для Кремля напрямку.

Така сама ситуація зі створенням іміджу нелегітимності українського уряду, який прийшов до влади шляхом «військового перевороту».

Коли на Заході та у Росії переважно формується імідж фашистів виключно з представників української влади та частини українців, що «шанують нацистського коллабораціоніста Бандеру», для мешканців ОРДЛО змальовується образ «братського народу». Для територій, на яких здійснюється агресія, подібна пропаганда створила символізм ототожнення українця з бандерівцем (націоналістом), бандерівця з фашистом.

Вагомим дипломатичним інструментом для Кремля є Рада Безпеки ООН, де Росія використовує можливість заветувати будь-яке негативне рішення, звинувачує Україну та країни Заходу в ескалації ситуації.

Для громадян Росії послідовно відновлюють штампи зовнішньої загрози радянської доби. Разом із старими прийомами в обіг вводяться й нові символи, на кшталт «ввічливих людей» – членів диверсійних груп, військових розвідників та агентів Служби зовнішньої розвідки РФ, які «відстоюють інтереси росіян, відновлюють міць та престиж Росії на противагу засиллю американського впливу в країнах бувшого Радянського Союзу». Успішно використаний для легітимізації Криму як невід'ємної складової РФ образ «міста руської слави» Севастополя. Наразі використовувалася символічність міста Слов'янськ – центру тероризму на Донбасі, де «постала слов'янська єдність проти фашистської хунти Києва».

Зазначені чинники внутрішньої обробки населення Росії частково діють і на територіях України, де точиться агресія. Сприяє цьому інформаційний вакуум – сепаратисти відключили телевізійне та радіомовлення українських каналів на Донбасі, замінивши їх російськими.

Агресивна інформаційна кампанія російських ЗМІ, постійні провокації підготовкою ракетних обстрілів, руйнувань, які ніби здійснює українська армія, впливають на емоційний стан людей, що перебувають у постійному стресі та пригніченні, що сприяє ще більшій дестабілізації.

Поширеним символом, який чинить психологічний вплив на населення Донбасу, є ідея допомоги «братського народу», «руської (слов'янської) єдності», тісно переплетена з мовною ідентифікацією. Відповідно багаторічне використання риторики захисту російськомовного населення, яку сповідує Москва, ностальгія за радянським минулим та величчям, знаходить підтримку серед місцевого населення. Подібна риторика диктує тактику ведення бойових дій, коли терористи-ополченці, скеровані офіцерами ГРУ РФ, прикриваючись цивільним населенням, проводять військові акції. Сепаратисти організовують провокації, ведучи вогонь по позиціях української армії з мінометних та зенітних розрахунків, встановлених на подвір'ї багатоповерхових житлових комплексів, де проживає мирне населення. Ці акції терористів намагаються організувати масові вбивства мирних жителів руками сил антитерористичної операції, що відображає сутність нової брудної та прихованої війни Росії.

Відносно неефективним, але вживаним методом, є застосування релігійної складової інформаційної кампанії, зокрема створення на Донбасі «російської православної армії».

До не надто ефективних, але так само вживаних факторів психологічного тиску є апелювання до місцевих донбаських штампів, які формувались роками від часів Радянського Союзу. Використання подібних гасел, на кшталт «Донбасс порожняк не гонит», представниками ОРДЛО має на меті лише самозапевнення в силі регіональної ідентичності.

Варто також торкнутися теми сталості психологічної обробки населення, окупованих територій. Саме психологічний фактор є основною причиною значного відтоку населення з Донбасу, як у напрямку Росії (спричинений істеричними закликами російських ЗМІ) так і у більш безпечні регіони України. Немає сумнівів, що Росія й далі буде продовжувати випробовувати нерви українців на стійкість. Натомість українцям все ще треба віднайти «вправні ліки» проти психологічного терору «братів-росіян».

З метою надійного забезпечення національної безпеки України в інформаційній сфері необхідно вжити низку невідкладних заходів.

1. Створити ефективну систему забезпечення інформаційної безпеки держави як інструменту протидії зовнішнім інформаційним загрозам та інформаційної підтримки зовнішньої і внутрішньої політики України.

2. Вдосконалити систему підготовки фахівців у ВНЗ України з метою кадрового забезпечення структур, що мають ефективно протидіяти загрозам національній безпеці держави в інформаційній сфері.

Рахімов В.В.

# МОНІТОРИНГ ІНФОРМАЦІЙНОГО ПРОСТОРУ З МЕТОЮ ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ У ВОЄННІЙ СФЕРІ

З моменту проголошення незалежності нашої держави малу увагу спрямували на підхід до захисту інформаційного простору. Інформаційні технології застосовуються майже у всіх сферах нашого життя, що в свою чергу безпосередньо впливає на людину, суспільство і державу. Все частіше інформаційні технології використовуються для маніпулювання свідомістю, впливу та управління людьми. Комунікаційними каналами виступають мас-медіа та всесвітня мережа Internet, які створюють так звану викривлену реальність, у якій відбувається формування підпорядкованості свідомості ідеям, які пропагуються ЗМІ, що робить людину відкритою і беззахисною перед маніпулятивними технологіями. Інформація стає зброєю. Для надійного захисту національних інтересів в інформаційній сфері потрібен комплексний моніторинг зовнішніх і внутрішніх інформаційних загроз та дієві нормативно-правові, організаційно-адміністративні, науково-технічні та інші методи й засоби регулювання рівня інформаційної безпеки. По суті треба забезпечити постійний контроль і аналіз усіх джерел підвищеного інформаційного ризику, завчасне прогнозування процесів їхнього прояву та оперативне відпрацювання адекватних контрзаходів для відвернення чи мінімізації небажаних наслідків.

Поняття *"моніторинг"* (від англ. monitoring - відстеження) використовується у тому випадку, коли мова йде про постійне спостереження за будь-яким процесом з метою виявлення його відповідності очікуваному результату. Крім того, можна сказати, що моніторинг це також опис фактичного поточного стану інформаційного простору.

Проведення моніторингу інформаційного простору та виявлення загроз інформаційній безпеці у воєнній сфері надаватиме якісну оцінку рівню інформаційного впливу на елементи інформаційної інфраструктури сектору безпеки і оборони України, а це, у свою чергу, дасть змогу розробляти адекватні контрзаходи з нейтралізації інформаційних загроз.

Користуючись такими терміни які використовуються у методиці виявлення, аналізу та оцінювання інформаційних загроз державі у воєнній сфері, а саме інформаційна атака, інформаційна акція, інформаційна операція та інформаційна компанія. Розглянемо їх визначення та вплив на наш інформаційний простір.

Інформаційна атака – сукупність узгоджених та взаємопов’язаних за метою і часом інформаційних заходів, спрямованих на втручання у процес функціонування визначених об’єктів інформаційної інфраструктури. Я протикає від декількох днів до тижня

Інформаційна акція – сукупність узгоджених та взаємопов’язаних за метою, завданнями, об’єктами і часом заходів інформаційно-психологічного впливу на особовий склад збройних сил та населення противника або заходів

інформаційно-технічного впливу, спрямованих на втручання у процес функціонування його інформаційних систем, телекомунікаційних систем або інформаційно-телекомунікаційних систем. Яка протикає від декількох тижнів до декількох місяців.

Інформаційна операція - сукупність узгоджених та взаємопов'язаних за метою, завданнями, об'єктами і часом інформаційних ударів, атак та заходів, що проводяться як послідовно, так і одночасно за єдиним замислом та планом для сприяння вирішенню завдань національної політики в оборонній сфері життєдіяльності держави. Яка протикає від місяця до декількох місяців.

Інформаційна компанія – сукупність узгоджених та взаємопов'язаних за метою, завданнями, місцем і часом інформаційних операцій, ударів, акцій та атак, що проводяться послідовно й одночасно за єдиним замислом і планом для сприяння вирішення завдань реалізації національної політики в декількох сферах життєдіяльності держави. Яка протикає від декількох місяців до декількох років.

Виходячи з цих визначень, сьогодні ми бачимо, що наша держава втягнута у потужну інформаційну компанію яку веде Російська Федерація. Нас собі ми відчули та відчуваємо всі ці прояви негативного впливу через ЗМІ та мережу Internet. Організований інформаційно-психологічний вплив на людей виступає ефективним засобом досягнення різних цілей на тактичному, оперативному і стратегічному рівнях.

Доцільно розглянути деякі моменти з розвідки з відкритих джерелах якою користуються сухопутні війська США. Розвідка у відкритих джерелах (OSINT) є одним з методів ведення розвідки шляхом збору інформації з відкритих джерел, її аналізу, підготовки і своєчасного надання кінцевого продукту вищестоящому керівництву в цілях розв'язання певних розвідувальних задач. Спрощення процесів збору розвідданих. Дослідження з використанням відкритих джерел підтримує заходи щодо спостереження і рекогносцировки, в той же час, відповідає інформаційно-розвідувальним вимогам. OSINT надає інформацію (наприклад: біографія, культура населення, геопросторова інформація і технічні дані), тим самим, виключаючи необхідність залучення зайвих технічних і людських методів ведення розвідки.

Виходячи з методики розвідка у відкритих джерелах OPEN-SOURCE INTELLIGENCE (OSINT) яка викладена в «АТР 2-22.9» та різних методів та визначень можливих загроз інформаційного простору ми можемо вдосконалити нашу систему моніторингу. Спираючись на об'єктивні результати аналізу та прогнозування розвитку ситуації в ході інформаційно-аналітичної діяльності необхідно прагматично та обґрунтовано формулювати висновки для прийняття вірного рішення щодо зростання рівня небезпеки інформаційного характеру.

Цілодобовий моніторинг інформаційного простору дозволить обґрунтовано спрогнозувати підвищення рівня небезпеки, своєчасно відреагувати на його зростання або вжити адекватні заходи щодо запобігання переростання у загрозу, що в значно підвищить ефективність виявлення та оцінки загроз національній безпеці України в інформаційній сфері.

Руденко В.В.
канд. техн. наук Берека В.В.
Заєць О.В.

# ПЕРСПЕКТИВНА ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ПРИХОВАНОЇ ВОГНЕПАЛЬНОЇ ЗБРОЇ ТА БОЄПРИПАСІВ В УМОВАХ ВЕДЕННЯ ПРОТИ УКРАЇНИ ГІБРИДНОЇ ВІЙНИ

Однією з особливостей гібридної війни, яка ведеться проти України, є участь в ній нерегулярних збройних формувань. В цьому випадку, поряд з контролем за інформаційними потоками в гібридній війні, важливе значення набуває контроль за потоками зброї та боєприпасів. На сьогоднішній день фіксуються численні спроби незаконного переміщення зброї та боєприпасів. Виявлення прихованої вогнепальної зброї та боєприпасів методом прямого контакту з потенційним порушником не завжди є можливим з ряду причин, що спонукає до пошуку перспективних технологій та принципів побудови засобів виявлення вогнепальної зброї та боєприпасів на основі використання нових фізичних явищ та ознак.

У цьому контексті доповідається перспективна технологія виявлення прихованої вогнепальної зброї та боєприпасів шляхом застосування нелінійної радіолокації. Наводяться теоретичні аспекти безконтактного виявлення прихованої вогнепальної зброї та боєприпасів на основі RedOx – моделі.

На підставі аналізу електрохімічних процесів корозії зброї та боєприпасів викладається теоретичне підґрунтя до використання корозії, яка виникає при їх взаємодії з електролітами під час зберігання та бойового застосування, в якості ознаки для їх виявлення методом нелінійної радіолокації.

Стверджується, що на відміну від не окисленого металу, вольт-амперна характеристика переходу метал-окисел є суттєво нелінійною і при наведенні гармонійного сигналу нелінійним локатором на переході метал-окисел у спектрі струму з’являються друга та третя гармоніки, які можуть бути ознакою наявності прихованої зброї.

Доповідаються результати досліджень з можливості розпізнавання прихованої вогнепальної зброї та боєприпасів на фоні металевих аксесуарів одягу, прикрас з дорогоцінних металів та засобів мобільного зв’язку. Показується, що в результаті корозії зброї та боєприпасів утворюються структури метал-окисел, які мають нелінійні вольт-амперні характеристики, що суттєво відрізняються від вольт-амперних характеристик металевих аксесуарів одягу, прикрас з дорогоцінних металів та засобів мобільного зв’язку.

Пропонуються методи та способи розпізнавання прихованої вогнепальної зброї та боєприпасів з використанням багаточастотних сигналів. Оцінюється можливість такого розпізнавання при двохчастотному опроміненні та аналізі комбінаційних складових в спектрі перевипроміненого сигналу.

Використання в якості ознаки нелінійних властивостей переходу метал-окисел для безконтактного дистанційного виявлення прихованої вогнепальної

зброї дозволить підвищити ймовірність її виявлення та створити ефективний контроль за несанкціонованим розповсюдженням зброї.

Запропонована перспективна технологія виявлення прихованої вогнепальної зброї та боєприпасів в умовах ведення проти України гібридної війни відповідає проекту G 4992 в межах програми з співпраці з НАТО “Наука заради миру та безпеки”.

д-р техн. наук Савченко В.А.,

## МЕХАНІЗМ КООРДИНАЦІЇ ДІЯЛЬНОСТІ СУБ’ЄКТІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Структура та основні суб’єкти Національної системи кібербезпеки визначені Стратегією кібербезпеки України, затвердженою Указом Президента України від 15 березня 2016 року № 96/2016 (далі Стратегія). Відповідно до положень Стратегії здійснення координації та контролю діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України покладається на Раду національної безпеки і оборони України (РНБОУ).

Для запровадження дієвого механізму координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах існує необхідність у розробленні окремого керівного документу (Закону України чи постанови Кабінету Міністрів України), який би встановлював основні елементи системи кіберзахисту та порядок їх взаємодії, зокрема:

1. Створення у складі Національного координаційного центру кібербезпеки РНБОУ *Ситуаційного центру кібербезпеки*, як головного підрозділу оперативного контролю стану захищеності інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави.
2. Створення в структурах власників об'єктів критичної інформаційної інфраструктури незалежно від форми власності відповідних *відомчих ситуаційних центрів* та/або підрозділів реагування на кіберінциденти (команд CERT).
3. Створення національної телекомунікаційної мережі, як єдиної платформи захищених електронних комунікацій органів державної влади.
4. Регулювання обміну інформацією щодо спроб вчинення та/або вчинення стосовно об'єктів критичної інформаційної інфраструктури кібератак та інших несанкціонованих дій, визначення необхідних каналів обміну інформацією, форматів, періодичності та змісту для кожного із суб’єктів забезпечення кібербезпеки.
5. Визначення порядку спільного використання Національною поліцією та Службою безпеки України цілодобової контактної мережі для надання невідкладної допомоги під час розслідування кіберзлочинів.

6. Визначення порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави, порядок додавання та вилучення об’єктів з зазначеного переліку.

7. Імплементація правових норм Європейського Союзу у сфері захисту критичної інфраструктури (директива 2008/114/ЄК), зокрема з питань кібербезпеки та кіберзахисту об’єктів критичної інфраструктури.

8. Запровадження індикаторів кібербезпеки, чітке визначення понять “кібератака”, “кіберінцидент” та ін. з встановленням конкретних критеріальних оцінок зазначених термінів та порядку їх застосування.

9. Визначення відповідальності суб’єктів забезпечення кібербезпеки за порушення порядку і правил обміну інформацією про кібератаки та інші несанкціоновані дії стосовно об’єктів критичної інформаційної інфраструктури.

Загальний протокол функціонування системи забезпечення кібербезпеки повинен передбачати 3 фази (етапи):

**І. Фаза моніторингу.**

Постійний збір та аналіз Ситуаційним центром кібербезпеки РНБОУ розвідувальної інформації щодо загроз національній безпеці у кіберпросторі, контррозвідувальної інформації, інформації про кіберзагрози (кібератаки) від CERT інших країн, аналітичної інформації від власників об’єктів інформаційної інфраструктури та суб’єктів забезпечення кібербезпеки.

**ІІ. Фаза реагування.**

Зазначену фазу для різних категорій учасників доцільно розглядати за сценаріями:

**Сценарій 1.** Здійснення кібератаки/інциденту проти громадян (приватних структур):

1) звернення громадянина (приватної структури) до правоохоронних органів (МВС, Національна поліція);

2) аналіз інформації правоохоронними органами (Ситуаційний центр, CERT), прийняття рішення щодо наявності/відсутності факту кібератаки/інциденту. Надання допомоги громадянам (приватним структурам);

3) у разі підтвердження факту кібератаки/інциденту і виявлення складу злочину проведення слідчих дій, розшук та затримання підозрюваних осіб. Інформування Ситуаційного центру кібербезпеки РНБОУ;

4) у випадку масового здійснення однотипних або пов’язаних одна з одною за єдиним сценарієм кібератак/інцидентів – негайне інформування Ситуаційного центру кібербезпеки РНБОУ;

5) аналіз інформації та прийняття рішення Ситуаційним центром кібербезпеки РНБОУ щодо попередження суб’єктів кібербезпеки та запровадження специфічних заходів (блокування електронних інформаційних ресурсів, видалення контенту тощо).

**Сценарій 2.** Здійснення кібератаки/інциденту проти приватних (комерційних) банків, підрозділів Національного банку України:

1) звернення установи банку до відомчого ситуаційного центру (команди CERT НБУ);

2) блокування, усунення або локалізація їх негативних наслідків власними силами (силами команди CERT НБУ);

3) негайне інформування Ситуаційного центру кібербезпеки РНБОУ. Прийняття рішення Ситуаційним центром кібербезпеки РНБОУ щодо попередження суб'єктів кібербезпеки та запровадження специфічних заходів (блокування електронних інформаційних ресурсів, видалення контенту тощо);

4) надання інформації до Служби безпеки України. У разі виявлення факту/намірів, які можуть становити загрозу національній безпеці – проведення слідчих дій, розшук та затримання підозрюваних осіб.

**Сценарій 3.** Здійснення кібератаки/інциденту на об'єкти критичної інформаційної інфраструктури:

1) звернення власника об'єкта до відомчого ситуаційного центру (команди CERT);

2) блокування, усунення або локалізація їх негативних наслідків власними силами (силами команди CERT);

3) негайне інформування Ситуаційного центру кібербезпеки РНБОУ. Прийняття рішення Ситуаційним центром кібербезпеки РНБОУ щодо попередження суб'єктів кібербезпеки та запровадження специфічних заходів (блокування електронних інформаційних ресурсів, видалення контенту тощо);

4) надання інформації до Служби безпеки України. У разі виявлення факту/намірів, які можуть становити загрозу національній безпеці – проведення слідчих дій, розшук та затримання підозрюваних осіб.

Інформаційний обмін між суб'єктами забезпечення кібербезпеки здійснюється через існуючі мережі зв'язку та передачі інформації: пошта, телефон, Інтернет та ін. з дотриманням чинного законодавства щодо захисту державної таємниці. У подальшому, після створення національної телекомунікаційної мережі, як єдиної платформи захищених електронних комунікацій органів державної влади, зазначена мережа може бути використана для обміну інформацією про кібератаки/інциденти.

Для автоматизації процесів інформаційного обміну та організації взаємодії між суб'єктами забезпечення кібербезпеки в режимі реального часу є необхідним створення єдиної комплексної автоматизованої системи управління кібербезпекою (АСУ КБ) об'єктів критичної інформаційної інфраструктури. Зазначена АСУ КБ повинна охоплювати ситуаційні центри, команди CERT та підрозділи кіберзахисту критичної інформаційної інфраструктури. Можливості АСУ КБ повинні дозволяти автоматичне/автоматизоване виявлення, розпізнавання, аналіз та формування пропозицій щодо реагування на кібератаки/інциденти, збереження інформації та оцінювання варіантів рішень, що приймаються.

**ІІІ. Фаза узагальнення та удосконалення системи кіберзахисту.**

На підставі рекомендацій, одержаних від Ситуаційного центру кібербезпеки РНБОУ та відомчих ситуаційних центрів (команд CERT) власник об'єкта інформаційної інфраструктури здійснює заходи щодо удосконалення системи захисту, протоколів взаємодії, реорганізації структур тощо. Суб'єкти забезпечення кібербезпеки проводять аналіз існуючих нормативно-правових актів і, при необхідності, вносять пропозиції щодо зміни законодавства стосовно порядку функціонування та протоколів взаємодії суб'єктів.

канд. техн. наук Сакович Л. М.
Гиренко І. М.

# МОДЕЛЮВАННЯ РОБОТИ АПАРАТНОЇ ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ

В дійсний час отримані нові наукові результати в галузі теорії дискретного пошуку кратних дефектів, процесу дефектації засобів зв'язку з аварійними та бойовими пошкодженнями, оцінки втрат та можливостей ремонтних органів щодо відновлення пошкоджених засобів зв'язку під час ведення бойових дій, а також удосконалення метрологічного обслуговування засобів спеціального зв'язку у гібридній війні набули все більшої актуальності. Але комплектування матеріально-технічної бази польових вузлів зв'язку здійснюється за застарілими методиками без врахування цих наукових досягнень, що не дозволяє суттєво збільшити пропускну спроможність за рахунок підвищення ефективності роботи фахівців спеціального зв'язку.

Тому дослідження напрямів обґрунтування спеціалізації і кількості робочих місць ремонтного органу є досить актуальною науковою задачею, спрямованою на забезпечення необхідної укомплектованості польових вузлів зв'язку за рахунок відновлення засобів зв'язку зі слабкими ступенем пошкодження.

Під час обґрунтування і комплектування матеріально-технічної бази територіальних вузлів урядового зв'язку (далі – ТВУЗ) апаратними технічного забезпечення (далі – АТЗ) для їх ефективного використання в польових умовах необхідно вирішити завдання: розрахунок ремонтного фонду, завантаження спеціалізованих робочих місць, оцінка якості функціонування. Існуючи універсальні і спеціалізовані АТЗ призначені для виконання в польових умовах поточного ремонту (далі – ПР), вимірювання параметрів засобів спеціального зв'язку (далі – ЗСЗ) під час їх технічного обслуговування (далі – ТО) та усунення аварійних і бойових пошкоджень слабкого ступеня.

Розглянемо формування ремонтного фонду окремих груп ЗСЗ ТВУЗ для мирного часу. Кількість ПР залежить від надійності ЗСЗ та інтенсивності їх використання, а також кваліфікація користувачів:

$$z = \frac{1}{T}\sum_{i=1}^{N} t_i \ ,$$

де $T$ – наробіток на відмову, год.; $N$ – кількість ЗСЗ групи в складі ТВУЗ; $t_i$ – час використання виробу і за рік, год.

Час ПР ЗСЗ залежить від кількості електрорадіоелементів в виробі ($L$), середнього часу виконання перевірки ($t$) і усунення несправності ($t_y$), кількості фахівців (екіпажа АТЗ) ($\mu$), показників якості засобів вимірювальної техніки (далі – ЗВТ) зі складу АТЗ, тобто ймовірності правильної оцінки результату перевірки ($p$), кількості перевірок для визначення технічного стану виробу під час пошуку дефекту ($K$): $T_B(L,t,t_y,\mu,p,K)$. Значення $p$ суттєво впливає на

вартість ЗВТ, а кількість перевірок $K$ залежить від якості діагностичного забезпечення – виду і форми умовного алгоритму діагностування (далі – УАД), характеру взаємодії фахівців під час групового пошуку дефектів (далі – ГПД). Розрізняють види ГПД: зонний – кожний фахівець працює на окремій ділянці ЗСЗ (наприклад, радіоприймач або збуджувач радіопередавача), сумісний – коли всі фахівці працюють одночасно в об'єкті великої розмірності з рознесеними в просторі елементами (наприклад, підсистема електроживлення апаратної зв'язку) з обміном інформацією про результати перевірок. Для скорочення часу ПР пропонується використання агрегатного метода: спочатку визначення і заміна несправного блоку ЗСЗ, а потім пошук і заміна несправного елемента в ньому. Ця обставина потребує виконання двох умов: $T_{\text{В}} \le T_{\text{ВП}}$, $\rho \le 0,5$, тобто несправний елемент навіть при одній помилці фахівця в оцінці результату перевірки знаходиться в блоці, що замінюється.

При проектуванні перспективних АТЗ для сучасних ЗСЗ необхідно їх комплектувати ЗВТ мінімальної вартості з врахуванням пропозицій.

Крім виконання ПР АТЗ використовують для вимірювання значень параметрів ЗСЗ під час їх ТО. Загальний час використання ЗВТ АТЗ для цього складає $T_{\text{ТО}} = NT_{\text{ПП}}$, де $T_{\text{ПП}}$ – час перевірки параметрів ЗСЗ при ТО на протязі року. Встановлено, що до 10 % ПР виконують екіпажі апаратних зв'язку, а з врахуванням необхідності підготовки ЗВТ і схем вимірювання параметрів, розбирання та збирання ЗСЗ під час діагностування, аналізу результатів та оформлення документації розрахунковий час ПР і ТО збільшується в 2,5 рази, тобто загальне навантаження АТЗ за рік складає

$$W = 2,5\left( \frac{0,9(K_{\mu} + t_y \sum_{i=1}^{N} t_i + NT_{\text{ПП}}}{PT} \right),$$

де значення $T_{ПП}$ визначають з інструкції з експлуатації ЗСЗ.

Встановлено, що за винятком бойової підготовки фахівців ремонтного органу, чергування та несення вартової служби, час на ремонт ЗСЗ кожного фахівця складає за рік 900 годин, в такому разі необхідна кількість робочих місць для обслуговування і ПР групи ЗСЗ складає $R = W / 900\mu$.

Якщо $R < 1$, то фахівці і робочі місця АТЗ можливо використовувати для ТО і ПР інших груп ЗСЗ. АТЗ використовують під час польових виходів і навчань ТВУЗ, при розміщенні в місцях постійної дислокації аналогічні робочі місця фахівці використовують на пунктах технічного обслуговування і ремонту (далі – ПТОР).

Під час ведення бойових дій до розрахункового завантаження ремонтного органу мирного часу додається відновлення працездатності ЗСЗ зі слабкими ступенями пошкодження, коли кількість дефектів в ЗСЗ $Q \le 0,1L$. Відомо, що кількість втрат ЗСЗ при веденні активних бойових дій з часом зростає: якщо в кінці Великої Вітчизняної війни середньодобові втрати від штатної укомплектованості складали 1%, то з появою озброєння масового ураження вони зростають до 3%, а високоточна зброя збільшує втрати до 5%.

Втрати ЗСЗ залежать від їх місця в системі зв'язку і розташування на театрі бойових дій, а також бойових можливостей супротивника і виду операції: втрати під час наступальної операції на 15-20% більше, ніж при оборонної. В середньому вважаючи загальні втрати ЗСЗ за $\tau = 14$ діб операції $U = 0{,}35N$.

Попередня дефектація виконується екіпажами апаратних зв'язку або на збірних пунктах пошкоджених машин (далі – ЗППМ). При цьому, якщо $S = Q/L > 0{,}4$ ЗСЗ відносяться до безповоротних втрат, доля яких складає до $0{,}25U$, що підлягають списанню. Окремі справні конструктивні одиниці можливо використовувати під час ремонту аналогічних виробів агрегатним методом.

Потім під час повної дефектації з ремонтного органу $0{,}35U$ ЗСЗ направляють в середній ремонт ($0{,}25U$) або в капітальний ($0{,}1U$), якщо $0{,}1 < S \le 0{,}2$ або $0{,}2 < S \le 0{,}4$. До $0{,}4U$ ЗСЗ зі слабким ступенем пошкодженням $\delta \le 0{,}1$ підлягають відновленню в ремонтному органі ТВУЗ в польових умовах. Крім того, вони виконують ПР і ТО ЗСЗ як і в мирний час, але фахівець працює 10 годин за добу.

Розглянемо використання отриманих результатів на прикладі формування матеріально-технічної бази ремонту найбільш масових ЗСЗ – радіостанцій малої потужності. Для мирного часу ТВУЗ має $N = 200$, $t_i = 200$ год., $T = 1000$ год., тоді кількість ПР за рік

$$z = \frac{Nt_i}{T} = 40.$$

З врахуванням $T_B = 1$ год., $T_{\text{ПП}} = 0{,}5$ год. отримуємо завантаження за рік $W = 2{,}5\left(\frac{0{,}9 \cdot 1 \cdot 40}{0{,}95} + 200 \cdot 0{,}5\right) = 345$ год., тобто достатньо мати одного фахівця $\mu = 1$ з завантаженням робочого місця $W = 0{,}38$. Наприклад, на пункті технічного обслуговування і ремонту 10 ТВУЗ є одне робоче місце з вимірювальним комплектом ИК-3 для перевірки параметрів радіостанцій та набором ЗВТ загального використання (осцилограф, генератори, тестер), що достатньо.

У військовий час завантаження АТЗ складає

$$W = \frac{0{,}35 \cdot 0{,}4 \cdot 200 \cdot 2{,}5 \cdot 3}{14} + \frac{345}{365} + \frac{0{,}75 \cdot 0{,}35 \cdot 200 \cdot 1}{14} = 19{,}7$$

та потребує $\mu = 2$ робочих місця або двохзмінну роботу на одному робочому місці.

Таким чином, в результаті аналізу сучасних досягнень в галузі експлуатації складних технічних об'єктів отримана математична модель функціонування робочих місць апаратних технічного забезпечення в мирний та військовий час. В подальшому отримані результати доцільно використовувати під час модернізації існуючих або розробки перспективних ремонтних органів польових вузлів урядового зв'язку.

д-р. техн. наук Сініцин І.П.,
канд. фіз.-матем. наук Слабоспицька О.О.

# ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМИ КЕРУВАННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

Система керування Збройних сил України (ЗСУ) є складною організаційною системою, яка забезпечує саме існування держави, але постійно потребує значних ресурсних інвестицій, особливо наразі за умов гібридної війни. Тому її розбу-дову доцільно розгортати як процес прийняття, на стратегічному, оперативному й тактичному рівнях, взаємопов'язаних управлінських рішень. Вони стосуються:

а) встановлення/уточнення цілей керування ЗСУ, актуальних для забезпечення національної безпеки та обороноздатності України, і заходів для них;

б) діагностування незадовільності досягнення цілей, щойно вона виникає, та добору організаційних заходів з її усунення й запобігання їй надалі;

в) визначення обсягів ресурсів, насамперед часових, фінансових і людських, та технологій для виконання вибраних заходів.

Через організаційну, аналітичну й контекстну складність рішень а)-в), зростаючу за сучасних умов гібридної війни, вони гостро потребують актуальних і вірогідних інформаційних підстав та відстеження відповідності наслідків очікуванням зацікавлених сторін, насамперед осіб, що їх приймають, і виконавців.

Для задоволення цієї потреби в роботі запропоновано спеціалізовану інформаційну технологію експертно-аналітичного оцінювання ефективності системи керування ЗСУ (ІТЕ). Її призначення – своєчасне надання всім учасникам процесів прийняття рішень а)-в) згідно з їх рольовими повноваженнями:

– обґрунтованих кількісних оцінок базових показників ефективності системи керування ЗСУ, відповідних її фактичному чи прогнозованому стану на певний
момент часу і деталізованих за аспектами, актуальними для адресата оцінок;

– рекомендацій доцільних заходів з реформування системи керування ЗСУ.

Формальний апарат ІТЕ ґрунтується на методології "Діагностична експертиза", розробленій за участі авторів. Він поєднує п'ять складників:

– визначення базових показників ефективності системи керування ЗСУ;
– моделі та методи обчислення їх оцінок з показниками обґрунтованості;
– аналітичний процес добору експертних груп для отримання оцінок;
– технологічний процес обчислення оцінок ефективності та їх поширення між зацікавленими суб'єктами системи керування ЗСУ;
– систему сервісів автоматизованої підтримки технологічного процесу в середовищі спеціалізованих програмних засобів вітчизняного виробництва. Їх перспективним прототипом є Програмний комплекс формування та

інтелектуаль-ного узагальнення багатокритеріальних експертних оцінок, створений в ІПС.

В ІТЕ обрано три базові показники ефективності системи керування ЗСУ:

а) її результативність (effectiveness);

б) віддачу від витрат – результативність, обумовлену витратами 1 млн. грн.;

в) питому вартість результативності – обсяг коштів (млн. грн.), необхідний для досягнення 1% результативності.

*Результативність* визначено як рівень досягнення цілей керування, або "правильності складу" заходів з їх досягнення за висловом П.Друкера. Її вимірюють у % по відношенню до зазначеного рівня на момент початку реформування системи керування ЗСУ ($t_0$), який умовно приймають рівним 100%.

У свою чергу, показники б) і в) кількісно характеризують *економічну ефективність* (efficiency). Її розглядають як міру окупності витрат ресурсів на "достатньо правильні" дії, тобто правильності їх виконання.

Обчислення оцінок показників а)-в) ґрунтується на виокремленні трьох розподілених підсистем керування ЗСУ згідно з виконуваними функціями державного керування, а саме: керівництва ЗСУ ($S_1$), керування військами (силами) ($S_2$); керування бойовими засобами (зброєю) ($S_3$).

Запропоновано три групи показників ефективності системи керування ЗСУ станом на довільний момент $t$:

1) оцінки її базових показників – результативності ($R_4(t)$), віддачі від витрат ($ER_4(t)$) і питомої вартості результативності ($EC_4(t)$)

$$R_4(t)=((R_1(t)\times R_2(t)\times R_3(t))^{1/3}(\%);\ R_4(t_0)=100\%\ ; \quad (1)$$

$ER_4(t) = R_4(t) / C_4(t)$(%/млн. грн.); $EC_4(t) = (ER_4(t))^{-1}$ (млн. грн/ %.);

2) деталізуючі оцінки результативності ($R_v(t)$), віддачі від витрат ($ER_v(t)$) і питомої вартості результативності ($EC_v(t)$) для підсистеми $S_v$ керування ЗСУ

$$R_v(t)=(RO_v(t)\times RI_v(t))^{1/2}\ (\%); \quad (2)$$

$ER_v(t)=R_v(t)/C_v(t)$ (%/млн. грн.), $EC_v(t) = (ER_v(t))^{-1}$ (млн. грн/ %.), $v$=1,2,3;

3) оцінки результативності ($R_5(t)$), віддачі від витрат $ER_5(t)$ і питомої вартості результативності ($EC_5(t)$) для заходів з реформування керування в період $[t_1; t]$:

$$R_5(t_1, t) = (R_4(t) - R_4(t_1))\ (\%); \quad (3)$$

$ER_5(t_1,t) = R_5\ (t_1,t)/C_5(t_1,t)$ (%/ млн. грн.), $EC_5(t_1,t) = (ER_5\ (t_1,t))^{\ 1}$ (млн. грн/ %.),

де $RO_v(t)$ й $RI_v(t)$ – оцінки рівнів досягнення цілей підсистеми керування $S_v$, $v$=1,2,3, пов'язаних з об'єктами її зовнішнього або внутрішнього ділового середо-вища, які названі зовнішньою та, відповідно, внутрішньою результативністю;

$C_v(t)$ – вартість заходів з переведення системи керування ЗСУ ($v$=4) або підсистеми $S_v$ ($v$=1,2,3) з початкового стану на момент $t_0$ у стан на момент $t$;

$C_5(t_1,t)$ – вартість заходів з реформування системи керування в період $[t_1; t]$.

Для експертного оцінювання зовнішньої та внутрішньої результативності підсистем $S_v$, $v$=1,2,3 в ІТЕ застосовано модель переваг класу Діагностичне дерево цінності з методології "Діагностична експертиза". Воно утворене:

а) деревом (зв'язним ациклічним графом, вершини якого не повторюються і мають, крім кореня, єдиного безпосереднього попередника) ознак підсистеми $S_v$, $v$=1,2,3, що визначають її результативність з погляду адресата формованої оцінки;

б) необов'язковою множиною продукційних правил вибору доцільних заходів
з реформування $S_v$ за її індивідуальними та узагальненими експертними оцінками.

Рамкові дерева для зовнішньої результативності $S_v$, $v$=1,2,3 базуються:

– на деталізації виконуваних $S_v$ базових функцій державного керування за воєнно-політичним, адміністративним і безпосередньо військовим напрямами на страте-гічному, оперативному й тактичному рівнях керування ЗСУ;

– на типізації ресурсів підвищення результативності, наведеній в табл. 1.

Таблиця 1 – Ресурси підвищення результативності, враховані в ІТЕ

| № | Врахований ресурс |
|---|---|
| 1 | Нормативна база |
| 2 | Організаційна структура ЗСУ |
| 3 | Технології фахового навчання і бойової підготовки |
| 4 | Озброєння та військова техніка |
| 5 | Телекомунікації, засоби зв'язку, комп'ютерна техніка |
| 6 | Процеси й технології керівництва та керування |
| 7 | Автоматизовані системи керування |
| 8 | Технології забезпечення комп'ютерної безпеки |
| 9 | Інформаційні ресурси |
| 10 | Особовий склад |

Підсистемі керівництва ЗСУ зіставлені спеціальні функції [5], що деталізують функції прогнозування, координації й регулювання. На підсистему керування військами (силами) покладено деталізацію решти базових функцій – планування, організації, обліку й контролю – або відповідні їм завдання крім тих, об'єктом яких є бойові засоби (зброя). Останні розглядаються як функції системи керування бойовими засобами (зброєю). Натомість, єдине рамкове дерево для внутрішньої результативності цих підсистем зумовлене їх спільними внутрішніми цілями: мінімізацією ресурсів на прийняття управлінських рішень та підвищенням їх інформаційної обґрунтованості й оперативності.

Як показано на рис. 1, коренями рамкових дерев для оцінки результативності підсистем керування є сама ця результативність, вузлами – аспекти її розгляду, прагматично значущі для адресата оцінки, а листками – безпосередньо оцінювані експертами ознаки підсистем.

Подальша деталізація яких надлишкова для непротирічного оцінювання. Вершини довільного рівня задають покомпонентне розбиття вершини – безпосереднього попередника за аспектами, відповідними її розгляду користувачем оцінки. Кореню, вузлам, що подають актуальні для нього аспекти, і листкам дерева зіставлені необов'язкові джерела інформації для врахування експертами під час оцінювання та обов'язкова шкала – числова або вербальна. Всім вершинам надано також додатні коефіцієнти їх поточного відносного впливу на вершину-попередника порівняно з рештою її безпосередніх нащадків (одиничні за промовчанням).

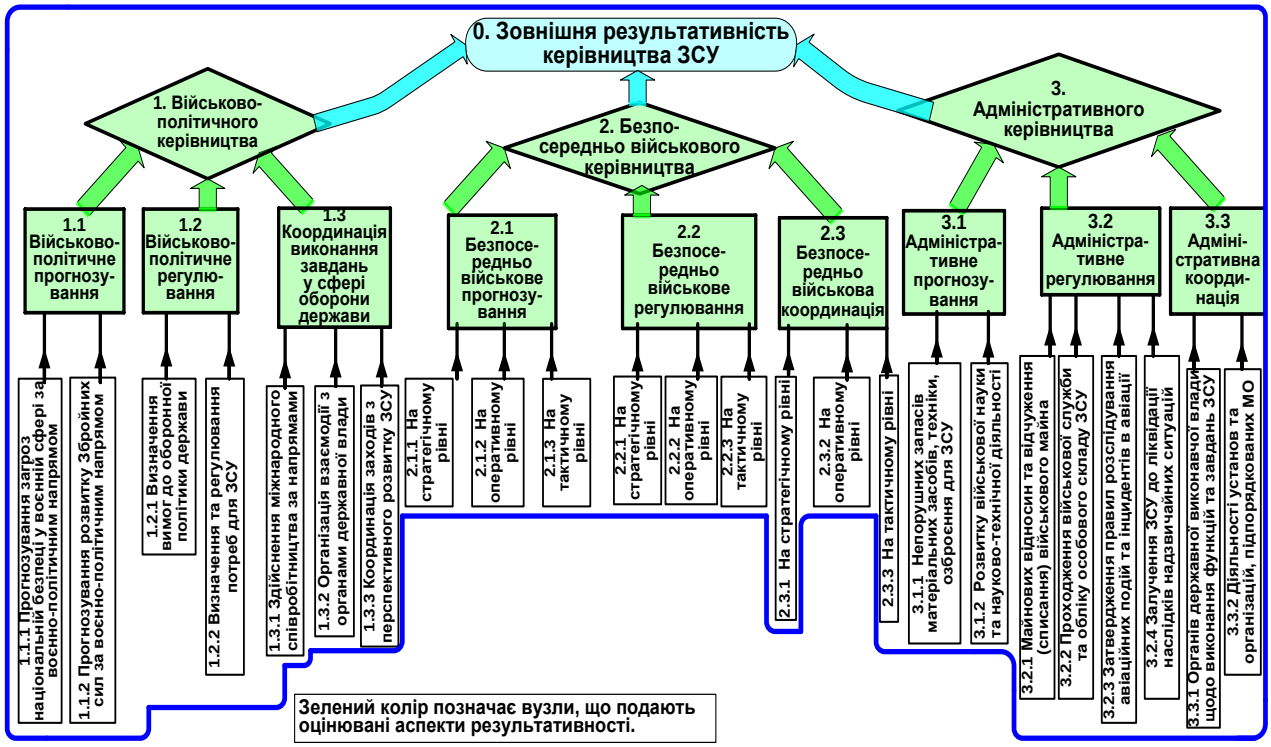


Рисунок 1 – Дерево цінності для зовнішньої результативності Керівництва ЗСУ

Узгоджені вербальні шкали для оцінювання результативності системи керування ЗСУ, її підсистем і заходів з реформування подано в табл. 2.

Для обчислення оцінок $RO_v(t)$, $RI_v(t)$ з (1)-(3) станом на запитані моменти $t \in \{t_i, i \geq 1\}$ в ІТЕ передбачено:

а) індивідуальне оцінювання листків дерев для підсистем $S_v$, $v$=1,2,3 станом на моменти $t \in \{t_i, i \geq 1\}$. Воно полягає у виборі експертом релевантної градації шкали (фрази з першого стовпця табл. 2) і наданні необов'язкових зауважень щодо структури дерева, шкали, моментів $t$ або відмові від такого вибору з обов'язковим аргументуванням його причини;

Таблиця 2 – Вербальні шкали для оцінювання результативності в ІТЕ

| № | Фраза природною мовою | Вага фрази (%) | | |
|---|---|---|---|---|
| | | Для листків рамкових дерев | Для системи керування ЗСУ та її підсистем | Для заходів з реформування |
| *Градації зростання результативності внаслідок заходів з реформування* | | | | |
| 1 | Максимально можливе підвищення | 190 | (170; 190] | (70; 90] |
| 2 | Дуже сильне підвищення | 170 | (150; 170] | (50; 70] |
| 3 | Значне підвищення | 150 | (130; 150] | (30; 50] |
| 4 | Неістотне підвищення | 130 | (105; 130] | (5; 30] |
| 5 | Практична незмінність | 100 | [95; 105] | (-5; 5] |
| *Градації спадання результативності внаслідок заходів з реформування* | | | | |
| 6 | Неістотне зниження | 70 | [70; 95) | [-30; -5) |
| 7 | Значне зниження | 50 | [50; 70) | [-50; -30) |
| 8 | Дуже сильне зниження | 30 | [30; 50) | [-70; -50) |
| 9 | Неприйнятне зниження | 10 | [10; 30) | [-90; -70) |

б) узагальнення оцінок коренів і актуальних вузлів дерев для оцінюваних підсистем та їх обґрунтування: розрахунок метричного і статистичного показників вірогідності, показника нестандартності, виявленої експертної оцінки.

Технологічний процес ІТЕ – система інформаційно спадкових підпроцесів формулювання й експертного розв'язання задачі оцінювання ефективності систе-ми керування ЗСУ в єдиному інформаційному середовищі, утвореному БД фор-мованих об’єктів структур знань ІТЕ. Окремий підпроцес охоплює етапи:

1) формулювання задачі оцінювання, що продукує її Постановку;

2) декомпозицію цієї задачі, що зіставляє первинній Постановці похідні Постановки задачі оцінювання результативності (зовнішньої та внутрішньої) підсистем $S_v$, $v$=1,2,3 з відповідними рамковими деревами або їх модифікаціями в разі незадовільності;

3) організацію й проведення експертиз за похідними Постановками, що надає Оцінки результативності (зовнішньої і/або внутрішньої) підсистем $S_v$ з первинної Постановки та обновлювані Оцінки діяльності в експертизах залучених експертів;

4) формування Розв’язку задачі оцінювання ефективності за її Постановкою.

Для реалізації підпроцесів передбачено три режими:

1) спрощений – без залучення експертів, який передбачає єдину функціональну роль Аналітика – організатора оцінювання ефективності;

2) обмежений – з формуванням корпусу експертів його Менеджером під час експертиз;

3) повнофункціональний – з попереднім добором ядра корпусу.

Систематичне застосування запропонованої технології сприятиме підвищен-ню результативності, обґрунтованості, своєчасності, цільової й ресурсної узгодженості управлінських рішень з реформування системи керування ЗСУ, оптимізації витрат ресурсів на вироблення й виконання рішень, врахуванню їх позитивних і запобіганню негативних віддалених наслідків.

канд. військ. наук Слюсарчук О.О.

## СКЛАД ОРБІТАЛЬНИХ УГРУПОВАНЬ ГЕОСТАЦІОНАРНИХ МЕРЕЖ СУПУТНИКОВОГО ЗВ’ЯЗКУ Х-ДІАПАЗОНУ

Спираючись на назви країн-заявників та назви супутникових мереж було здійснено пошук інформації щодо космічних апаратів, які входять до складу відповідних орбітальних угруповань, зокрема:

SKYNET – національна супутникова система зв’язку воєнного призначення Великобританії. На цей час знаходиться у володінні комерційної компанії Astrium Services, яка здійснює керування системою з розміщених на території Великобританії оперативних центрів управління Міністерства оборони Великобританії;

HISDESAT – іспанський супутниковий оператор, який забезпечує потреби воєнного відомства Іспанії. Вона володіє та керує супутником Spainsat;

GALS – супутники ретранслятори Х-діапазону Російської Федерації, які призначені для організації стратегічного і оперативного зв'язку в інтересах Міністерства оборони Росії і урядового зв'язку;

GOMS – російський супутник гідрометеорологічного забезпечення "Электро-Л № 1", який використовується підрозділами Росгідромета, відповідних служб Міністерства оборони Російської Федерації, а також інших відомств;

DSCS (Defense Satellite Communication System) – система стратегічного зв'язку Міністерства оборони США, яка забезпечує зв'язком вище воєнно-політичне керівництво, об'єднані і спеціальні командування з об'єднаннями, з'єднаннями, частинами (до рівня бригади) та об'єктами усіх видів і родів військ Збройних сил США. До її завдань входить передавання дипломатичної, розвідувальної а також іншої воєнної і державної інформації. З 2007 року угруповання космічних апаратів DSCS-III поступово замінюється супутниковою системою зв'язку нового покоління – Wide Global Satcom (WGS);

Syracuse-3A(B) – космічний сегмент національної супутникової системи зв'язку воєнного призначення Франції;

Sicral -1(1B) – космічний сегмент національної супутникової системи зв'язку воєнного призначення Італії, який використовується в інтересах Збройних сил, а також правоохоронних органів і агенцій з надзвичайних ситуацій;

ARABSAT-5A і BADR-5 - космічні апарати міжурядової організації Arabsat

SATCOMBw -1(2) – космічний сегмент національної супутникової системи зв'язку воєнного призначення Німеччини.

д-р військ. наук Телелим В.М.

## ЕВОЛЮЦІЯ ПОГЛЯДІВ НА РОЗВИТОК СИЛ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ ВІДПОВІДНО ДО ХАРАКТЕРУ СУЧАСНИХ ВОЄННИХ КОНФЛІКТІВ

Ще декілька років назад мало хто міг уявити, що група хакерів може спробувати вплинути на результати президентських виборів в такій країні, як Сполучені Штати Америки; що соціальні мережі Інтернет здатні формувати громадську думку і впливати на переважну більшість суспільних процесів практично в будь-якій країні світу, в якій розвинені інформаційні технології і забезпечується вільний доступ населення до Інтернет; що шляхом розповсюдження інформаційних повідомлень, часто неперевірених та неправдивих, можна впливати на кадрові рішення в вищому воєнно-політичному керівництві, тим самим визначаючи на роки розвиток цілих галузей…

Подібних прикладів можна наводити багато. Однак, неправильним буде сказати, що використання інформаційних технологій для перемоги у воєнних конфліктах властиве тільки для сьогодення.

В історії воєнного мистецтва є дуже багато прикладів використання тих чи інших форм, способів, окремих технологій інформаційної боротьби, які у фаховій літературі називались військовими хитрощами, мистецтвом воєначальників тощо.

Так, заходи, які сьогодні відносяться до психологічних та інформаційних операцій успішно застосовував ще в XIII сторіччі Чингізхан. Наприклад, при захоплені Хорезму, оцінивши співвідношення сил та з метою уникнення зайвих втрат, Чингізхан заблокував кордони Хорезму, а з усіма купцями проводив зустрічі, під час яких розповідав про силу та доблесть монгольських воїнів, обумовлені поїданням серця і печінки переможених ворогів. Ці зустрічі супроводжувались криками, які імітували процес. Крім того, купці вочевидь могли бачити пил до небес, який здіймався від начебто незчисленного монгольського війська, яке щодня поповнювалось новими загонами. В подальшому, купці розповсюджували отриману інформацію, вже від свого імені, в самому Хорезмі. Представляючи ці заходи в сучасних термінах, Чингізхан використовував:

демонстративні дії військ;

дезінформацію (з метою введення противника в оману);

залякування (один із основних способів психологічних операцій);

залучення до співпраці ключових лідерів (купців).

Причому, всі заходи проводились комплексно, за єдиним задумом, тобто повністю реалізовувались принципи сучасних стратегічних комунікацій.

В результаті, керівництво Хорезму прийняло невірне воєнно-стратегічне рішення щодо організації оборони держави, зосередженої на утриманні ключових міст, без відкритої битви. Таке рішення було прийняти при рівному співвідношенні сил, наявності підготовленої та забезпеченої армії, а також при повній підтримці власного населення. Це дало змогу Чингізхану майже безперешкодно захопити території Хорезму і послідовно знищити всі захищені пункти, які на той час вже не мали ні централізованого управління, ні взаємодії.

З появою та розвитком засобів масової інформації, їх, практично відразу, почали використовувати в воєнному мистецтві для впливу на різні цільові аудиторії.

Так, відома знаменита теза Наполеона Бонапарта: “Чотири газети зможуть принести ворогові більше зла, ніж стотисячна армія”, та менш відома, але більш змістовна цитата начальника канцелярії Особливого відділу Міністерства поліції Австрії (в ті часи) фон Фока: “Неосвічені люди, що живуть в Імперії, а особливо середній клас і простолюдини, які звикли приймати за істину все що надруковано, приходять в захват від перемог і завоювань Наполеона, особливо в віддалених містах і селищах, де кожний хто вміє читати - світило. А кожен надрукований рядок – Євангеліє”.

Воєнна пропаганда, яка є основою психологічних операцій, успішно застосовувалась в I та II світових війнах. Так, картинка, наведена на слайді

характеризує зміст воєнної пропаганди за поглядами вищого керівництва Великобританії в роки Першої світової війни.

В Другій світовій війні власні структури воєнної пропаганди мали вже більшість провідних (на той час) країн світу: Німеччина, Радянський Союз, США, Великобританія. Їхня діяльність охоплювала інформування міжнародної спільноти та власного населення, вплив на противника, здійснювала підтримку зовнішньої та внутрішньої політики держав.

Визначальна роль інформаційних операцій в воєнних конфліктах сучасності проявилась з 1991 року, з операції ОЗС НАТО “Буря в пустелі”.

Згідно замислу цієї операції, розробленого під безпосереднім керівництвом генерала Нормана Шварцкопфа, головний удар мав бути нанесений з півночі Іраку після здійснення більш ніж 100км маршу. Одночасно з маршем проводились демонстративні заходи підготовки до висадки морської піхоти на узбережжя Кувейту. Проводились посилені заходи маскування та приховування власної діяльності. Квінтесенцією заходів введення противника в оману стала прес-конференція командувача ОЗС НАТО, на якій він повідомив журналістам, що Пентагон та Брюссель прийняли рішення на нанесення головного удару з моря: силами флоту та морської піхоти.

Демонстративні дії разом з офіційно оприлюдненим замислом зіграли свою роль. Керівництво Іраку посилило оборону узбережжя Кувейту двома резервними дивізіями Республіканської Гвардії, перекинувши їх з центральних регіонів Іраку. Це дало змогу НАТО практично безперешкодно провести наступальну операцію і досягти своїх цілей.

При розробці замислу повітряних ударів в операції “Буря в пустелі” була сформульована концепція ведення воєнних дій “на основні ефектів”, яка визначила характер воєнних дій на майбутнє.

Концепція “операцій на основі ефектів” ґрунтувалась на моделі сучасної держави-нації, яка являла собою структуру з п’яти концентричних кіл. Центральне коло, яке представляло національних лідерів (найбільш критично важливий елемент в військовій термінології), оточене та захищене чотирма іншими. Другим колом представлені системо утворюючі, життєво важливі для держави противника елементи: стратегічні підприємства, електростанції, нафтопереробні заводи, сховища стратегічних ресурсів, установи банківської сфери тощо. Державна інфраструктура: транспорт, системи передачі та розподілу електроенергії, інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи тощо утворювали третє коло. Четверте коло відображало різні соціальні системи, які представляли населення держави противника. Останнім, п’ятим, колом були збройні сили та інші силові структури держави противника.

Згідно поглядів розробників: “На стратегічному рівні ми досягнемо мети, викликаючи зміни в одній та більше частинах фізичної системи противника таким чином, щоб противник був вимушений адаптуватись до нашої мети, або, взагалі, не зміг продовжувати опір. Ми назвемо це стратегічним паралічем. Які елементи різних систем противника ми будемо атакувати (з застосуванням різних видів зброї: від звичайної до комп’ютерних

вірусів) буде залежати від того, чого ми хочемо досягти, скільки часу ворог зможе протистояти нам, які він має можливості та які ми можемо прикласти фізичні, моральні та політичні зусилля".

Дана концепція сьогодні застосовується в усіх, без виключення, воєнних конфліктах, як і в сьогоднішній гібридній війні.

Якщо проаналізувати систему різнорідних дій, характерних для гібридної війни, то в ній чільне місце займають інформаційні дії. Це обумовлено стрімким розвитком інформаційних технологій, що в свою чергу, дало змогу створити глобальний інформаційний простір, в якому вже можна дистанційно впливати на політичну, економічну, соціальну, воєнну та решту сфер національної безпеки держави противника.

Зміщення акценту міждержавного протиборства в сторону інформаційних воєн висуває вимоги до формування відповідних сил та засобів.

Хочу акцентувати увагу на тому, що Україна ще з середини 90-х років XX сторіччя мала відповідні наукові напрацювання з питань створення системи інформаційної боротьби.

Так, до сих пір актуальними залишаються наші, з першим заступником Міністра оборони України Іваном Степановичем Руснаком, дослідження з зазначеного питання, які були викладені в статті (в журналі "Наука і оборона") ще в 2000му році.

Аналіз цих пропозицій свідчить про їхню повну відповідність умовам сьогодення та досвіду провідних країн світу. Так, централізація управління інформаційними заходами відповідає принципам стратегічних комунікацій, акцентування уваги (ще тоді) на важливості комп'ютерної безпеки сьогодні знайшло відображення в Стратегії кібербезпеки України, сьогодні розвиваються Сили спеціальних операцій Збройних Сил України, які відповідають за підготовку та проведення психологічних операцій, створені органи управління інформаційними операціями.

Основною тенденцією сьогодення є інтегрування всіх сил та засобів боротьби в інформаційному просторі в єдиному командуванні. Такий шлях вже обрали Німеччина, заявивши про створення єдиного командування інформаційного і кіберпростору та наш сьогоднішній противник – Російська Федерація, яка в лютому цього року оголосила про створення військ інформаційних операцій, включивши до їх складу (за досвідом проведених у 2016 році військових навчань "Кавказ – 2016") кіберкомандування збройних сил , військові частини радіоелектронної боротьби, центри інформаційного протиборства округів, а також, служби захисту інформації збройних сил.

Очевидно, що ми маємо враховувати цю тенденцію, шляхом підготовки до оборони України та застосування Збройних Сил України в умовах комплексного інформаційного впливу з боку противника.

Ткаченко А.Л.
Пилипчук Ю.В.
Троцько Л.Г.

# ІНФОРМАЦІЙНИЙ ВПЛИВ ТА ЙОГО СКЛАДОВІ

З початком гібридної війни проти України Російська Федерація значним чином посилила інформаційний вплив на аудиторію України та західних країн. Основними характерними рисами такого впливу на населення України стало розповсюдження ідеї “русского мира” серед російськомовного населення. При цьому інформаційний вплив містить три складові.

Перша складова. Пропагандистська. Вона спрямована на ту частину населення, яка частково або повністю не сприймає ідею розвитку України як самостійної держави. До цієї складової входять інформаційні повідомлення, що носить форму неприкритої дезінформації. При такому розкладі російську сторону абсолютно не турбує достовірність інформації, оскільки підтримка впевненості в діях РФ на території України серед такого роду аудиторії досить висока, інша точка зору,практично, не сприймається цією категорією населення. Інформація такого роду, переважно, розповсюджується на окупованій території Автономної Республіки Крим, та на окупованих територіях Донецької та Луганської областей.

Друга складова. “Інформаційно-просвітницька”. Вона розрахована на ширшу аудиторію, і полягає у викриванні дій “незаконної” української влади проти власного народу. У формуванні і розповсюдженні такої інформації приймають участь частина українських засобів масової інформації, що певним чином, контролюються проросійськими політичними силами на території України.

Третя складова. Інтернет-ресурси – розраховані на українську аудиторію. Особливо активно вони були задіяні на початковому етапі гібридної війни. Так, званий інтернет-тролінг був організований з метою впливу на активних користувачів інтернету в Україні.

Спроби агітації та розповсюдження інформації шляхом поширення чуток великого успіху не мали, ні на початковому етапі гібридної війни, ні сьогодні.

Всі зазначені складові продовжують активно використовуватися Російською Федерацією в гібридній війні проти України.

Вплив на аудиторію за кордоном характеризувався посиленням інформаційних ресурсів, таких як телебачення та радіо. Суттєво зросла пропаганда російських інформаційних каналів іноземною мовою. Лібералізм і свобода інформаційного простору значним чином сприяють розповсюдженню російської пропаганди за кордоном, на яку Україна фактично не може дати адекватну відповідь. Становище стало настільки серйозним для ряду західних країн, що вони мали вдатися до контрзаходів і створення пропагандистських ресурсів, що виконують завдання виявлення і викриття потоків неправдивих повідомлень, що здійснюють російські інформаційні канали.

Основний пропагандистський меседж Кремля в гібридній війні стосується розмежування “братнього українського народу” та “київської влади, яка перебуває під зовнішнім управлінням”. На Україну покладається провина за невиконання Мінських домовленостей. Окупований Крим позиціонується як “історично російський регіон”, “повернення” якого відбулося відповідно до норм міжнародного права.

США російські пропагандисти, зазвичай, звинувачують у агресивній політиці, подвійних стандартах та втручанні у внутрішні справи “третіх країн”. Європейців ця пропаганда позиціонує як “політичних заручників” власних урядів, які “визначили лояльність до Вашингтона вищою за власні національні інтереси”.

Стійкими тенденціями інформаційного впливу РФ на Україну в гібридній війні залишаються:

підтримання функціонування пропагандистських каналів за кордоном, і формування потоків неправдивих повідомлень про Україну та її владу;

подальший розвиток сучасних способів впливу на аудиторію за допомогою Інтернету, що включає активне використання соціальних мереж з одночасним обмеженням можливості всесвітньої мережі на власну аудиторію. Україна значною мірою узалежнена від Рунету та його інформаційних ресурсів. За оцінками експертів, щонайменше 50% усіх міжнародних зв’язків України зі всесвітньою мережею припадають на РФ. А завдяки популярності ресурсів “ВКонтакте”, Yandex та “Одноклассников” серед наших співвітчизників 55–60% Інтернет-трафіка йде з країни-агресора. За даними Gemius, у січні 2016 р. у ТОП-10 найпопулярніших серед українців сайтів чотири були “родом” із РФ: vk.com і mail.ru (2- ге і 3- тє місця – відразу після google.com), yandex.ru та ok.ru (5-т е і 9-те місця).

В умовах гібридної війни з РФ подолання Рунет-залежності є нагальним імперативом української інформаційної політики, і вимагає відповідних заходів владних структур, незалежних інтернет-організацій та кожного громадянина зокрема.

Толочко О.А.

## БЛОКУВАННЯ ДЕСТРУКТИВНОГО ВПЛИВУ СЕПАРАТИСТСЬКОЇ ТА РОСІЙСЬКОЇ ІНФОРМАЦІЙНОЇ ПРОПАГАНДИ В ЗОНІ ПРОВЕДЕННЯ АТО - ОДНА З ПРІОРИТЕТНИХ ЗАДАЧ

Сучасні події на сході України називають “гібридною війною” з боку Росії. Інформаційна складова є чи не найвагомішою у мережево-центричній війні, яку Російська Федерація веде проти України на Донбасі. Саме російські ЗМІ створюють паралельну реальність, у який занурена значна частина мешканців охопленої збройним протистоянням території.

Ця форма війни Росії проти нашої держави є якісно новим підходом ведення воєнних кампаній, ключовим моментом яких є психологічний та інформаційний вплив на місцеве населення Донбасу, що дає змогу на

сучасному етапі Росії проводити активну пропаганду на Сході України. Інформаційний вплив містить спотворення фактів або нав'язує аудиторії емоційне сприйняття, вигідне стороні країни-агресора.

Як правило, методом інформаційної пропаганди є дезінформація, або подання інформації у вигідному для себе ключі. Дані методи дозволяють спотворювати оцінку того, що відбувається, деморалізувати громадян, і в перспективі, забезпечити перехід на сторону інформаційного агресора.

В даній інформаційній пропаганді ударними угрупованнями Російської Федерації є: Перший канал, РТР, НТВ, РенТВ, "Росія-24" та ТК "Звезда". Вони вміло використовують вже давно відпрацьовані методи інформаційного впливу за наданими зверху темниками. Канал транслює загибель і нещастя місцевого мирного населення, успіхи "ополчення Донецької та Луганської народних республік", слабку підготовку і оснащеність, деморалізацію українських силовиків і звірства націоналістів. Їх мета – щоб громадська думка була на російській стороні. Цим вони нав'язують громадськості уявлення, що "Росія – країна-миротворець, "братня країна" й проти війни". У своїх випусках новин, висвітлюючи події на Донбасі, російські журналісти використовували кадри вбивств людей під час каральної операції на Північному Кавказі; бомбардування фосфорними боєприпасами противників режиму Башира Асада у Сирії, видаючи свої "сенсації" за дії Збройних Сил України на Донбасі. Ці інформаційні вкиди одразу спростовувалися в українських медіа, з наведенням фактів.

Постійна трансляція відверто неправдивої інформації, повний контроль усіх альтернативних медіа-ресурсів, джерел інформації, "залучення" широкої мережі агентів впливу в інших країнах світу проводиться Росією з метою, аби всі побачили "обличчя українця-ворога" таким, яким воно буде вигідним авторитарній країні.

В ефірі тимчасово окупованих територій Донецької та Луганської областей у переважній більшості відсутні українські телеканали. За словами мешканців окупованої Макіївки, на звичайну телеантену приймаються 16 телеканалів, 2 з яких ("1+1", й "5-й канал") – українські, з перебоями у мовленні, 4 сепаратистських (з особливо агресивною пропагандою) й 10 – російські.

На частотах українських телеканалів відбувається трансляція російських: ОРТ, НТВ, РТР, Росія-24. Також з ефіру зникли регіональні мовники. Тільки абоненти деяких операторів кабельного телебачення та Інтернет-ТВ IPTV можуть дивитись українське телебачення майже без обмежень. Проте не роблять цього з-за побоювання, що на них донесуть терористам.

Так, війна Росії проти України є інформаційною пропагандою, де головною мішенню виступає розум та політична свідомість українців. За допомогою психологічно-інформаційної зброї ворог зумів атакувати свідомість російськомовних луганчан і донеччан, скоригувавши їх морально-психологічний стан, політичну психологію та соціально-політичну поведінку у необхідному для кремлівських маніпуляторів напрямку. Головною метою російської пропагандистської машини – нав'язати світовій громадськості

думку, начебто Росія є сильною державою, спотворено видати інформацію про події на сході України, залякати своїх опонентів.

На даний час Росія продовжує реалізовувати свої плани у формі продовження "гібридної війни", посилюючи інформаційну складову. Серед засобів здійснення впливу, якими керується Російська Федерація, активно використовуються друковані засоби, книговидання, телебачення, радіо.

Дивлячись на легкість, з якою країна-агресор заволоділа медійним ресурсом України, можна говорити про недостатній рівень складової інформаційної безпеки на технологічному рівні, адже в країні вже понад три роки триває антитерористична операція на території окремих районів Донецької та Луганської областей.

Секретар Ради національної безпеки і оборони України Олександр Турчинов під час засідання Національного координаційного центру кібербезпеки наголосив: «Інформаційна агресія - одна з найнебезпечніших складових гібридної війни, яку веде проти нас Росія. Тому блокування деструктивного впливу сепаратистської та російської інформаційної пропаганди в зоні проведення АТО - одна з наших пріоритетних задач».

За його словами, керівництво Державної служби спеціального зв'язку та захисту інформації доповіло про детально розроблений проект інформаційного захисту, «який дозволить заблокувати антиукраїнське телерадіомовлення вздовж лінії розмежування в зоні проведення АТО».

Зважаючи на невідкладність реалізації цього завдання, Секретар РНБО України звернувся до Прем'єр-міністра України Володимира Гройсмана з пропозицією виділити з резервного фонду Уряду фінансові ресурси, необхідні для реалізації проекту.

«Запропоноване Державною службою спеціального зв'язку та захисту інформації обладнання - українського виробництва, воно ефективно вирішує покладені на нього завдання та на порядок дешевше за іноземні аналоги», - відзначив О. Турчинов.

Підсумовуючи, зазначимо, що подолання інформаційної ворожої пропаганди може бути успішним для України лише за умови коли всі її інформаційні засоби займатимуть активну патріотичну позицію, та будуть готові до протистояння на інформаційній лінії фронту.

канд. педаг. наук Трембовецький О. Г.
канд. психолог. наук Лазоренко О. В.

## ПРОТИДІЯ ОСНОВНИМ ГЛОБАЛЬНИМ ЗАГРОЗАМ У ПРИКОРДОННОМУ ПРОСТОРІ

Радикальні зміни міжнародної обстановки, які відбуваються сьогодні, значно впливають на погляди щодо характеру загроз безпеці у прикордонному просторі, шляхів їх своєчасного виявлення, запобігання та нейтралізації. Тому є актуальними виявлення, формулювання та систематизація проблем, що виникли на цей час, загострилися та мають перспективу розвитку у сфері

прикордонної безпеки. Їх розгляд доцільно проводити через призму визначення значення системи охорони державного кордону у загальній системі протидії загрозам у прикордонному просторі в умовах швидкоплинних змін в міжнародному та загальносвітовому безпекових середовищах.

Спектр основних можливих загроз національній безпеці України розкрито в Законі України «Про основи національної безпеки України», Воєнній доктрині та Стратегії національної безпеки України. Проте на сьогодні окремі їх положення потребують уточнення та конкретизації з урахуванням їх існування у прикордонному просторі.

Нацбезпека є складною системою, де тільки люди здатні вибирати способи, прийоми та методи діяльності, які захищають від загроз або націлені на їх знешкодження, ґрунтуючись на аналізі можливості зміни характеру та змісту умов зниження безпеки. У прикордонному просторі, як і загалом, безпека і небезпека існує в умовах взаємодії суб'єктів і об'єктів та середовища їх існування.

Як вказують фахівці, незалежно від того, про кордон якої держави іде мова, можна відокремити загальні особливості нацбезпеки у прикордонному просторі:

сучасні загрози перетинають державні кордони. Вони взаємопов'язані між собою та повинні усуватись на глобальному, регіональному та національному рівнях;

жодна держава, якою б сильною вона не була, не може самостійно убезпечити себе від сучасних загроз;

охорона кордону – це частина безпеки, тому кожна держава повинна визначити її місце і роль як в системі національної, так і регіональної безпеки;

національна та відомча стратегії розвитку є тими основними елементами, які сприяють створенню обґрунтованої, всебічної системи охорони кордону та планомірно її розвивають;

без детального нормативно-правового оформлення успішна охорона кордону не можлива;

в охороні кордону може приймати участь одна або декілька організацій, координацію діяльності яких повинна здійснювати структура з охорони кордону;

для успішного функціонування системи охорони кордону необхідна наявність спеціалізованої системи навчання та підготовки кадрів;

інфраструктура та технічні засоби повинні забезпечити виконання завдань прикордонного відомства;

фінансування повинно здійснюватись державою планомірно та цілеспрямовано.

Сьогодні як ніколи раніше стає очевидним, що жодна держава не може спиратись тільки на свої сили при вирішенні питань національної безпеки. Виходячи з цього, сучасні небезпеки, або загрози, повинні усуватись на глобальному, регіональному, локальному та національному рівнях. Для протидії цим загрозам необхідно створити дієвий механізм на кожному із рівнів безпеки. Отже, кожному рівню загроз повинен протистояти відповідний рівень

безпеки. Загрози вищестоящих рівнів повинні знайти своє вирішення на всіх рівнях, що стоять нижче.

Сьогодні в умовах глобалізації раніше існуючі загрози погіршилися та набули нових рис та якостей, ставши транскордонними та транснаціональними. В першу чергу до них слід віднести: міжнародний тероризм; зростання транскордонної злочинності; розповсюдження наркотичних засобів; нелегальна міграція; порушення прав людини; розповсюдження зброї масового знищення; інформаційний вплив; бідність; хвороби; конфлікти та ін.

Вирішення проблем безпеки ускладнює той факт, що більшість загроз переплітаються та взаємно доповнюють одна одну. Наприклад, тероризм взаємопов'язаний з незаконним обігом зброї та наркотиків, конфлікти та бідність – з нелегальною міграцією тощо. Для протидії цим сучасним глобальним проблемам необхідні, понад усе, скоординовані зусилля світового співтовариства, взаємодопомога, підтримка та своєчасний аналіз ризиків.

Глобальні загрози прикордонній безпеці не тільки здійснюють негативний вплив на прикордонний простір, але і шкодять національній безпеці, підривають суверенітет і авторитет держави. Тому протидія визначеним загрозам є пріоритетним завданням прикордонного відомства.

Зрозуміло, що самотужки Держприкордонслужба не в змозі протидіяти виявленим загрозам. Тому охорона державного кордону здійснюється шляхом впровадження певного комплексу заходів: політичних; організаційно-правових; дипломатичних; економічних; оборонних; прикордонних; міграційних; митних; природоохоронних; санітарно-епідеміологічних та інших заходів.

Як свідчить практика, ці заходи пов'язані між собою та створюють систему прикордонної безпеки держави і визначають систему охорони кордону. Однак основні завдання виконує прикордонне відомство. Таким чином, система охорони кодону – основна підсистема, базовий елемент національної та регіональної прикордонної безпеки.

Забезпечення захисту України від загроз є одним із пріоритетних напрямів діяльності держави, що законодавчо визначено та закріплено у відповідних актах. Проведене дослідження підтверджує, що охорону державного кордону необхідно розглядати як комплексну систему, яка вимагає багатостороннього підходу та системного мислення. Відповідальність за охорону кордону лежить не лише на плечах прикордонників, а і на представниках компетентних державних органів, політиках, співробітниках інших правоохоронних, контрольних та силових органів, представниках міністерств, органів місцевого самоврядування та членів громадських організацій.

Туранський М.О.

# ЗАСТОСУВАННЯ РОСІЙСЬКОЮ ФЕДЕРАЦІЄЮ ОРГАНІВ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ В ПИТАННІ АНЕКСІЇ КРИМУ

Війни та збройні конфлікти сучасності дедалі більшою мірою доводять значну роль та вагу інформаційно-психологічного фактора, враховуючи всю його багатогранність. Останні події в Україні також підкреслюють значимість інформаційного фактора у збройному протистоянні протиборчих сторін.

Російська Федерація довгі роки продовжувала та продовжує активно застосовувати до нашої держави концепцію «гібридної війни», невід'ємною складовою якої є цілеспрямований систематичний негативний інформаційно-психологічний вплив.

Анексії Російською Федерацією Автономної Республіки Крим, також передували тривалі та масштабні заходи інформаційно-психологічного характеру.

Все це підкреслює нагальну необхідність дослідження російської концепції «гібридної війни», з метою збору, узагальнення, всебічного аналізу та виокремлення найбільш дієвих напрямів протидії планам противника.

Ізраїльське «цифрове» комунікаційне агентство «Nether Ocean», що спеціалізується на рекламі, маркетингу і консалтингу в Інтернеті на своєму сайті опублікувало доповідь «Armies Online», в якому аналізувався процес формування за допомогою соціальних мереж і ЗМІ позитивного іміджу Армії оборони Ізраїлю і Російської армії. Хто виступив замовником подібного дослідження, автори доповіді не повідомили, однак, відомо, що саме Ізраїль в конфлікті Росії і України, в тому числі в коментарях з питання приєднання Криму до РФ, зайняв нейтральну позицію.

Окрему главу вищезазначеної доповіді було присвячено аналізу змісту «Кримської гібридної війни» (КГВ), в якій стверджувалось, що, «застосовуючи досвід Ізраїлю, Росія використовувала правильні медійні канали під час кримської операції». Ізраїльські дослідники «як дуже позитивний момент в КГВ наводило формування в Twitter аккаунта @vezhlivo «Ввічливі люди». (Цей термін ввів в обіг міністр оборони РФ Сергій Шойгу, коли коментував діяльність військовослужбовців РФ на півострові навесні 2014 року). У свою чергу експерти «Nether Ocean» відзначали як знакову появу такого сайту. На їхню думку, він «вирішував важливе завдання» а саме: спростовував ту пропаганду, яку вела українська сторона про дії «самооборони» в Криму.

За висновками авторів доповіді, в цілому інформаційну кампанію в соцмережах було проведено з величезним успіхом: більше 1,7 млн. твітів з підтримкою від 125 тис. акаунтів з Росії, південно-східних регіонів України, Білорусії і Казахстану (дані твіти були розміщені між 28 лютого і 1 квітня 2014 року). Кульмінацією кампанії стало проведення референдуму, на якому понад 90% жителів Криму висловилися за возз'єднання з РФ (фотографії та пости з підтримкою розлетілися по соцмережах). 125 тис. користувачів, які «активно

підтримували дії російських військ в Криму», автори доповіді вважають «абсолютним рекордом». Вони відзначають, що - для порівняння - «блог, спеціально створений для того, щоб об'єднати людей в розпал масових протестів в Москві в грудні 2011 року, на даний момент налічує трохи більше 46 тис. користувачів, з яких лише 4 тис. активні і схожі на реальні акаунти».

Також, за словами експертів «Nether Ocean», в блогосфері, яка, головним чином, була орієнтована на Крим та південний схід України, було досягнуто своєї мети, в тому числі і популяризацією «патріотичних і консервативних блогів, в яких легалізовано помірний націоналізм». Відзначалось, що «постмодерністський правоконсервативний популярний блог «Спутник и Погром» зміг не тільки привернути увагу 27 тис. користувачів Twitter і 85 тис. користувачів «ВКонтакте», але також і ввести систему платної підписки на свої матеріали». Абсолютним лідером, на думку ізраїльських експертів, було паблік «Армия - сила», що нараховував понад 400 тис. користувачів.

Іншою складовою проведення ІПСО в Криму стала російська експансія медіа-сфери півострова. Так, основними її напрямками стали введення нових правил, за якими повинні були працювати місцеві редакції та великі фінансові вливаннями з коштів російських платників податків. Процес розподілу цих коштів безпосередньо визначав і порядок роботи для кримських ЗМІ. Саме тому, що більшість з них вели і продовжують вести активну інформаційну війну проти України. За наявною інформацією особливостями подання інформації стало наповнення контенту кримських телеканалів, газет і інтернет-видань з одного боку, повідомленнями про «бандерівців» і «київську хунту», а з іншого - про успішне життя півострова в російських реаліях, де порушення прав людини - це вигадки «агентів Держдепу» та інших ворогів Росії. Варто відзначити, що також простежуються заборона щодо публікації в кримських ЗМІ інформації щодо масових обшуків в будинках кримчан (журналістів, активістів та інших громадян) протягом 2015-2016 рр.

Так, за висновками російського фонду «Медіастандарт» Комітету громадянських ініціатив, Крим є одним з регіонів з найнижчим рівнем критичності по відношенню до органів місцевої влади. За наявною інформацією, рівень фінансування кримських ЗМІ можна прирівняти до фінансування федеральних телеканалів і інформаційних агентств (їх бюджети оцінюються в мільярди рублів).

Найбільший обсяг фінансування в системі бюджетних асигнувань та грантів, передбачених для кримських ЗМІ, займає автономна некомерційна організація «ТРК «Крим»- колишня ДТРК «Крим», яка однією з перших була захоплена проросійськими силами на початку «Кримської весни».

У 2015 році загальний обсяг субсидій телеканалу за статтею «фінансове забезпечення витрат на створення і радіомовлення радіоканалів в Криму» склав 307,2 млн. російських рублів. Всі кошти використані до копійки.

За 2016 рік діяльність ТРК «Крим» обійшлася в 387 млн. рублів.

Слід зазначити, що бюджет «телевізійного російського фронту» в Криму за останній рік значно збільшений. Відразу ж після подій «Кримської весни» в 2014 році на фінансову підтримку виробництва і трансляції «республіканських»

інформаційно-аналітичних радіо-телевізійних програм і відеоматеріалів було витрачено всього 21,3 млн. рублів.

Протягом 2015 року збільшено фінансування друкованих ЗМІ Криму. Офіційне видання підконтрольної РФ Ради міністрів «Кримська газета» в 2015 році отримало в загальному 29,2 млн. рублів, а в 2016 році на її потреби витрачено вже 73 млн. рублів.

Бюджет «Кримського інформаційного агентства» (КІА) в 2016 році склав 5 млн. рублів. У порівнянні з 2014 роком, витрати на агентство збільшилися в п'ять разів.

На урядове видання «Кримські вісті» в 2016 році було виділено 73,2 млн. рублів. Згідно зі звітом, ці бюджетні дотації надані редакціям в рамках державної російської програми «Інформаційне суспільство» (підпрограма «Розвиток ЗМІ, видавництв і друкарень Криму, привернення уваги суспільства до культурних, історичних і сучасних інформаційних подій і досягнень Криму»).

Варто зауважити, що у 2014 році бюджетні витрати на провладні ЗМІ були набагато скромніші. Так, забезпечення діяльності офіційного видання кримського парламенту «Кримські вісті» обійшлося в 2,2 млн. рублів, «Кримської газети» - в 1,2 млн. рублів, журнал «Берега Тавриди» - 76 тис. рублів.

З метою здійснення інформаційного впливу на населення також активно залучають відомих кримських журналістів. Співробітники провладних ЗМІ отримують зарплату в 35-45 тисяч рублів.

Ще один рядок бюджету - субсидії державному унітарному підприємству Криму «Кримтехнології» на «створення і розвиток державних інформаційних ресурсів, спрямованих на задоволення інформаційних потреб громадян та організацій». У 2016 році на ці цілі було витрачено майже 19 млн. рублів. Ще 164 млн. рублів підприємство отримало для створення внутрішньовідомчих інформаційних систем виконавчих органів влади Криму і 342 млн. рублів - на створення державної інформаційної системи «Центр обробки даних Криму». Підприємство «Кримтехнології» в червні 2014 року заснувало Міністерство внутрішньої політики, інформації та зв'язку Криму, яке стало творцем пропагандистського сайту «Кримська весна».

Таким чином, можна стверджувати, що задовго до анексії Криму діяльність органів ІПСО Російської Федерації була підпорядкована завданням роботи на Крим та Україну в цілому.

Використовуючи ЗМІ та соцмережі, Російською Федерацією проведено довгострокову широкомасштабну ІПСО з інформаційного завоювання кримської аудиторії як до, так і після анексії Криму в тому числі шляхом поширення великого масиву інформації (як напівправдивої, так і недостовірної) з метою формування у кримчан стану захисної агресії (як наслідок цілеспрямованого залякування) по відношенню до новоутвореної влади з подальшим навіюванням думки про необхідність допомоги з боку Російської Федерації, у тому числі шляхом приєднання Криму до неї.

Російська Федерація, після анексії Автономної Республіки Крим, в контексті продовження власної інформаційної кампанії проти України, продовжує за рахунок значного збільшення щорічного фінансування ЗМІ Криму поширювати фейкові повідомлення про події в Україні, а також, інтерпретувати події в Україні у вигідному для себе контексті, головною метою є нав'язування українському суспільству бажаних для російської сторони думок та рішень у життєво важливих сферах державної і громадської діяльності та послаблення довіри до української влади з боку населення, а також маніпулювання громадською думкою. Систематичний аналіз ІПСО, що проводились і ведіться зараз Російською Федерацією є вкрай актуальним і необхідним задля забезпечення протидії цим операціям з боку українських силових структур та інших органів влади.

Фомін В.В.
канд. техн. наук Крайнов В.О.

## ОБҐРУНТУВАННЯ РЕКОМЕНДАЦІЙ ЩОДО ВВЕДЕННЯ ПРОТИВНИКА В ОМАНУ ТА ЗАБЕЗПЕЧЕННЯ СКРИТНОСТІ ДІЙ ВЛАСНИХ ВІЙСЬК (СИЛ) В АНТИТЕРОРИСТИЧНІЙ ОПЕРАЦІЇ

Основні події на півдні та сході України продемонстрували зростання вимог до ведення збройної боротьби в умовах підвищення можливостей технічних засобів розвідки противника, точності вогневого ураження за рахунок застосування противником високоточної зброї (ВТЗ), розвитку інформаційної зброї. В цих умовах особливого значення набуває проблема підвищення живучості військ. Одним з основних засобів вирішення цієї проблеми є проведення комплексу заходів введення противника в оману.

Введення противника в оману досягається проведенням комплексу заходів щодо нав'язування йому хибного уявлення про склад, положення підрозділів і об'єктів, які не відповідають дійсним. Способи введення противника в оману залежать від обстановки, яка склалася, бойового завдання, яке було поставлено, ступеня готовності підрозділів до рішучих і нешаблонних дій в умовах суворого маскування, а також від стану погоди, пори року і часу доби. Обманні дії повинні бути простими за замислом і виконанням, організовуватися приховано, проводитися переконливо і своєчасно.

Головною вимогою проведення заходів з введення противника в оману для найбільш повного досягнення цілей дезінформації є їх комплексність і не тільки у воєнній, але й в політичній й економічній сферах як на стратегічному так і на оперативно-тактичному рівнях. Завдання щодо їх проведення повинні виконуватись військово-політичним керівництвом країни, збройними силами та ІВФ, відповідними відомствами.

В проведенні заходів з введення противника в оману підвищується роль структур інформаційно-психологічної і кібернетичної боротьби на усіх рівнях, і в першу чергу на державному (стратегічному) рівні.

Головним змістом діяльності під час підготовки та ведення інформаційної

операції в частині, що стосується введення в оману, є ретельне узгодження всіх заходів (дій) з метою посилення взаємного ефекту та недопущення розкриття змісту і мети інших завдань (заходів) під час їх спільного виконання.

Таким чином результати дослідження можуть бути використані при розробці стандартизованих процедур планування заходів введення противника в оману, організації діяльності військ (сил) і засобів, які залучаються до їх проведення, налагодження між ними чіткої взаємодії, а також для оперативної оцінки ефективності роботи заходів введення противника в оману з метою вчасного і якісного їх корегування. Крім того, результати можуть бути використані в інтересах удосконалення навчального процесу у вищих військових навчальних закладах (за відповідною тематикою) та при проведенні наукових досліджень.

Шилов Р.Г.
канд. військ. наук Кацалап В.О.

## ОБҐРУНТУВАННЯ ПРОПОЗИЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІЙСЬКОВИХ ЧАСТИН АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ

Доповідь присвячена обґрунтуванню рекомендацій щодо забезпечення інформаційної безпеки військових частин антитерористичної операції.

В основу рекомендацій (тези) покладений досвід локальних збройних конфліктів сучасності, у тому числі проведення антитерористичної операції в Україні, аналізу концепцій інформаційних війн зарубіжних країн, змісту загроз національним інтересам України у воєнній сфері.

Проведений аналіз свідчить про таке:

Сучасним воєнним конфліктам притаманні такі риси, як підвищення ролі політичних, економічних, інформаційних засобів під час підготовки і в ході воєнного конфлікту; збільшення ролі інформаційно-психологічних операцій у досягненні цілей воєнних конфліктів; залежність політичного рішення щодо участі у воєнному конфлікті від суспільної думки на внутрішньому та міжнародному рівнях.

Однією з основних тенденцій розвитку воєнно-політичної обстановки у світі є прискорення розвитку інформаційних технологій, збільшення спроможностей держав щодо проведення інформаційних, інформаційно-технічного впливу (кібератак) та інформаційно-психологічних операцій, посилення чутливості суспільства до загибелі мирного населення та втрат особового складу військових формувань в антитерористичній операції.

В цих умовах визначальної ваги у воєнній сфері набуває завдання забезпечення власної інформаційної безпеки та кібербезпеки, під якою розуміється стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних

технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Вирішення цього завдання передбачає скоординовану діяльність різних структурних підрозділів Міністерства оборони України та Збройних Сил України.

Таким чином, забезпечення інформаційної безпеки, кібербезпеки військових частин антитерористичної операції є безумовно актуальне.

Проаналізувавши підходи різних країн світу до забезпечення власної інформаційної безпеки можна зробити висновок, що вирішити це завдання, поклавши всі відповідні функції на один, окремо визначений, орган неможливо. В той же час, координація всіх напрямів забезпечення інформаційної безпеки є обов'язковою.

В результаті аналізу ми бачимо необхідність застосування системного підходу до вирішення завдання забезпечення інформаційної безпеки. Його основними процедурами повинні бути: визначення в системі координуючого (щодо завдань забезпечення інформаційної безпеки) органу та різних підсистем; вироблення механізмів функціонування різних підсистем для забезпечення інформаційної безпеки; організація ресурсного забезпечення та підготовки кадрів.

Всю сукупність сучасних інформаційних загроз можна розділити на дві основні групи: інформаційно-психологічну, до якої відносяться загрози впливу на свідомість та психічний стан різних соціальних об'єктів, та інформаційно-технічну, до якої відносяться загрози втручання в роботу інформаційних систем, отримання доступу до конфіденційної інформації, стеження за окремими людьми в інформаційному (кібернетичному) просторі тощо.

Відповідно до визначених груп інформаційних загроз, будь-яка організація для забезпечення власної інформаційної безпеки повинна мати щонайменше дві підсистеми: підсистему інформаційно-психологічної безпеки та підсистему інформаційно-технічної (кібер) безпеки.

В структурі Генерального штабу Збройних Сил України завдання захисту особового складу від негативного інформаційно-психологічного впливу покладається на Головне управління по роботі з особовим складом, а завдання захисту інформації, забезпечення засекреченого, шифрованого і кодованого зв'язку, кібербезпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем військового призначення діляться між Головним управлінням зв'язку та інформаційних систем та Центральним управлінням захисту інформації та криптології. В той же час, єдиний координуючий орган щодо забезпечення інформаційної безпеки відсутній, що значно ускладнює як планування, організацію та проведення практичних заходів, так і їх належне ресурсне забезпечення.

Проблема забезпечення інформаційної безпеки ще більш складно вирішується на рівні окремих військових частин Збройних Сил України. Це обумовлюється відсутністю у їх складі штатних органів, призначених для вирішення відповідних завдань, недосконалістю нормативної бази, відсутністю практичних механізмів реагування на інформаційні загрози та їх нейтралізацію.

Нехтування проблемами забезпечення інформаційної безпеки в сучасних умовах постійного ведення провідними країнами світу інформаційної боротьби і особливо її загострення під час антитерористичної операції для військової частини може означати порушення всіх, без виключення, показників управління, зниження рівня морально-психологічного стану особового складу, виведення з ладу командних пунктів, вузлів зв'язку, порушення функціонування стартових позицій, військової техніки та озброєння, систем передачі даних і захисту інформації тощо.

Отже, для забезпечення інформаційної безпеки військових частин антитерористичної операції необхідно проаналізувати і вирішити основні питання:

проаналізувати вплив інформаційних загроз на функціонування військових частин антитерористичної операції;

розробити методику забезпечення інформаційної безпеки військових частин антитерористичної операції і Збройних Сил України в цілому;

розробити пропозиції та рекомендації щодо забезпечення інформаційної безпеки військових частин антитерористичної операції.

Штифурак Ю.М.

## ВИЗНАЧЕННЯ РАЦІОНАЛЬНИХ ВХІДНИХ ВПЛИВІВ НА СТАН РЕГІОНУ ЗА МЕТОДИЧНИМ ПІДХОДОМ

У процесі аналітичної обробки інформації необхідно оцінити ситуації, що можуть виникати в майбутньому. Внаслідок цього використання аналітичних прогнозів дозволить своєчасно надавати споживачам розвідувальної інформації упереджувальні та прогнозні дані про регіон. При цьому регіон розглядається як складна система, аналізування та синтезування якої здійснюється на основі когнітивного підходу. В кінцевому випадку стане можливим визначення раціональних вхідних впливів на стан регіон за методичним підходом.

Актуальність запропонованого дослідження визначається сучасними конфліктними ситуаціями в світі, що динамічно розвиваються, необхідністю оцінювати стабільність держави (регіону) для правильного вибору політичного та зовнішньо-економічного курсу України. Вирішення цього завдання здійснюється, здебільшого, шляхом використання якісних оцінок стану регіону на основі досвіду, знань та інтуїції експертів-аналітиків у конкретній області. Один з перспективних підходів до аналізу слабкоструктурованих проблемних галузей, що сформувався останніми десятиріччями, називається аналізом когнітивних карт або когнітивним моделюванням. Він ґрунтується на понятті когнітивної карти, яка є моделлю уявлень і знань експертів про закони розвитку та властивості аналізованої ситуації (системи) у вигляді елементарних семантичних категорій, пов'язаних відношеннями.

Визначення раціональних вхідних впливів на стан регіону за методичним підходом є знаходження його аналітичного функціоналу. Для його знаходження використовується метод групового врахування аргументів.

До переваг методу групового врахування аргументів можна віднести наступі властивості:

1. Можна відновити невідому довільно складну залежність по обмеженій вибірці. Число невідомих параметрів моделі може бути більше, ніж число точок навчальної послідовності.

2. Можливість адаптації параметрів моделі при одержанні нових даних експериментів.

Для знаходження аналітичного функціоналу стану регіону використовується програмний засіб «SHELL». Також за допомогою цього засобу визначається коефіцієнт детермінації.

При подальшому знаходження раціональних векторів, із списку найбільш імовірних, можна легко виділити з них найбільш задовільні. Таке виділення здійснюється за допомогою запропонованого методичного підходу.

Раціональні оцінки вхідних параметрів для аналітичного функціоналу визначаються за допомогою використання евристичного алгоритму OPTQuest, який реалізований в програмному засобі AnyLogic.

Кожен із вхідних параметрів має обмеження. Їх необхідно задати в табульованому вигляді. Використавши евристичний алгоритм необхідно знайти раціональні оцінки вхідних параметрів при яких значення об’єкта буде максимальним (мінімальним). Крім цього потрібно задати, що необхідно знайти максимум (мінімум) цільової функції.

Таким чином, знайдено раціональні оцінки вхідних параметрів для аналітичного функціоналу за евристичним алгоритмом OPTQuest. Отримані при цьому результати узагальнено та візуалізовано. Це стало можливим шляхом встановлення обмежень на значення вхідних параметрів та знаходження раціонального значення аналітичного функціоналу. Отримані результати дозволили проаналізувати стан регіону та надати відповідні рекомендації.

У кінцевому випадку використання методичного підходу до знаходження раціональних вхідних параметрів допомагає зрозуміти аналітику на який рівень необхідно виводити значення сфер, щоб досягнути раціональне вихідне значення.

Таким чином, використання методичного підходу визначення раціональних вхідних впливів на регіон забезпечить інформаційно-аналітичну підтримку процесів прийняття рішень відповідними посадовими особами.

ДЛЯ НОТАТОК