МВС УКРАЇНИ
НАЦІОНАЛЬНА ПОЛІЦІЯ
ДЕРЖАВНА ПРИКОРДОННА СЛУЖБА УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ ІМЕНІ БОГДАНА ХМЕЛЬНИЦЬКОГО
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
ГРОМАДСЬКА РАДА МВС УКРАЇНИ
ЦЕНТР ЗАПОБІГАННЯ ТА ПРОТИДІЇ КОРУПЦІЇ


«ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ»

Міжнародна науково-практична конференція
(16-17 листопада 2017 року)

НАДПСУ
Хмельницький-2017

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ:

голова оргкомітету

Мартиненко Володимир Олександрович – радник міністра в Міністерстві внутрішніх справ України, член колегії Міністерства внутрішніх справ України, голова Громадської ради при Міністерстві внутрішніх справ України, голова в Центрі запобігання та протидії корупції;

заступник голови оргкомітету

Кириленко Володимир Анатолійович – заступник ректора (проректор) Національної академії Державної прикордонної служби України з наукової роботи, доктор військових наук, професор;

члени оргкомітету:

Шевченко Артем Валерійович – директор Департаменту комунікацій Міністерства внутрішніх справ України;

Чернявський Сергій Сергійович – проректор Національної академії внутрішніх справ, доктор юридичних наук, професор, заслужений діяч науки і техніки України;

Андреєв Дмитро Володимирович – директор навчально-наукового інституту № 3 Національної академії внутрішніх справ, доктор юридичних наук, доцент, заслужений журналіст України;

Захарчук Володимир Ілліч – помічник ректора Національної академії Державної прикордонної служби України – начальник прес-служби;

Андрощук Олена Юріївна – начальник науково-дослідного відділу Національної академії Державної прикордонної служби України, кандидат психологічних наук, старший науковий співробітник;

Ставицький Олег Миколайович – начальник кафедри прикордонної безпеки Національної академії Державної прикордонної служби України, доктор педагогічних наук, доцент;

Дем’янюк Юрій Анатолійович – професор кафедри прикордонної безпеки Національної академії Державної прикордонної служби України, кандидат педагогічних наук, доцент.

ВІТАЛЬНЕ СЛОВО РЕКТОРА

Шановні учасники конференції, гості та присутні!

Щиро вітаю Вас у стінах Національної академії Державної прикордонної служби України імені Богдана Хмельницького. Сьогодні нашому навчальному закладу випала честь приймати у себе провідних науковців, представників державної влади, мас-медіа, фахівців правоохоронних структур для проведення міжнародної науково-практичної конференції «**ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ**», організатором якої виступило Міністерство внутрішніх справ України.

Присутність високоповажних гостей, велика кількість учасників конференції є прямим доказом виняткової актуальності її проблематики.

Четвертий рік поспіль триває збройна агресія Росії проти України, яка призвела до анексії Криму, втрати контролю над понад 400 км державного кордону і частиною Донбасу, значних людських жертв.

У цій неоголошеній війні, яку ще називають гібридною, Україна втратила більше 10 тис. своїх громадян, з них близько 3000 – військовослужбовців – представників як військових, так і правоохоронних структур.

Вічна пам’ять героям! Прошу вшанувати хвилиною мовчання наших побратимів.

…Дякую!

Гібридна війна Росії проти України – це реальна загроза світовій системі. Сьогодні вона підриває регіональну стабільність в країнах від Балтійського до Чорного моря, створює виклик для НАТО як ключового елемента Європейської безпеки, ставить під сумнів подальшу долю всього Європейського проекту й ідеї об’єднаної Європи. Але найбільшого збитку від цієї війни зазнає наша держава, все українське суспільство. На порядку денному постали питання збереження територіальної цілісності України, її суверенітету, виживання нації

загалом. У цій війні відсутні звичні канони її ведення. Попри те, що територіально вона локалізована на Сході України, наслідки її впливу мають масштабний характер. Бо цей вплив, насамперед, пов'язаний з використанням інформаційно-психологічних методів для маніпуляції масовою свідомістю.

Саме необхідність протидії інформаційним елементам гібридної війни зумовлює потребу комплексного забезпечення інформаційної безпеки. З огляду на це, нагальної актуальності набувають питання, які будуть обговорені на нашій конференції, а саме:

особливості взаємодії відомчих медіа-структур із засобами масової інформації;

запровадження дієвих механізмів комунікацій з громадськістю в системі МВС;

кризові комунікації в умовах гібридної війни.

Вирішення означеної проблематики вимагає від нас виходу на нові рубежі координації діяльності правоохоронних органів та інших суб'єктів сектору безпеки та оборони України у сфері протидії інформаційним загрозам. Ми повинні визначити пріоритетні напрями розвитку стратегічних комунікацій як ключової умови забезпечення інформаційної безпеки.

Шановні учасники конференції! Користуючись нагодою, мені дуже приємно сьогодні презентувати Національну академію Державної прикордонної служби України, в якій створено сучасні умови для наукової діяльності та освітнього процесу.

Національна академія є постійним організатором всеукраїнських та міжнародних науково-практичних конференцій з широкого кола актуальних питань для теоретиків, практиків, слухачів, курсантів та студентів.

Щира подяка всім учасникам конференції, які приїхали до нашого закладу поділитися своїм баченням щодо вирішення запропонованих питань.

Впевнений, що конференція сприятиме активному обміну думками, досвідом щодо пріоритетних напрямів розвитку комунікацій в системі МВС, спрямованих на забезпечення інформаційної безпеки України в умовах гібридної війни.

Усіх учасників запрошую до плідного та конструктивного діалогу.

Бажаю життєвого оптимізму, енергії та натхнення в роботі!

З повагою
Ректор Національної академії
Державної прикордонної служби України
Імені Богдана Хмельницького
генерал-майор Шинкарук О.М.

ПЛЕНАРНЕ ЗАСІДАННЯ

МОДЕЛІ ІНФОРМАЦІЙНОГО ВПЛИВУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ПРОБЛЕМА ЕФЕКТИВНОСТІ

Н. В. Грицяк

доктор наук з державного управління, професор, заслужений діяч науки і техніки України
професор кафедри інформаційної політики та електронного урядування Національної академії державного управління при Президентові України

«Гібридна війна: вжити і перемогти» – книжку з такою назвою написав Євген Магда, політичний експерт, директор Центру суспільних відносин (презентація видання відбулась у квітні 2015 року).

«В умовах гібридної війни бойові дії є другорядними, а на перший план виходять інформаційні операції та інші важелі впливу. Війна полягає у прагненні однієї держави агресивно діяти на свідомість жителів іншої. Іншими словами – це прагнення не знищити мільйони людей, а залякати й деморалізувати їх. Завдяки швидкості поширення інформації світом вона перетворилася не лише на товар, а й на зброю».

П’ять ознак «гібридної війни»:

1. Гібридну війну не оголошують.
2. Гібридна війна планується під стратегію інформаційної війни.
3. Метою гібридної війни є створення хаосу, безперервного конфлікту, руйнування інфраструктури.
4. Використовуються постановочні воєнні дії для зомбі-ЗМІ.
5. Суть гібридної війни – ідентоцид – знищення національно-державної громадянської ідентичності країни-суперника.

Три моделі інформаційних операцій: американська; британська; російська.

Американська модель.

Ціль – зміна відношення / ставлення людини до певного об’єкта.

Засіб – комунікації (м’яка сила).

Американська модель узяла свою базу з реклами та паблік рилейшнз, задаючи в якості цілі зміну відношення до якогось об’єкту.

Наприклад, після 11 вересня 2011 року США вирішили вплинути на мусульманські країни, щоб змінити їх відношення до США з негативного на позитивне чи нейтральне. Для цього вони порівняли системи цінностей – мусульманські і американські, знайшовши серед п'яти перших цінностей лише одну спільноту – відношення до сім'ї та дітей. У результаті саме на цю тему почали створювати рекламні ролики про те, як добре живуть мусульманські сім'ї в Америці.

Британська модель.

Ціль: зміна поведінки людини (оскільки зміна відношення є недостатньою).

М'яка сила – це не лише комунікація.

Засіб – правове регулювання.

Британська модель закладає іншу базову точку відліку: не зміни відношення, а зміну поведінки людини, оскільки вони вважають зміну відношення недостатньою.

Наприклад, юнак в Афганістані може підкладати міни на дорогах проти англійських солдат, щоб зібрати гроші на навчання в Великобританії. Тобто він позитивно налаштований у бік цієї країни і одночасно може встановлювати міни проти її солдат. Вони також підкреслюють, що м'яка сила – це не лише сама комунікація.

Російська модель.

Отримала назву рефлексивної.

База – уявлення людини про світ.

Змінюючи уявлення, можна людину зробити менш/більш войовничою.

Засіб – маніпуляції зі свідомістю.

Набір інструментарію рефлексивної моделі: тиск силою; переформатування розуміння вихідної ситуації; формування цілей супротивника; формування алгоритму прийняття рішень; вплив на час прийняття рішення.

Впливаючи на процес прийняття рішень можна або стимулювати якісь рішення, або блокувати їх. Росіяни в Криму, наприклад, увівши так званих «ввічливих людей» блокували фізичну реакцію на них українських військових.

П'єр Бурдье: габітус, класовий етос, політичне поле

Соціологія, на думку Бурдье, є соціальною топологією. Ідею топології Бурдье узяв з фізики.

Люди як біологічні індивіди і соціальні агенти виступають елементом, що розміщуються у фізичному просторі, займаючи повне місце і об'єм.

Це місце можна визначити абсолютно: як ту просторову крапку, де в даний момент часу розташовується агент або предмет, де він локалізований. Відносне ж місце, займане агентом, можна визначити як позицію або ранг в соціальній ієрархії.

Габітус (Habitus)

Габітус – одне з головних понять соціологічного учіння Бурдье. Пьер Бурдье визначає габітус як «систему стійких і водночас рухомих диспозицій».

Диспозиції – це схильності сприймати, відчувати, діяти і мислити певним чином, найчастіше несвідомо засвоєні кожним індивідом унаслідок об'єктивних умов його існування. Ці диспозиції стійкі, рухомі і утворюють систему, оскільки прагнуть об'єднатися.

У габітусі втілені способи оцінювання і мислення, естетичний смак, манера поведінки і мови, характерний стиль і образ життя, гендерна ідентичність, які відрізняють представника одного класу, професії, національності від інших.

Здатність агентів спонтанно орієнтуватися в соціальному просторі і більш менш адекватно реагувати на події і ситуації, здатність, що складається в результаті величезної роботи освіти і виховання в процесі соціалізації, кристалізується у визначений, відповідний соціальним умовам становлення індивіда, тип габітуса.

Habitus – це спонтанність поза усвідомленістю або волею.

Ранній досвід має особливе значення, оскільки habitus має тенденцію до постійності і захищений від змін запереченням інформації, здатної поставити під сумнів вже накопичену інформацію.

Наприклад, емпірично підтверджений факт, що люди схильні говорити про політику з тими, хто дотримується аналогічних поглядів.

Habitus – це принцип вибіркового сприйняття індикаторів, направлених швидше на підтвердження і посилення habitus'а, ніж на його трансформацію.

Приклад: «лівий» і «правий» габітуси.

Перехід від інформаційних операцій до операцій впливу

Ще в перших розробках Авіаційного університету про війну 2025 р. вже йшлося не просто про інформаційну війну, а війну мудрості (wisdom warfare). Сьогодні звичним також стає підхід, що отримав назву війни знань (knowledge warfare).

Знання розглядаються як такі, що можна отримати з інформації або з інших знань. І інтервенцію в систему прийняття рішень супротивника слід робити саме на рівні знань, змінюючи його сприйняття світу.

З історії становлення

Т. Рона, який був науковим радником і Пентагону, і Білого дому, в 1976 році вперше визначив інформаційну війну як битву систем прийняття рішень.

Десь на десять років пізніше Р. Шафранські з Авіаційного університету писав, що ціллю інформаційної війни є епістемологія супротивника, тобто ті знання, які ворог розглядає як правдиві і правильні.

Інформаційні і смислові війни

Інформаційні і смислові війни, впливаючи на індивідуальну чи масову свідомість, мають когнітивний простір впливу тільки як проміжний. Всі вони намагаються впливати на поведінку людини. Сьогодні відкрилися нові можливості для інформаційних і смислових війн завдяки інтенсивному розвитку соціальних мереж, які і спростили вихід на інформацію, і знизили контроль держави над нею.

Смислові війни, як правило, базуються на просуванні чужих смислів.

Росія у випадку конфлікту з Україною утримувала не нові, а старі радянські смисли. Саме вони були активовані в російського населення. Тобто було активовано «радянський» габітус.

Доктрина інформаційної безпеки України

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України.

Стратегічні комунікації – 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.

Урядові комунікації – комплекс заходів, що передбачають діалог уповноважених представників Кабінету Міністрів України з цільовою аудиторією з метою роз'яснення урядової позиції та/або політики з певних проблемних питань.

Кризові комунікації – комплекс заходів, що реалізуються державними органами України у кризовій ситуації і передбачають їх діалог із цільовою аудиторією з питань, що стосуються кризової ситуації.

Стратегічний наратив – спеціально підготовлений текст, призначений для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію.

Пріоритети державної політики в інформаційній сфері щодо забезпечення інформаційної безпеки (серед інших):

побудова дієвої та ефективної системи стратегічних комунікацій;

розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України.

Висновки:

1. Указ Президента України №47/2017 від 25 лютого 2017 року «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»» є базовим документом для розробки ефективної комплексної моделі інформаційного впливу як інструменту інформаційної протидії в умовах гібридної війни.

2. Методологічною основою такої моделі мають стати функціональні основи стратегічних комунікацій, а саме:

номінативна (визначення сутності явищ/подій/понять, створення наративів);

комунікативна (розробка засобів, заходів та способів комунікації з метою поширення, роз'яснення, переконання, досягнення взаєморозуміння);

інституційна (нормативно-правове, ресурсне, кадрове, технічне забезпечення).

МЕХАНІЗМИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ ВЗАЄМОДІЇ ПРЕС-СЛУЖБ МВС З НОВІТНІМИ ЗМІ

Д. В. Андреєв

доктор юридичних наук, доцент,
заслужений журналіст України
директор навчально-наукового інституту № 3 Національної академії внутрішніх справ

Засоби масової інформації за своєю суттю так само суперечливі, як і сучасне розуміння ролі медіа. До теперішнього часу існує поширений стереотип: маючи в управлінні «власний» засіб масової інформації, з його допомогою орган влади може переконливо, а головне, «напряму» доводити громадськості свої меседжі. Однак сучасна реалія – аудиторія споживачів інформації навчилася досить чітко відрізняти «замовні матеріали» від суспільно значимих, тому ефект від таких втручань у діяльність новітніх засобів масової інформації прямо протилежний.

Водночас сучасний етап розвитку інформаційного суспільства супроводжується гіперрозвитком системи засобів масової інформації, які втрачають усталені традиції й, перетворюючись на інноваційні засоби конструювання соціального простору, формують вже нові моделі взаємної відповідальності держави та громадянина. І особлива місія взаємної відповідальності правоохоронних органів та ЗМІ лише підштовхує нас до активізації цього діалогу.

При обранні механізмів вдосконалення інформаційно-комунікаційної взаємодії пре-служб МВС, систему засобів масової інформації, незалежно від інформаційно-комунікаційних аспектів і сфери розповсюдження, потрібно розглядати в двох аспектах: як суб’єкт інформаційної діяльності та як суб’єкт господарювання. Також слід наголосити на дуалістичності природи мас-медіа, суть якої полягає в тому, що, з одного боку, засоби масової інформації є найважливішим соціально-політичним інститутом демократичного суспільства, який покликаний забезпечувати громадський контроль за діяльністю органів державної влади, сприяти формуванню громадської думки. З іншого – медіа формують окрему галузь економіки, функціонування і розвиток якої залежить як від власних фінансово-економічних інтересів власників новітніх ЗМІ.

КІБЕРБЕЗПЕКА У ГІБРИДНІЙ ВІЙНІ

В. М. Кулик
кандидат технічних наук, доцент
заступник директора філії Донецького національного університету імені Василя Стуса «ДонНУ-Поділля»
І. С. Катеринчук
доктор технічних наук, професор
професор кафедри Національної академії Державної прикордонної служби України імені Богдана Хмельницького
П. Д. Біленчук
кандидат юридичних наук, доцент
професор кафедри Київського університету права Національної академії наук України

Світовою спільнотою тероризм визнаний найгострішою проблемою сучасності, загрозою для функціонування всієї системи міжнародної безпеки. Сьогодні тероризм являє собою реальну загрозу будь-якій державі і рівень його суспільної небезпеки постійно зростає. Під впливом численних факторів в політичній, економічній, соціальній, релігійній сферах діяльності суспільства він постійно змінює свої форми, поступово набуває своїх крайніх проявів.

Уже більше 3-х років Україна веде активну фазу неоголошеної гібридної війни з Російською Федерацією. Ще з моменту анексії Криму (а за деякими даними – з часів Євромайдану) Росія використовувала кібератаки як складову своєї гібридної війни проти нашої держави. Різноманітні «кіберберкути» з не до кінця зрозумілою «пропискою» та складом, а також спеціальні підрозділи безпекових структур нашого супротивника здійснювали атаки на державні інформаційні ресурси та на персональні дані окремих політиків і громадських діячів. Найбільш відомі випадки таких дій – DDoS-атаки на урядові ресурси (МЗС, сайт президента України, сайти органів сектора безпеки і оборони), цільові атаки на держоргани за допомогою шахрайських електронних листів, спроби порушення роботи системи ЦВК під час виборів президента і на парламентських виборах 2014 року, а також функціонування вірусу Uroboros, який, із високою часткою ймовірності, ідентифіковано як російський. Він мав усі ознаки використання проти України кібершпигунської акції, а під дію вірусу потрапили веб-ресурси органів державної влади (зокрема силових структур), засобів масової інформації, фінансових установ, великих промислових підприємств. Тобто вже сьогодні маємо приклади використання агресором кіберпростору (телекомунікаційної складової) у деструктивних цілях проти України.

Проведений аналіз свідчить про те, що найбільш поширеною в Україні мотивацією скоєння терактів, у т.ч. кібератак, виступає: кримінальна діяльність,

особливо її транснаціональні форми; намагання перешкодити громадській, політичній або економічній діяльності; створення ускладнень або напруження у міждержавних відносинах. Відповідно, убезпеченість кіберпростору держави від атак, а також від використання його проти інтересів національної безпеки та оборони – одне з пріоритетних завдань для країни. Причому рішення мають бути віднайдені вже зараз, а увага держави до кіберпроблематики має перейти з площини теорії у практику.

Інший бік проблеми. У США станом на 2016 рік понад 80 % родин володіли власними ПЕОМ (для порівняння – в Індії менш 5 %, в Україні – налічується 21,6 млн. користувачів ПЕОМ та 64,7 % дорослого населення мають доступ до Інтернет, а у віці 15-29 років 97 %) [1]. У відповідності до цього існує запит та створена ціла індустрія по продажу особистих даних громадян, незважаючи на прийнятий закон про захист персональних даних, що передбачає покарання до 5 років ув'язнення за махінації з особистими даними [2]. Їх ринкова вартість від 500 до 50 тис. грн., так як коли є попит – буде і пропозиція.

Додаткова сфера комп'ютерних злочинів, що здійснюються через Internet, з'явилася з виникненням електронних банківських розрахунків, тобто з введенням в обіг так званої електронної готівки і електронного підпису.

На сьогодні накопичені значні напрацювання у галузі інформаційної безпеки. Проблематикою етимології поняття кібер, кіберпростору, «гібридної війни», національної безпеки, інформаційних атак у державних і недержавних структурах займалися провідні українські та світові вчені: І. Кочан, Є. Магда, Р. Грищук, В. Горбулін, В. Пядишев, П. Біленчук, О. Рибальський, М. Делягін, В. Кутирьов, Г. Мірською, І. Міхеєв, В. Хорос, В. Антипенко, В. Крутов, В. Ліпкан, У. Еко, А. Гловацькі, С. Хантінгтон, С. Хоффман та ін. На їх думку наразі найбільшу загрозу для всієї міжнародної спільноти становить саме кібертероризм. Це жахливе явище має два крила: кіберзлочинність та тероризм. Виходячи з цього проблема інформаційних загроз кіберпростору є наднаціональною. Свідченням цього є Декларація, що була прийнята на саміті НАТО в Уельсі у 2014 році (п.п. 72-73), згідно з якою «кібератаки можуть досягати такого рівня результатів, що загрожують євроатлантичному добробуту, безпеці і стабільності… Рішення про те, коли кібератаки потребують використати статтю 5, буде прийматися Північноатлантичною радою на індивідуальній основі. Іншими словами, кібербезпека вторглась у «свята святих» НАТО, статтю 5 про колективне використання військової сили у випадку нападу на одного із членів Альянсу.

Тому шляхи забезпечення захисту даних в інформаційно-обчислювальних та телекомунікаційних мережах, розробка стратегії комплексного аналізу стану національної телекомунікаційної мережі для забезпечення пропорційності та адекватності заходів кіберзахисту реальним та потенційним загрозам є на сьогодні надзвичайно актуальними.

Одним з основних наслідків інформатизації, що виник в період формування сучасної інформаційної епохи і становлення економіки знань, стало

виникнення та швидкий розвиток нової сфери конфронтації між державами – конфронтації в кіберпросторі. Якщо на сьогодні між найбільш розвиненими у військовому та економічному відношенні державами, у деякій мірі склався стратегічний паритет у зброї масового знищення та звичайному озброєнні, то питання про паритет у кіберпросторі залишається відкритим. І, як наслідок, для любої держави безпека в кіберпросторі (кібербезпека) стала найбільш гострою проблемою забезпечення національної безпеки.

Розглянемо основні аспекти кібервійни та кібербезпеки. Кібервійна – це військові дії, що здійснюються в електронному просторі в електронному вигляді. Зброя в кібервійні – це інформація, інструменти – комп'ютери, театр військових дій – Інтернет. Мережа Інтернет стає потужною зброєю, яка суттєво підсилюється технологіями штучного інтелекту. Кіберзброя являє собою широкий спектр технічних і програмних інструментів, які найбільш часто спрямовані саме на використанні вразливих місць в системах передачі даних. Механізм дії кіберзброї може бути абсолютно різним. Наприклад, вірусні програми можуть заважати іншим програмам різними способами: відміняти команди або задавати свої, видаляти всі дані або змінювати їх. Однак, у більшості випадків достатньо проникнути в чужу програму, для того щоб отримати необхідні дані. Інструментами кібератак є шкідливі програми і віруси, тому для того, щоб протистояти кібератакам, необхідно використовувати високоякісний захист, і, безумовно, залучати компетентних фахівців.

Досліджуваний вид бойових дій складається з двох етапів: шпіонажу та атак. Перший етап включає збір даних, шляхом злому комп'ютерних систем інших держав. Атаки можуть бути розділені у відповідності з цілями і задачами військових дій: вандалізм, пропаганда, збір інформації, порушення роботи комп'ютерного обладнання, атака інфраструктури і критичних об'єктів.

Завдання кібервійни полягає в досягненні певної мети в економічній, політичній, військовій та інших галузях. При цьому ставиться додаткове завдання щодо здійснення цілеспрямованого впливу на соціум і владу заздалегідь підготовленою інформацією. Тому кібервійна є ще психологічною та одним із видів інформаційної війни в кібернетичному просторі. Адже комп'ютерні технології та Інтернет використовуються в усьому світі не тільки у повсякденному житті людей, а й на підприємствах і державних установах. Маніпулювання даними, що отримуються із зазначених вище установ, створюють загрозу національній безпеці держави. Отже, кібербезпека є невід'ємною частиною захисту національної безпеки при даному протистоянні. Вона являє собою набір принципів, інструментів і стратегій для забезпечення невразливості та захисту кіберсередовища, а саме наявності цілісності і конфіденційності даних. У наш час загальноприйнята концепція, що роль інформаційної безпеки в системі національної безпеки суттєво зростає і є однією із її складових.

Мета кібервійни – порушення функціонування комп'ютерних систем, які відповідають за роботу ділових і фінансових центрів, державних установ, створення хаосу в житті держави. Тому в першу чергу страждають найбільш

життєво важливі і функціональні системи. До них відносяться системи водо- і енергозабезпечення, транспорту, комунікаційні мережі тощо. Відмітимо, що найбільша кількість атак в Україні у 2016-2017 роках в критичній інфраструктурі прийшлась на енергетичний сектор та урядові установи.

Таким чином, у зв'язку з глобальним розповсюдженням інформаційних технологій у всі сфери нашого життя, аналогічна підривна діяльність, якщо вона успішна, може нанести збитки, які можна порівняти з вибухом декількох атомних бомб. Це може деморалізувати і дезорганізувати противника, не застосовуючи при цьому звичайних озброєнь і жодного солдата.

Як показали проведені дослідження (рис. 1), більшу частину кіберзлочинів здійснюють так називаємі хактевісти (37 %). Це хакери, що здійснюють атаки на сайти урядів держав, сервери великих компаній, використовуючи при цьому таємні бази даних. На думку економістів збитки світової економіки від такої діяльності кіберзлочинців становить орієнтовно $114 млрд [3].

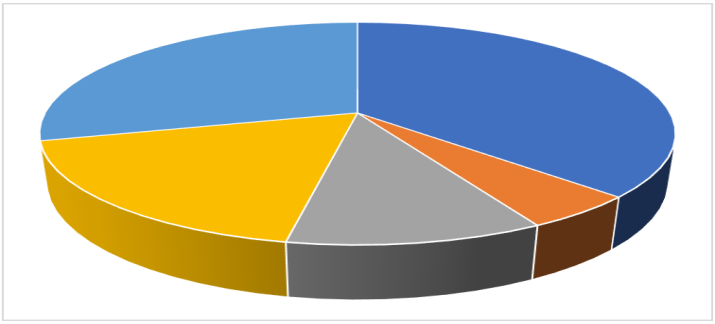

Рис. 1. Сегментація направленості кіберінцидентів у світі в 2016 році

Забезпечення безпеки критичної інфраструктури (Critical Infrastrurture Protection, CIP) являє собою концепцію готовності протистояти серйозним загрозам роботи важливих об'єктів інфраструктури та обєктів підвищеної загрози в регіоні чи державі, особливо в умовах розповсюдження інформаційних технологій.

Історично, першим кроком на цьому напрямі було створення в 1996 році Комісії по захисту життєво важливої інфраструктури при Президенті США: було поставлене завдання розробити всеохоплюючу національну стратегію по захисту інфраструктури від фізичних і кібернетичних загроз. Подібна директива видана в ЄС в 2008 році [4]. В Україні рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» введено Указом Президента 15 березня 2016 року [5]. Основні ж напрями державної політики по захисту критично важливих об'єктів інфраструктури прийняті Верховною Радою в Законі України від 5 жовтня 2017 року №2997-VIII «Про основні засади забезпечення кібербезпеки України». У цьому документі поставлена мета забезпечити безпеку об'єктів кібербезпеки та кіберзахисту. До таких об'єктів віднесено [6]:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси;

2) об’єкти критичної інформаційної інфраструктури (перелік затверджується КМУ);

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Відмітимо, що основна роль в забезпеченні кіберзахисту критичної інфраструктури належить телекомунікаціям – як у забезпеченні власної безпеки, так і всіх важливих об’єктів. На жаль, українські мережі зв’язку (глобальні, метропольні та локальні) побудовані в основному на базі іноземного обладнання (маршрутизатори, телекомунікаційні процесори, роутери, їх прогамне забезпечення тощо).

Основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації, Національна поліція України, СБУ, МО України та ГШ ЗСУ, розвідувальні органи, Національний банк України.

Загроза кібервійни привела до вражаючого факту: в США урядовий зв’язок відмовився від IP-телефонії. Поворотним моментом послужив теракт 11 вересня 2001 року в Нью-Йорку, і, як міра протиборства була сформована надпотужна структура – Міністерство внутрішньої безпеки, хоча боротьба з тероризмом розпочалася значно раніше. Було поставлено завдання розробити всеохоплюючу національну стратегію по захисту інфраструткури від фізичних і кіберзагроз. Спеціальна комісія із 5-ти команд, що представляли дев’ять інфраструктур виділила п’ять напрямів захисту:

телекомунікації, ПЕОМ і програмне забезпечення, Інтернет, супутники і оптоволокно;

залізниці, повітряний і морський транспорт, трубопроводи;

електроенергія, газ, нафта, виробництво, зберігання і транспортування;

фінансові операції, фондові і ринки облігацій;

вода, аварійні служби, державна служба.

У відповідності до вказаних напрямів був розроблений стандартизований опис критичної інфраструктури для полегшення контролю і підготовки до ліквідації НС. Відпрацьована Рамочна концепція, яка складається із 5-ти функцій кіберзахисту:

виявити – відпрацювати ризики і управління ними;

захистити – розробити заходи по кіберзахисту об’єктів;

виявити – впровадити відповідні заходи;

відповісти – здійснити заходи кіберзахисту;

відновити порушені функції і забезпечити стійкість роботи системи.

Ці п’ять функцій складаються із 22 заходів та включають множину стандартів, методик, процедур і процесів, що детально описані і підлягають виконанню операторами критичної інфраструктури. Крім того вони зобов’язані

повідомляти про інциденти ІТ-безпеки. Не виконання приписів передбачає досить строгі покарання:

до 20 років позбавлення волі – за розкрадання інтелектуальної власності американських компаній з використанням інформаційних технологій;

до 30 років позбавлення волі без права дострокового звільнення – за проникнення в державні мережі, енергомережі, транспортні канали зв'язку або системи управління водоспоживанням;

до 100 років позбавлення волі – за кіберзлочини.

Окрім того Президент США Барак Обама в 2015 році затвердив нову Стратегію національної безпеки держави і політику в інформаційній сфері згідно якої військове керівництво США розглядає кіберпростір як одну із сфер проведення військових операцій поряд з наземною, морською, повітряною і космічною операціями. В якості потенційних противників називають Росію, Китай, Північну Корею і Іран.

У Китаї політика в кіберпросторі визначається з 2005 року стратегією розвитку інформатизації, яка просуває Інтернет у народне господарство з метою розвитку економіки. При цьому китайці застосовують обмежувальні заходи в кіберпросторі. Так, наприклад, користувачі не мають права реєструватися в соціальних мережах, використовуючи псевдонім. Окрім того в рамках фільтрації Інтернет-контенту «Вогняна стіна « в Китаї офіційно заборонені найбільша в світі соціальна мережа Facebook, відеохостингова компанія You Tube та соціальна мережа мікроблогів Twitter.

Великобританія прийняла стратегію у сфері кібербезпеки у 2011 році і реалізує інформаційну політику з метою виводу країни на перше місце по інноваціям, інвестиціям і якості сервісів у сфері ІТ-технологій.

У Німеччині документ по кібербезпеці був прийнятий у 2011 році і передбачає створення внутрішньої системи звітності про інциденти ІТ-безпеки. Не виконання вимог про вказану звітність підлягає штрафу у розмірі 100 тис. €, які можуть бути накладені на оператора критичної інфраструктури, який не зміг реалізувати вказані міри ІТ-безпеки.

У Росії Доктрина інформаційної безпеки РФ була затверджена у 2016 році. До основних положень Доктрини відноситься стратегічне стримування і відвертання військових конфліктів, які можуть виникнути в результаті застосування інформаційних технологій. Росія відноситься до п'ятірки країн, що володіють потужними кібервійськами (у 2014 році були створені війська інформаційних операцій РФ). До таких країн відносяться: США, Китай, Росія, Велика Британія і Південна Корея [7].

Таким чином, розвиток інформаційних технологій обумовлює появу нових видів кібератак. Відповідно, однією з основних складових національної безпеки держави стає забезпечення інформаційної безпеки. В Україні почалась активна робота в цьому напрямі. Для реалізації інформаційної безпеки необхідно застосовувати не тільки інфраструтуру, стійку до кібератак (квантові комп'ютери, можуть стати одним із компонент вирішення цієї задачі), але і забезпечувати цифровий суверенітет (розвивати українське програмне і

апаратне забезпечення). Крім того необхідно прискорити міжнародне співробітництво за напрямками протидії кібератакам зі сторони терористичних організацій і країн, а також застосування кіберзброї для боротьби з ними. Але на сучасному етапі, найбільш перспективним напрямом вдосконалення інформаційної безпеки об'єктів управління і зв'язку та інформації в рамках існуючих технологій є багаторівневий багатопозиційний захист (ББЗ) з використанням апаратно-програмних засобів і способів захисту об'єктів і інформації [8].

Звичайно, що технічна основа ББЗ повинна базуватись на наступних основних принципах:

1) незалежно від фізичної природи потенційних загроз система захисту повинна протидіяти її реалізації з певною (необхідною) мірою надійності;

2) в системі повинен здійснюватись моніторинг стану захищеності об'єкта захисту, основна функція якого своєчасне і достовірне виявлення небезпечних подій;

3) в системі повина здійснюватись ідентифікація виявленої небезпечної події та прийняття заходів по її нейтралізації;

4) система у будь-якому випадку завжди реалізує умови припинення (нейтралізації) загрози;

5) система повина забезпечувати припинення дій дестабілізуючих факторів із заданою мірою надійності.

У відповідності з розглянутими принципами ББЗ має містити наступні рівні:

рівень безпосереднього захисту, що забезпечує відвертання фізичних чи логічних атак;

рівень виявлення, що забезпечує своєчасне і достовірне виявлення небезпечної події і передачі інформації органу, який приймає рішення на її нейтралізацію;

рівень збору і обробки інформації;

рівень оперативного реагування системи захисту, що забезпечує створення своєчасних умов для нейтралізації небезпечної події;

рівень нейтралізації небезпечної події.

Кожен із вказаних рівнів захисту може бути реалізований з використанням різних технічних і програмних засобів, які забезпечують високу логічну, технічну і оперативну стійкість роботи системи захисту. При цьому можливі наступні підходи для рішення задачі ідентифікації [9]. Перший заснований на використані додаткових спеціальних засобів, таких як засоби відеоконтролю для систем фізичного захисту, вимірювальні прилади і апаратура для засобів захисту інформації від витоку та спеціальні програмні продукти для верифікації і ідентифікації комп'ютерних програм. Другий підхід базується на застосуванні шаблону ситуацій. Ці шаблони повинні включати у собі параметри, які описують стан системи і об'єкта захисту, поведінку порушників, зовнішні фактори. Співпадіння ситуацій із заданим в одному із шаблонів вказує

на наявність небезпечної події.

Далі здійснюється вироблення варіанта реагування на небезпечну подію. Його реалізація полягає в синтезі можливих варіантів, що задовольняють критерію виконання вимог до ефективності нейтралізації небезпечної події і процесам, які її реалізують. Задача синтезу може формуватися як оптимізаційна. У цьому випадку відшукується єдине найкраще рішення.

На 4-му рівні здійснюється оперативне реагування на небезпечну подію з метою її нейтралізації (видалення). Реалізація процедур даного рівня залежить від організації управління захистом і від просторово-технологічних можливостей системи захисту по припиненню небезпечних подій. Міри, які реалізуються на даному рівні, є обов'язковими тільки для систем захисту інформації.

Останній п'ятий рівень захисту передбачає безпосередню нейтралізацію небезпечних подій. Складність заходів даного рівня полягає у вирішенні конфліктної ситуації, яка вимагає використання спеціальних ресурсів. Завершує дану послідовність контроль результатів нейтралізації небезпечної події і оцінка по заданому критерію.

Висновки. З наведеного вище можна зробити наступні висновки:

кіберпростір має стати інструментом нашої асиметричної відповіді на агресію;

добиватися управління не тільки своїми засобами, але й супротивником;

створювати і вдосконалювати інтелектуальний потенціал (де чільне місце займає підготовка кадрів), мислити по-новому;

усі органи і системи управління «тримати в формі» шляхом проведення впорядкованих тренувань із управління у кризових ситуаціях із охопленням всіх можливих варіантів розвитку подій;

багаторівневий захист може використовуватися для вирішення завдань забезпечення інформаційної безпеки об'єктів різного призначення як для захисту самого об'єкта, так і для захисту інформації, яка в ньому циркулює.

У відповідності до висновків кібербезпека сьогодні набуває значення нової галузі у нашому ВПК і призначена забезпечити національну безпеку держави. Тому своєчасне планування і реалізація заходів забезпечення кібербезпеки та інформаційного протиборства на глобальному і регіональному рівнях стає одним із пріоритетних завдань держави. Україна не просто може, а вимушена перестати концентруватися виключно на оборонних заходах. Маючи один із найкращих у світі людських потенціалів, фахівців з ІТ, здатність працювати швидко та ефективно, високу мотивацію до протистояння зовнішній агресії, держава повинна робити ставку не лише на оборонні технології, а й на наступальні, у т.ч. – кіберозброєння.

Список використаної літератури

1. Електронний ресурс [Режим доступу https://uk.wikipedia.org/wiki].

2. Закон України від 01.06.2010 р. №2297-VII «Про захист персональних даних». [Електронний ресурс Режим доступу http://zakon0.rada.gov.ua/laws/show/2297-17/page].

3. О.Г. Ніщеглотова. Протидія кібервійні як засіб забезпечення національної безпеки. Інформаційні технології і право. – 2016. №6. – С. 22-27.

4. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 jn the identification of European critical infrastructures and the assessment of the need to improve their protectoin.

5. Указ Президента України від 15.03.2016 р. «Про Стратегію кібербезпеки України». [Електронний ресурс Режим доступу zakon.rada.gov.ua/laws/show/96/2016].

6. Закон України від 05.10.2017 № 2297-VIII «Про основні засади забезпечення кібербезпеки України». [Електронний ресурс Режим доступу http://zakon2.rada.gov.ua/laws/show/2163-19.

7. Паршин С.А., Горбачев Ю.Е. Кибервойны – реальная угроза национальной безопасности. – М: Из-во КРАСАНД, 2011.

8. Никифоров О.Г. Концептуальные вопросы многоуровневой защиты объектов информации. Информационная и кибербезопасность. -№6. 2013. С. 34-37.

9. Масовець В.В., Фісун А.П. Методи комплексного контролю безпеки інформації на об’єктах телекомунікаційних систем органів державного управління: Монографія. Під заг. Ред. В.В. Масовця. – М:, 2009 – 368 с.

КРИЗОВЕ КОМУНІКАЦІЙНЕ ПЛАНУВАННЯ ПРЕС-СЛУЖБИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

В. А. Бутенко
головний редактор журналу «Енергозбереження Поділля»

Коли ми говоримо за раціональну організацію кризових комунікацій, то маємо на увазі створення системи комунікацій, план їх розгортання під час кризи. Така система являє собою послідовність дій, які в загальному вигляді відображають особливості встановлення і функціонування ефективної системи кризових комунікацій. Для конкретної ситуації система комунікацій матиме певні особливості, проте в загальному вигляді вона вимагає здійснення всіх або деяких з наступних дій:

- визначити всі можливі контактні аудиторії, які очікуватимуть інформації про розвиток кризи.

Для цього потрібно виділити контактні групи та визначити їх інтереси. Установити, яким чином розсилатимуться їм повідомлення, передбачені антикризовим планом. Нині склад контактних груп значно поширився і це сталося впродовж останніх років, завдяки світовій мережі Інтернет. Тепер, крім журналістів державних та недержавних друкованих та електронних ЗМІ, додаються блогери та користувачі соціальних мереж. А це значно ускладнює роботу прес-служб, лише тому, що як правило блогери та користувачі – непрофесійні журналісти і висловлюють далеко непрофесійний погляд на ті, чи інші події, що може у деяких випадках сприйматися за істину. Крім цього, з боку сусідньої держави працюють і спеціальні служби, завдання яких не що інше, як дестабілізувати ситуацію в Україні. Вперше, з так званими «тролями» українська спільнота зіткнулася у 2013-2014 роках з початком гібридної війни;

- продумати, яким чином довести, що керівництво організації виявило проблему і діє для її розв’язання.

Для цього потрібно враховувати, що не лише журналісти, а й інші учасники інформаційного процесу будуть збентежені і налаштовані вороже, якщо відчують, що керівництвом (або командуванням) проблема сприймається легковажно, чи неадекватно загрозі. Вони чинитимуть тиск на керівництво та персонал, поки не переконаються, що відбувається правильне оцінювання проблеми та загроз. Нарешті, вони усвідомлюють, що проблема не буде розв’язана, доки керівництво не визнає, що вона існує. У своїй практиці керівникам прес-служби потрібно враховувати і те, що як правило їх інформація сприйматиметься критично, а коментарі негативно налаштованих користувачів можуть звести роботу до заперечливого результату. Вихід з цієї ситуації є. Так, прикладом, прес-служба одного з відомств створила кілька дружніх інтернетівських спільнот в соціальних мережах, які у критичній ситуації мали позитивний психологічний вплив на аудиторію, видаючи позитивні відгуки на ті або інші матеріали, або критикуючи особо активних опонентів;

- швидко розробити невелику кількість повідомлень для журналістів, що описують проблему і шляхи її розв’язання в загальних рисах.

Згодом конкретизувати повідомлення, наблизити їх зміст до інтересів цільових аудиторій і розробити найкращі способи спілкування з ними, використовуючи наявні напрацювання з арсеналу антикризових заходів. Інформаційні повідомлення мають висвітлювати усію послідовність ліквідації кризи;

- повідомляти тільки те, що може бути впевнено перевірено і підтверджено.

Тут головна вимога, якої потрібно дотримуватися, це остерігатися робити припущення щодо ситуації. Краще чітко і ясно пояснити кілька пунктів позиції керівництва, ніж гадати про можливі дії і підірвати довіру до повідомлень, якщо в майбутньому вони не підтвердяться. Положення, які мають бути доведені до відома аудиторії, повинні бути виражені впевнено і не залишати місця для різночитань і сумнівів. Неперевірену інформацію краще опускати, також як утримуватися від домислів і припущень – цю роботу в будь-якому випадку зроблять журналісти;

- не повідомляти неправдивої інформації.

Одна невелика брехня перетвориться на потужний ланцюг неправди. Це найгірша помилка, яку організація може здійснити, для захисту і збереження своєї репутації під час кризи. Бути спійманим на брехні – найгірше, а це найбільша шкода з усіх можливих;

- не коментувати гіпотетичні ситуації.

Засоби масової інформації зазвичай вимагають коментарів гіпотетичних ситуацій. «Що ви будете робити, якщо відбудеться ..?», «Якщо трапиться .., як відреагує ваша організація?». Часто спроби таких коментарів подаються пресою як зобов'язання діяти певним чином. Підрив сформованих очікувань може завдати великої шкоди іміджу організації;

- створювати і підтримувати стійке враження, що керівництво організації доступно для спілкування та комунікації.

У багатьох випадках відразу після кризи підтвердити і обговорити можна небагато. У такій ситуації важливо пояснити, що може, а що не може бути повідомлено в даний момент, і створити атмосферу чесності, відкритості та доступності. Це найважливіший з чинників ефективного управління кризою.

Для цього реально створити кілька груп журналістів:

перша група – повністю лояльна відомству (зовсім небагато чисельна). Представники цієї групи запрошуються «випадковими свідками» оперативних заходів (затримання, патрулювання). Реалізується, так звана, іміджева програма відомства (документальні фільми, інтерв'ю з керівництвом та персоналом);

друга група – ситуаційно лояльна. У більшості нейтральні до відомства ЗМІ, які можуть як підтримати позицію прес-служби, так і виступити опонентами. Представники цієї групи разом з представниками першої запрошуються на прес-конференції, брифінги, постійно забезпечуються прес-релізами;

третя група нелояльних ЗМІ, які з урахуванням їх політичної або іншої заангажованості, стають постійними опонентами та критиками відомства. З цією групою слід ретельно співпрацювати, постійно запрошувати до висвітлення тих інформаційних приводів, коли відомство у виграшному

становищі. А от висвітлення подій у критичному світлі лише надає відомству авторитета;

- бути оперативними і заповзятливими.

Для доведення контактним аудиторіям, що для подолання кризи робиться все можливе, у розпорядженні звичайно є кілька годин або днів (в залежності від типу кризи). Ситуація вимагає від керівництва швидких дій та прийняття інформаційних рішень. На ранніх етапах кризи важливо довести свою компетентність і наявність контролю над ситуацією. У той же час буде важко створити таке сприйняття, якщо керівництво зайняло оборонну позицію;

- не говорити «без коментарів» представникам преси.

Існує кілька способів зберігати мовчання, але в той же час підтримувати відчуття контролю, доступності, чесності та довіри. Говорячи «без коментарів», прес-секретар організації бере на себе роль дилетанта, який, поза всяким сумнівом, ніколи раніше не керував кризою;

- повідомляти всі погані новини одночасно.

Це майже завжди більш ефективно, оскільки дозволяє знизити кількість проблем у взаєминах з журналістами, що виникають щоразу, коли повідомляється погана новина.

- встановити канали отримання відгуків і інформації від контактних аудиторій.

Не варто вважати, що достатньо просто поширити інформацію. Важливо отримати відгуки, пропозиції та ідеї від представників ЗМІ. Доцільно використовувати і соціальні мережі. Відсутність двосторонніх комунікаційних каналів під час кризи майже завжди веде до розриву відносин;

- організувати облік документів.

Отримані телефонні дзвінки, протоколи нарад, контакти і переговори, що відбуваються під час кризи, повинні фіксуватися. Інформація може в майбутньому знадобитися адвокатам, піарникам та іншим фахівцям. Може стати важливою у майбутньому, наприклад, така інформація: хто був той громадянин, який погрожував нам; як звали телевізійного репортера, який брав у нас інтерв'ю; кого і коли ми сповіщали?

- постійно контролювати й оцінювати ситуацію.

Як ми отримуємо повідомлення? Які повідомлення перетинаються? Які питання ми отримуємо? Відповіді на ці та подібні питання допоможуть визначити, як краще скорегувати комунікаційний процес;

- не припиняти комунікації, навіть якщо пік кризи подолано.

Багато заспокоюються вдалим початком комунікацій в перші дні кризи і роблять висновок, що їх контактні аудиторії більше не потребують подальших комунікацій. Навіть якщо можна вже не говорити власне про кризу,

припинення комунікацій – завжди помилка. Криза дає керівництву можливість вступити в тісний контакт з цільовими аудиторіями. Потрібно використовувати момент і шукати шляхи до подальшого зміцнення відносин.

Представлений список принципів показує, наскільки складні комунікаційні проблеми стоять перед керівниками. У реальному житті дуже важко або просто неможливо виключно пунктуально виконувати всі вимоги раціональної організації комунікацій. Як реагувати на допущені помилки і помилки у впровадженні комунікацій? Можливі два варіанти дій: визнати помилку або продовжувати працювати, не звертаючи на неї уваги.

У більшості випадків досить імовірно, що люди пробачать і підтримають організацію, якщо її керівник визнає помилку. Але якщо виникає підозра, що керівництво не визнає помилок, то виникне розчарування в розумності та достатності антикризових заходів. У такій ситуації журналісти стають роздратованими, недоброзичливими, до тих пір поки їм не будуть пред'явлені переконливі докази того, що для вирішення проблеми робляться прийнятні для них заходи. Такі проблеми можуть виникати, якщо робиться коментар, ненавмисно зачепив якусь із цільових аудиторій, повідомляються неприпустимі чи неточні дані щодо проблеми. У такій ситуації майже напевно буде краще дотримуватися наступної послідовності дій для виправлення ситуації.

Визнати помилку.

У більшості випадків, якщо в роботі сталася помилка (у тому числі з вини керівництва), очевидно, хто в цьому винен. Одним з найкращих кроків, у таких випадках, буде визнати помилку і вжити впевнені кроки для усунення її негативного ефекту.

Вибачитися, якщо це доречно.

Якщо допущена помилка, яка негативно вплинула на настрої представників ЗМІ, керівнику доцільно вибачитися і взяти на себе відповідальність. Навіть якщо проблема виникла не з вини керівника, йому слід показати, що він більше всіх засмучений і засмучений через це. Більшість людей прощає помилку, якщо хто-небудь її визнає і вибачається.

Визначити кроки, щодо швидкого та ефективного розв'язання проблеми.

Багато журналістів будуть продовжувати нападати на керівництво організації, поки не переконаються, що воно розв'язує проблему. У багатьох випадках вони воліють почути, що конкретно зроблено для корекції ситуації, щоб самостійно вирішити, чи належним чином це робиться.

Пояснити, що робиться, щоб подібна ситуація не повторилася.

Цільові аудиторії бажають почути, що буде зроблено для профілактики проблеми. Сюди можна включити зміни в політиці, в процедурах або в

управлінні персоналом. Важливе їх бажання дізнатися, коли надійде наступна інформація.

Таким чином, багатьох помилок вдасться уникнути, якщо заздалегідь, ще до кризи, провести роботу з аналізу комунікаційних можливостей під час кризи. Такий аналіз припускає, що будуть визначені можливі проблеми та слабкі місця комунікаційного процесу, сегментовані аудиторії та визначені бажані результати. Не слід ускладнювати проблему з роз'яснення її суті аудиторії, особливо якщо для адекватного розуміння проблеми потрібні спеціальні знання. За короткий час безпосереднього вербального контакту з аудиторією або інтерв'ю навряд чи вдасться роз'яснити з належною глибиною суть проблеми, а мистецтвом популяризації та умінням просто говорити про складне володіють не всі люди. Допомогти в цьому випадку можуть посилання до спеціально підготовлених для цього довідок та інших документів, що містять цифровий, графічний, табличний матеріал та іншу інформацію, яка погано сприймається на слух. Не слід посилювати й деталізувати проблему, робити здогадки (нехай навіть і компетентні) про те, що викликало проблему і шляхи її розв'язання. У цьому випадку існує ризик мимоволі повідомити неправдиву інформацію.

Важливо заздалегідь визначити ключові повідомлення, які потрібно довести до кожної конкретної аудиторії. Треба пам'ятати, що проблема найчастіше має кілька варіантів розв'язання, а ставлення різних журналістів до таких варіантів буде відрізнятися. Тому доцільно під час спілкуванні з різними аудиторіями робити акцент на тому варіанті, який виглядатиме більш привабливо в очах даної аудиторії. Зрозуміло, мова йде про варіанти, які не суперечать один одному і базуються на деяких загальних принципах.

Продуманою має бути і тактика влаштування комунікацій. Коли визначені варіанти антикризових дій, складено план і визначено час початку комунікаційних заходів, слід негайно і енергійно розпочати роботу. Краща тактика – швидкість і інтенсивність реалізації плану комунікацій. Також швидко потрібно визначити найкращий спосіб комунікації з різними контактними аудиторіями (представниками ЗМІ, лідерами громадських організацій, посадовими особами, політиками). Тактика може включати особисті та групові збори, листи та доповідні записки, телефонні дзвінки, повідомлення електронною поштою, інформаційні бюлетені, листівки, брошури і оголошення в газеті.

Для того щоб уникнути помилок кризового спілкування в майбутньому, потрібно затратити зусилля для оцінки сильних і слабких місць проведених комунікаційних заходів. Це можна зробити шляхом тестування, зборів фокус-груп, телефонних опитувань, інтерв'ю «віч-на-віч», постановки завдань і

формування спеціальних аналітичних груп. Слід проаналізувати відгуки, оцінки, ідеї та пропозиції, а потім у випадку необхідності намітити і здійснити заходи, що коректують комунікації.

Досить часто у колі журналістів відчувається негативне ставлення до тих чи інших керівників прес-служб, мовляв, він не має журналістської освіти. На мою думку керівник прес-служби не обов'язково має бути професійним журналістом, хоча відповідна освіта та досвід роботи у ЗМІ значно допоможуть йому будувати плідні стосунки з представниками мас-медіа.

Керівник прес-служби передусім менеджер, який зобов'язаний, використовуючи інформацію, націлити ЗМІ на висвітлення подій з максимальним позитивним ефектом для відомства та держави у рамках спільної міжвідомчої програми. Він обов'язково повинен мати досвід роботи у своїй організації, для того щоб знати про що йдеться у підготовленому прес-релізі. Також немаловажне програмування наслідків, до яких можуть призвести зайві слова або речення, для співробітників, які цей інформаційний привід створювали. У той же час вислів: «я лише керівник прес-служби, мені таємниць не довіряють, тому нічого зайвого сказати не можу» – безграмотний та найнебезпечніший для відомства. До того ж представник прес-служби має бути психологічно урівноваженим і завжди готовим до «незручних» запитань з боку журналістів. Неадекватна поведінка, зайве нервування, розгубленість, непереконливі коментарі можуть завадити відомству у виконанні операцій.

Досить негативно сприймається громадськістю з'ясування стосунків між відомствами із залученням ЗМІ. В умовах гібридної війни міжвідомчі війни можуть викликати панічні настрої серед людей, що буде використано державою-агресором, для проведення інформаційної операції з дискредитації України перед міжнародними партнерами. У такому випадку виправдання на рівні МЗС вже є вторинним і не створить очікуваного результату.

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ТА ОСОБЛИВОСТІ ВЗАЄМОДІЇ ІЗ ЗАСОБАМИ МАСОВОЇ ІНФОРМАЦІЇ

РОЛЬ І МІСЦЕ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОРГАНАХ УПРАВЛІННЯ ВІЙСЬКОВИМИ ТА ПРАВООХОРОННИМИ ПІДРОЗДІЛАМИ

О. С. Андрощук
В. Б. Корчев
О. Ю. Андрощук

Події кінця XX – початку XXI ст. відбуваються на фоні трансформації суспільства від постіндустріального до інформаційного. Бурхливо розвиваються інформаційні технології (далі – ІТ), які проникають в усі сфери діяльності людини: соціальну, економічну, політичну, військову, правоохоронну. Характерними рисами революції в інформатизації і комунікаціях у військовій справі на сучасному етапі є:

глобалізація інформаційних процесів в арміях провідних країн світу;

мініатюризація елементної бази обчислювальної техніки і полегшення її інтеграції зі зразками озброєння;

зростання надійності і мобільності обчислювальних мереж як матеріальної основи для побудови різних інформаційних систем військового призначення.

Усе вищеперераховане зумовлює і значні зміни, які відбуваються у військовій справі:

розроблення нових концепцій ведення військових конфліктів, передусім концепції «неконтактних бойових дій», удосконалення форм і способів застосування військ. Сучасні військові конфлікти набули специфічних рис:

рішучості в досягненні політичних цілей, спрямованості на порушення роботи систем державного військового управління і критичної інфраструктури держави-опонента, динамічності, швидкоплинності, високої технологічності застосовуваних засобів;

удосконалення автоматизованих систем управління військами і зброєю (розроблення і виготовлення автоматичних систем управління зброєю);

удосконалення засобів високоточної зброї, які завдяки включенню в інформаційне середовище «бойового простору» можуть бути коригованими навіть після запуску;

удосконалення засобів розвідки, здатних діяти автономно тривалий час і

перебувати на достатньо великих відстанях.

На сьогодні можна вести мову про континуум вимірювань, у яких можливе ведення збройної боротьби не тільки у традиційних вимірах простору й часу, а й в інформаційному.

Аналіз застосування ІТ дозволяє достатньо чітко визначити такі напрями застосування ІТ у сучасній збройній боротьбі: у системах управління військами, у системах управління зброєю, як зброї, яка є основою для структурно-функціональної трансформації збройних сил і розроблення нових концепцій ведення конфліктів й форм застосування військ.

ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА УКРАЇНИ

М. В. Бурак

Слід відзначити, що за останній рік політика держави у сфері захисту її інформаційного простору та забезпечення інформаційної безпеки загалом стала більш комплексною й ефективною. Можна констатувати, що після особливо складних 2014-2015 рр. держава почала формувати в 2016 р. комплексну систему протидії інформаційному складнику гібридної війни. У 2017 р. триває активний розвиток цього процесу, приймаються узгоджені рішення, додержується досить вдалий баланс між обмежувальними (для ворожого контенту та деструктивних дій супротивника) і стимулюючими (для власного контенту) заходами як стосовно захисту інтересів громадян, суспільства та держави, так і для подальшого розвитку її інформаційного простору.

Важливим етапом формування сучасної державної інформаційної політики стало ухвалення Доктрини інформаційної безпеки України.

До інших важливих кроків розвитку та захисту національного інформаційного простору слід віднести: вирішення проблеми обміну інформацією з обмеженим доступом між Україною та НАТО; удосконалення процедури застосування санкцій Національною радою України з питань телебачення і радіомовлення та розширення переліку підстав для переоформлення ліцензії, що спрямовано на забезпечення дієвого механізму здійснення нагляду у сфері телебачення та радіомовлення; позбавлення російських спецслужб можливостей слідкувати за громадянами України через блокування відповідних сайтів тощо.

З метою більш ефективного впровадження положень Стратегії кібербезпеки України розроблено комплекс заходів, спрямованих на подолання кіберзагроз національній безпеці, та розпочато їх реалізацію. Передусім це ухвалення Указу Президента України від 13 лютого 2017 р. № 32/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».

ДО ПРОБЛЕМИ ПІДГОТОВКИ ІНФОРМАЦІЙНИХ МАТЕРІАЛІВ ІЗ ЗОНИ ЛОКАЛЬНОГО ЗБРОЙНОГО КОНФЛІКТУ

Ю. А. Дем'янюк

У разі підготовки представниками правоохоронних органів матеріалів для засобів масової інформації в зоні локального конфлікту необхідно зосередити увагу на такому:

показати проблему як таку, яку можна конструктивно вирішити;

орієнтувати громадянське суспільство на подолання труднощів, надати підстави до надії та віри у краще;

чітко орієнтувати людей на головні морально-патріотичні цінності;

показувати конкретні приклади мужності та стійкості співробітників правоохоронних органів;

акцентувати не на розгубленості, а на активних діях людей у важких ситуаціях, описувати будь-які випадки активного спротиву;

закликати суспільство до всебічної підтримки владних та силових структур;

стимулювати психологічно-соціальну підтримку постраждалим і родинам полеглих;

показувати мужнє сприйняття трагічної ситуації з боку родин полеглих воїнів; висвітлювати найкращі риси загиблих героїв;

де-героїзувати агресора;

закликати до згуртованості у складний час;

широко висвітлювати всебічну підтримку світового співтовариства;

чітко аналізувати конкретні проблеми та послідовно інформувати громадськість про їх розв'язання, а після цього – акцентувати увагу на перемозі та на врятованих життях;

апелювати до почуття національної гідності;

широко висвітлювати також і героїзм «працівників тилу» та волонтерів, їхнє гаряче бажання допомогти тим, хто воює «на передовій».

Важливо пам'ятати, що спрямовуючи інформаційні матеріали до редакцій національних та місцевих засобів масової інформації, необхідно:

до кожного відеофайлу зробити супровідний текст із «розкадровкою» та чіткими поясненнями до неї;

у поясненнях до «розкадровки» особливо старанно поставитися до зазначення назв місцевостей, підрозділів чи службових об'єктів , військових звань, посад, прізвищ та імен – керуючись при цьому міркуваннями службової доцільності та збереження військової таємниці;

те ж саме слід зробити (у вигляді окремих анотацій) щодо фоторепортажних матеріалів чи фотоілюстрацій для статей, заміток тощо;

не включати до оперативних медіа-матеріалів для «цивільних» засобів інформації ті відеофрагменти чи фотознімки, де є хоч-якась прив'язка до місцевості (дорожні вказівники, різноманітні пам'ятники, характерні об'єкти тощо).

Все викладене вище належить до прямих завдань прес-служб правоохоронних органів.

КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ ПРАВОВОЇ ПОЛІТИКИ ДЕРЖАВИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

О. О. Іляшко

Політика України, як держави, де ведеться процес євроінтеграції, максимально направлена на забезпечення прав, свобод людини та громадянина, приведення всіх сфер діяльності держави до міжнародних стандартів.

Правова політика держави як соціальний феномен створює передумови та вказує напрями розвитку суспільства загалом. Втілення у правовій політиці принципів демократизму і соціальної справедливості забезпечує функціонування всієї політичної системи у правовому полі, є первинним етапом у формуванні громадянського суспільства, орієнтованого на соціальну справедливість та побудову правової держави. Правова політика забезпечує консенсус між членами суспільства, державною владою та громадськістю, неурядовими організаціями. Враховуючи специфіку стану в суспільстві під час гібридної війни, держави особливо стрімко мають спрямовувати свою правову політику на забезпечення дотримання принципу законності та установлення правопорядку.

Правова політика держави в умовах гібридної війни потребує більш детального дослідження, враховуючи те, що людське суспільство неможливо уявити без агресії та бойових дій. Війна або загроза застосування сили давно стали елементом великої політики.

Проаналізувавши думки вчених з приводу поняття «правова політика держави», можна надати авторське визначення правової політики держави в умовах гібридної війни. Так, правова політика держави в умовах гібридної війни – це вид державної політики, що є обґрунтованою та послідовною діяльністю органів державної влади, органів місцевого самоврядування з метою забезпечення ефективного механізму правового регулювання суспільних відносин в умовах гібридної війни та виражається в комплексі ідей, заходів, завдань, програм, настанов, що реалізуються у сфері права і завдяки праву та базується на основоположних правових принципах.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВИЯВЛЕННЯ МЕТАМОРФНИХ ВІРУСІВ В ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

О. С. Савенко
А. О. Нічепорук

Сьогодні значна увага приділяється дослідженням в напрямку виявлення шкідливого програмного коду, проте ефективність методів виявлення

метаморфних вірусів відносно невисока. Складність виявлення метаморфних вірусів зумовлено використанням ними технік переміщення та переписування власного коду. Кожна нова копія, що створюється метаморфним вірусом відрізняється від вже існуючих.

Тому, з метою підвищення достовірності виявлення метаморфних вірусів пропонується інформаційна технологія виявлення метаморфних вірусів в локальних комп'ютерних мережах. Використання мережі продиктоване наявністю, окрім обфускаційних технік, антиемуляційних засобів, що перешкоджають здійсненню процесу емуляції виконання – одного із головних методів виявлення метаморфних вірусів, що в свою чергу призводить до низької ефективності виявлення. Тому, здійснення виявлення метаморфних вірусів, які застосовують антиемуляційні технології, засобами однієї КС є неможливим, у зв'язку з чим досліджується саме локальна комп'ютерна мережа.

В основі розробленої інформаційної технології закладено метод виявлення метаморфних вірусів на основі аналізу поведінки з використанням модифікованих емуляторів.

Метод, що розроблений, заснований на відстеженні API викликів, що описують потенційно небезпечну поведінку метаморфного вірусу, та порівнянні дизасембльованого коду функціональних блоків метаморфного вірусу з кодом функціональних блоків його зміненої версії. Для формування висновку про схожість підозрілої програми до метаморфного вірусу використовується система нечіткого логічного висновку. У випадку недостатнього прояву шкідливої поведінки та підвищення рівня достовірності для виявлення метаморфного вірусу залучаються інші хости локальної мережі.

ОСОБЛИВОСТІ ВЗАЄМОВІДНОСИН ПРАВООХОРОННИХ ОРГАНІВ З ПРЕДСТАВНИКАМИ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ В КРИЗОВИХ СИТУАЦІЯХ

О. М. Ставицький

Найголовнішим принципом щодо оприлюднення інформації серед представників засобів масової інформації в часі будь-якої кризової ситуації є таке: керуватися, насамперед, службовими (оперативними) вимогами, а потім уже іншими потребами. У кризових ситуаціях необхідно:

від самого початку мобілізуватися на те, щоб утримати під контролем все, що засоби масової інформації пишуть про неї;

важливо обмежити всі якнайменші витоки інформації назовні; особливо це стосується нижчих ланок управління;

спілкування необхідно звести до двох представників правоохоронного органу: «речника» (бажано, щоб це був медіа-працівник) та одного з керівників (рівень визначають в залежності від ситуації);

категорично не можна подавати представникам засобів масової інформації недостовірну інформацію, видаючи бажане за дійсне;

не припустимо говорити невизначено, неозначено чи розпливчасто посилатися на «причини певного характеру», не варто також ухилятися від найгостріших запитань преси;

не можна виправдовуватися чи називати надумані причини;

офіційні повідомлення слід формулювати надзвичайно чітко так, щоб уникнути двозначностей і довільних трактувань;

найважливішу, ключову інформацію слід подавати тільки найрейтинговішим, найавторитетнішим і найвиваженішим засобам масової інформації;

оприлюднюючи інформацію, слід акцентувати не на негативі, а на позитиві;

категорично не слід вживати хоч найменші елементи гумору на медіа-заходах, де журналісти розглядають ту чи іншу кризову ситуацію.

СЕКЦІЯ № 2. ДІЄВІ МЕХАНІЗМИ КОМУНІКАЦІЙ З ГРОМАДСЬКІСТЮ ЯК ОСНОВА ДІЯЛЬНОСТІ МВС УКРАЇНИ

ВЗАЄМОДІЯ ПОЛІЦІЇ З НАСЕЛЕННЯМ: ЗАРУБІЖНИЙ ДОСВІД

А. В. Калайда

Розглянувши положення Закону України «Про Національну поліцію», ч.2 ст.9 вимагає від поліції забезпечення постійного інформування громадськості про свою діяльність у сфері охорони та захисту прав і свобод людини, протидії злочинності, забезпечення публічної безпеки і порядку. Також, у ч.1 ст.11 зазначеного Закону закріплюється положення про те, що «діяльність поліції здійснюється в тісній співпраці та взаємодії з населенням, територіальними громадами та громадськими об'єднаннями на засадах партнерства і спрямована на задоволення їхніх потреб».

Досліджуючи взаємодію поліції з населенням, яка, основана на законі, можна дійти висновку, що – це є нагальною потребою сьогодення.

Використання зарубіжного досвіду щодо взаємодії поліції з населенням є позитивним. У таких країнах, як США, Великобританія, Німеччина, Австрія, Бельгія, Італія, Франція, Японія та інших вважається, що взаємодія поліції з населенням є необхідною умовою для ефективної роботи таких підрозділів. Відомі західні програми взаємодії поліції з населенням – «Зупини злочинця», «Громадський патруль», «Сусідська допомога», «Допомога жертвам правопорушень», утворення наукових та педагогічних організацій, які передають поліції результати своєї роботи та надають рекомендації по підвищенню ефективності роботи правоохоронних органів. Такий досвід іноземних держав, сприяв би активізації взаємодії поліції з громадськістю в забезпеченні публічного порядку, профілактики та розкриття злочинів в Україні.

Отже можна зробити висновок, що аналіз і використання зарубіжного досвіду участі населення у правоохоронній діяльності є дійовим інструментом якісного покращення співробітництва поліції і громадськості, дійсна перспектива підвищення ефективності роботи поліції. Впровадження в роботу правоохоронних органів моделей діяльності поліції зарубіжних країн по використанню консультативного механізму та співпраці з населенням у справі охорони громадського порядку є необхідністю теперішнього часу.

МЕТОДОЛОГІЧНІ ТА КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ У СОЦІАЛЬНИХ БЕЗПЕКОВИХ СИСТЕМАХ МІСЦЕВОГО РІВНЯ (НА ПРИКЛАДІ СИСТЕМИ ПРИКОРДОННОЇ БЕЗПЕКИ)

Д. А. Купрієнко

Результати аналізу нормативно-правових, інформаційно-аналітичних, наукових та навчально-методичних джерел свідчать про значне підвищення ваги іррегулярної компоненти при веденні сучасних воєн і збройних конфліктів, особливо, гібридного характеру. Військова агресія маскується під різні форми партизанських і повстанських рухів, а також терористичних дій для повалення легітимної влади й режимів, які не влаштовують противника.

Спектр способів формування додаткових сил та сприятливого організаційного середовища для дій агресора або злочинних угруповань різного масштабу досить широкий: починаючи від вербування пособницької бази (інформаторів, переправників, провідників тощо), і аж до впровадження злочинної агентури у різні органи та гілки влади з послідуючою побудовою мережі прибічників своїх ідей. Зокрема, в умовах відсутності цілеспрямованих комплексних впливів державних органів щодо формування психологічної стійкості та інтегрітету суспільства місцевого населення, значною є ймовірність його самоорганізації в інтересах, які не збігаються з державними. Зазначене вкрай негативно впливає на гарантування національної і міжнародної безпеки – спотворює та руйнує їхні системи.

Методологічні основи протидії інформаційним загрозам у соціальних безпекових системах місцевого рівня представлені взаємопов’язаними моделями і методами теорій стабільності систем, синергетики, мотивації особистості. На базі цієї методології запропоновано концептуальні основи протидії інформаційним загрозам, які відображають методичний підхід щодо формування психологічної стійкості та інтегрітету суспільства місцевого населення, комплексного управління його потенціалом в інтересах забезпечення безпеки.

ВЕРХОВЕНСТВО ПРАВА ПРИ ВЗАЄМОДІЇ ПОЛІЦІЇ З НАСЕЛЕННЯМ НА ЗАСАДАХ ПАРТНЕРСТВА. ПРИНЦИПИ ДІЯЛЬНОСТІ ПОЛІЦІЇ УКРАЇНИ

Я. В. Малик

Вагомість принципів діяльності поліції прослідковується в тому, що їм присвячено цілий другий розділ чинного Закону України «Про Національну

поліцію» від 02.07.2015 № 580-VIII, на відміну від правоохоронного органу, що функціонував раніше – міліції, принципи якого знайшли своє відображення в одній статті Закону України «Про міліцію», що на сьогоднішній день втратив чинність.

Другим розділом Закону України «Про Національну поліцію» передбачено сім статей, які відповідно визначають сім основних принципів діяльності поліції. Такі принципи, є взаємопов'язаними між собою.

Статтею 6 вказаного закону передбачено, що «поліція у своїй діяльності керується принципом верховенства права, відповідно до якого людина, її права та свободи визнаються найвищими цінностями та визначають зміст і спрямованість діяльності держави», а статтею 11 передбачається, що «діяльність поліції здійснюється в тісній співпраці та взаємодії з населенням, територіальними громадами та громадськими об'єднаннями на засадах партнерства і спрямована на задоволення їхніх потреб». Зазначені принципи тісно взаємопов'язані між собою, оскільки в кожному з них трактується головною цінністю це права людини, або населення.

Важливим для діяльності української поліції є принцип, що передбачає активну взаємодію поліцейських з місцевим населенням, гаслом якого фактично взято «поліція для громади і громада для поліції».

Залучення громадськості до правоохоронної діяльності є одним з факторів підвищення ефективності діяльності поліції, а таке залучення можливе тільки за попереднього дотримання принципу верховенства права поліцією і повинне супроводжуватись цим принципом при співпраці. Отже можна дійти висновку, що реалізація зазначених принципів будується саме на паритетних засадах.

ЗВ'ЯЗКИ З ГРОМАДСЬКІСТЮ, ЯК СИСТЕМА МАСОВОЇ КОМУНІКАЦІЇ НА ОСНОВІ ДОСВІДУ ЄВРОПЕЙСЬКИХ КРАЇН

І. Я. Табенська
С. М. Табенський

В наш час засоби масової інформації є невід'ємною складовою сучасного світу. Вся діяльність фахівців зі зв'язків з громадськістю спрямована, насамперед, на створення і утримання взаємовигідних відносин взаєморозуміння і співпраці в суспільстві, на вирішення кризових і конфліктних ситуацій цивілізованими і правовими методами з найменшими втратами для учасників подій. Сучасна наука, технічний прогрес, інформаційні технології, що еволюціонують соціально-суспільні зв'язки, інтеграційні процеси в економіці, міжнародна глобальна кооперація в політиці та суспільному житті і т.д., все це

сприяє нарощуванню досвіду і укоріненню традицій у зв’язках з громадськістю.

Але потрібно розуміти, що досвід набутий іншими країнами є безцінним уроком та прикладом для досягнення цілей та компромісів в комунікації між суспільством та безпосередньо органами МВС. Так, в Німеччині була створена програма для зменшення кількості злочинності в певних районах. Створювалися комунікативні групи, які складалися з громадян, різних професій, які мали спільні мету та інтерес. Якщо перенести цей досвід в нашу країну, то враховуючи ситуацію в країні, в комунікативну групу можуть увійти як дільничий, так і директори навчальних закладів, голови ОСББ, ЖЕК, активісти громадських організацій. Вирішуючи спільні проблеми певної місцевості, ця комунікативна група може не тільки покращити криміногенну ситуацію району, а й знайти причину безпосереднього її прояву для подальшого знищення.

Е. Л. Бернейз сказав, що це: «...творча сила, за допомогою якої надається інформація, в результаті чого підвищується інтерес до основних і важливих питань життя, до соціального, економічного і політичного життя суспільства».

Досвід європейських країн у сфері зв’язків з громадськістю є соціальною наукою, яка дозволить аналізувати тенденції, передбачати їх наслідки, консультувати керівництво організацій і втілювати в життя заплановані програми дій, які служать інтересам як органів МВС, так і громадськості.

СЕКЦІЯ № 3. КРИЗОВІ КОМУНІКАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

ДО ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄДИНОЇ ДЕРЖАВНОЇ СИСТЕМИ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

С. А. Єременко

В умовах сьогодення особливого значення набуває здійснення ефективної інформаційної політики під час надзвичайних ситуацій техногенного, соціального та природного характеру. Забезпечення національної безпеки є невід'ємною функцією кожної держави, як суспільного утворення, що має гарантувати сприятливі умови для життя і продуктивної діяльності її громадян.

Особливістю інформаційного забезпечення цивільного захисту є те, що обсяг і характер інформації повинен відповідати покладеним на ці органи завданням. На основі своєчасного збору та всебічного аналізу інформації вповноважені органи мають можливість: глибоко вивчати стан техногенної та природної безпеки на конкретній території, об'єкті, у криміногенному середовищі; спланувати заходи реагування; внести корективи у розстановку сил і засобів; своєчасно прийняти управлінське та оперативно-тактичне рішення; правильно організувати взаємодію з іншими органами, задіяними у справі цивільного захисту.

Одним із пріоритетних напрямів безпекової політики України повинно стати підвищення безпеки та стійкості цивільного захисту по відношенню до усього спектру загроз і ризиків, оскільки саме критична інфраструктура забезпечує життєво важливі для населення, суспільства та держави послуги та функції, без яких неможливі їх безпечне існування та благополуччя, а також належний рівень національної безпеки. Мета інформаційної безпеки цивільного захисту полягає в забезпеченні постачання населенню, суспільству, бізнесу і державі життєво важливих товарів і послуг. Для виконання функцій держави необхідно гарантувати безперебійне стале функціонування об'єктів критичної інфраструктури у визначених режимах, мати спроможність запобігати руйнуванню чи завданню невиправної шкоди, припиненню функціонування або втраті контролю над об'єктами критичної інфраструктури.

ІНФОРМАЦІЙНА БЕЗПЕКА МВС УКРАЇНИ У ВИМІРІ ПОСИЛЕННЯ КОНТРРОЗВІДУВАЛЬНОГО РЕЖИМУ

О. В. Копан

Загострення соціально-політичної, криміногенної ситуації загрожує політичному устрою держави, державній безпеці України.

Проведення всього комплексу контррозвідувальних заходів, встановлення жорсткого контррозвідувального режиму є необхідними умовами протидії активності спецслужб іноземних держав. Це стає можливим у результаті їхньої діяльності по збору політичної, економічної, військової, науково-технічної інформації. Особливу загрозу представляють агентурні мережі військової розвідки, діяльність агентів іноземних спецслужб, їх негативний вплив на нормальне функціонування органів державної влади України, безпеку посадових осіб та об'єктів. Володіння розвідувальною інформацією надає їм можливість маніпулювати корумпованими посадовцями, впливати на суспільно небезпечну діяльність учасників організованих злочинних формувань, використовувати їх в якості конфідентів.

Президентом України підписано Указ № 310/2017, яким введено в дію рішення Ради національної безпеки і оборони України від 13 вересня 2017 року «Про Концепцію забезпечення контррозвідувального режиму в Україні».

Реалізація положень, що містяться в Концепції, передбачає організаційні форми, спрямовані на забезпечення ефективного функціонування механізму запобігання, своєчасного виявлення та попередження зовнішніх і внутрішніх загроз безпеці України, припинення розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, які їм сприяють, і причин їх виникнення.

Пошук джерел загроз, виявлення джерел небезпеки, стеження за джерелами загроз, оперативна перевірка джерел загроз, локалізація та нейтралізація можливих збитків безпеці, виявлення або припинення джерел можливих загроз є сутністю контррозвідувального режиму.

КРИЗОВІ АСПЕКТИ СОЦІАЛЬНОЇ ІННОВАЦІЙНОСТІ

А. О. Кудлай

Зростання інтенсивності трансакцій, поєднане з синдромом хронічної неадекватності, призводить до нового різновиду суспільної кризи – кризи інноваційності.

Сучасна цивілізація виробила власний механізм динамічного самовідтворення, що базується на феномені суспільної ідеї, яка через свою

утилітарність втратила статус соціальної інновації. Кризовий стан, породжений новим режимом продукування та реалізації суспільних ідей, знаходить своє вираження у двох видах патологій соціального інтелекту:

а) синдромі надцінних ідей;

б) ідейному ескапізмі.

Кризовий стан суспільства провокує гіперкреативність – надлишок інноваційних пропозицій, що викликає захисну реакцію колективної свідомості – когнітивний імунітет, який може виявлятися в надмірних реакціях (когнітивна алергія).

Разом зі зниженням соціальної компетентності у суспільстві втрачається базис соціальної організації – суспільна довіра. Зникає довіра не лише до іншого члена суспільства, але й до всього суспільства в цілому, а разом з тим – і до себе, до своєї здатності адекватно розуміти і діяти. Замінником такої довіри виступає довірливість до професійних комунікаторів – до ЗМІ.

Досить переконливою видається думка М. Кастельса про те, що сучасні медіа є «символічною тканиною нашого життя» і в цій своїй ролі «діють на свідомість і поведінку таким самим чином, як реальний досвід діє на сни, надаючи сирий матеріал, над яким працює наш мозок».

Висновок: взаємна детермінація мас-медіа і суспільних процесів, про яку говорить іспанський дослідник М. Кастельс, не лише створює ситуації «зворотного зв’язку між кривими дзеркалами», але й спричиняє небезпеку дедалі більшої віртуалізації суспільної комунікації, її закритості, втрати критичного зв’язку з дійсністю, а відтак – створення передумов для тотальної маніпуляції.

ПРОБЛЕМИ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ОКУПАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Ю. О. Левченко

Гібридна війна, розв’язана Російською Федерацією проти України, містить не тільки військову, політичну та соціально-економічну складову, але й ставить українську державу і суспільство перед складними викликами у сфері інформаційної політики. Не зважаючи на те, що відкрита форма україно-російського конфлікту триває вже більше трьох років, можна констатувати, що дотепер в Україні відсутня адекватна, дієва відповідь на широкомасштабну інформаційну війну.

Як відомо, складовими елементами інформаційної безпеки є як забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, так і захист від негативних інформаційних впливів, що у сукупності мають сприяти цілісності суспільства.

Очевидно, що, зважаючи на анексію Криму, на окупацію окремих

територій Донбасу, українська держава не має можливості повною мірою забезпечувати реалізацію зазначених складових інформаційної безпеки, що дає підстави для застосування щодо цієї ситуації терміну «інформаційна окупація».

Відтак, першочерговим завданням соціальних і державних інститутів має бути розробка термінових ефективних заходів щодо нейтралізації інформаційно-диверсійної діяльності Росії проти України та запобігання її подальшому розгортанню.

Рішення цієї комплексної проблеми дозволить як захистити інтереси суспільства і держави, так і сприяти реалізації права громадян на отримання всебічної та якісної інформації.

ЕКОЛОГІЧНІ АСПЕКТИ ГІБРИДНОЇ ВІЙНИ

Г. С. Поліщук

Застосування Російською Федерацією технологій гібридної війни проти України призвело до збройного конфлікту, що триває вже більше трьох років та зумовив виникнення чисельних додаткових соціальних і гуманітарних проблем.

Однією з найтрагічніших, але мало висвітлених у засобах масової інформації проблем, є багаторічне поступове нищення здоров’я людей, які знаходяться в регіоні проведення АТО та навколишнього середовища, зокрема руйнування цілісних природних ландшафтів, забруднення води, ґрунтів, атмосферного повітря, знищення біоресурсів.

Реальні загрози екологічній безпеці у регіоні оцінити важко, адже відсутня фактична можливість контролюючих органів об’єктивно оцінити шкоду, нанесену довкіллю. Водночас, очевидно, що чисельні випадки руйнування, пошкодження, виникнення пожеж на екологічно небезпечних підприємствах, а також величезна кількість відходів, небезпечних хімічних речовин, що використовуються у промисловості, в умовах відсутності контролю та можливостей ліквідації негативних наслідків екологічного забруднення, потенційно збільшують масштаби негативного впливу на довкілля з кожним днем.

Ситуація ускладнюється тим, що екологічні ефекти неможливо обмежити державними кордонами. В умовах глобалізації екологічна криза та реальна можливість екологічної катастрофи в окремому взятому регіоні не може залишатися замкнутою в її межах і розглядатися як приватна внутрішньодержавна проблема. Відтак, розв’язання наявної проблеми потребує як відповідного інформаційного забезпечення, так і узгоджених організаційних та правових дій на міждержавному рівні.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ПРАВА ЛЮДИНИ НА СПРАВЕДЛИВИЙ СУДОВИЙ РОЗГЛЯД

О. М. Маркевичус

Проголошення та закріплення у міжнародно-правових та нормативно-правових актах окремих держав права особи на судовий захист демонструє готовність міжнародної спільноти до ведення відкритого діалогу в цій сфері. Найбільша проблема реалізації права особи на судовий захист полягає у реальному забезпеченні процесу реалізації цього права. З огляду на специфічність соціального змісту право як система загальноприйнятних норм поведінки передбачає необхідність їхнього дотримання таким чином, щоб не виходити за межі визначених і санкціонованих державою моделей суспільних відносин.

Аналіз категорії «механізм реалізації права», призвів до розуміння категорії «право на справедливий судовий розгляд» у двох аспектах: як сукупність задекларованих норм, що регламентують порядок звернення особи до національних чи міжнародних судових інстанцій у процесі захисту своїх інтересів та як об’єктивний і невід’ємний елемент правовідносин, застосування якого особою відбувається за її бажанням та зумовлюється зовнішніми обставинами.

Відповідно до доктринально визначених критеріїв, механізм реалізації права на справедливий судовий розгляд доцільно розуміти як комплекс організаційних і матеріально-технічних засобів практичного виконання юридичних приписів та закріплюються в міжнародно-правових актах, що регулюють діяльність тієї чи іншої міжнародної установи (інституції) у сфері захисту прав і свобод особи.

Право на справедливий суд є суб’єктивним правом особи, яке забезпечує реалізацію інших її прав у разі їхнього невизнання, оспорювання або порушення іншими суб’єктами правовідносин, у тому числі державою в особі її органів та посадових осіб. Право на справедливий суд належить до процесуальних прав-гарантій, закріплених на національному та міжнародному рівнях, у забезпеченні яких держава і міжнародна спільнота відіграють важливу роль. [1, с. 181–184].

На думку О. В. Девятової, специфіка внутрішньодержавного механізму застосування загальновизнаних принципів та норм міжнародного права про права людини полягає в тому, що застосування таких норм відбувається впродовж трьох етапів.

На першому етапі загальновизнані принципи та норми щодо прав людини трансформуються в конституцію, на другому – конституційні норми конкретизуються в галузевому законодавстві, а на третьому – відбувається пряме застосування загальновизнаних принципів і норм, які юридично обов’язкові, але часто не враховані при конкретизації конституційних норм у галузевому законодавстві [2, с. 28–30].

Водночас слід звернути увагу на сукупність міжнародних механізмів реалізації права на справедливий судовий розгляд.

Зокрема, можна запропонувати такі критерії класифікації:

1) за етапами (стадіями) дії права: правоутворення, правотворчість, правореалізація;

2) за змістом окремих складових механізму реалізації права: соціальний, психологічний тощо.

Доцільність їхньої класифікації полягає в підвищенні ефективності їхнього застосування, оскільки аналіз кожного окремого елементу механізму реалізації права дає змогу точно виокремлювати найбільш проблемні складові процесу захисту особою своїх прав загалом.

Так, на основі викладеного вище можна виокремити декілька критеріїв, за якими ці механізми можна класифікувати. Це означає, що вони утворюють доволі складну і навіть громіздку систему, супроводжуючи кожен з етапів формування та реалізації міжнародно-правових норм. Сукупність міжнародних органів та інституцій у сфері захисту прав особи можна розділити на три типи:

– комітети або комісії, які провадять постійний моніторинг стану дотримання прав та свобод людини;

– інституції прямого втручання та реагування на порушення прав людини (інститути уповноважених у справах людини);

– судові інстанції.

Слід зауважити, що механізм реалізації права на справедливий судовий розгляд власне в інстанціях та в інших міжнародних установах відрізняється ступенем обов’язковості виконання рішень таких інстанцій державою або окремими державними органами, щодо яких було прийнято рішення про усунення порушень прав особи та їхнє відновлення. Міжнародні та регіональні судові інстанції є свого роду наддержавним продовженням судової системи країни, а отже, виконання їхніх рішень відбувається в рамках чинного національного виконавчого законодавства. Водночас рішення міжнародних судів – це конкретні приписи, реагування на які є обов’язковим, що передбачається відповідними конвенціями та деклараціями.

Відповідаючи на питання, яким чином механізм реалізації права на справедливий судовий розгляд стосується діяльності міжнародних несудових інстанцій, слід зазначити, що міжнародний механізм реалізації права на справедливий судовий розгляд закріплюється безпосередньо в Конвенції про захист прав людини і основоположних свобод 1950 року.

У розділі І Конвенції 1950 року декларуються права та свободи особи, в тому числі право на справедливий судовий розгляд, а в розділі ІІ закріплюється механізм реалізації такого права особи.

Розглядаючи міжнародний механізм реалізації права особи на справедливий судовий розгляд загалом, доходимо висновку, що реалізація такого права передбачає наявність п’яти етапів: декларація права, звернення до компетентного органу для захисту права або відновлення права особи, розгляд такого звернення, винесення вмотивованого рішення та виконання цього рішення. При цьому перший етап – декларація права – є необхідною та достатньою умовою для подальшої реалізації всіх інших етапів. Отже, доцільно більш детально проаналізувати загальну структуру міжнародного механізму реалізації права на справедливий судовий розгляд.

Так, першим його елементом є встановлення (закріплення) та легітимізація можливого способу реалізації особою права на справедливий судовий розгляд або на захист особою інших прав і свобод шляхом звернення до міжнародної судової інстанції.

Цей елемент передбачає не лише декларацію такого права особи в міжнародно-правовому акті, а й належним чином ратифікацію такого акта на національному рівні. Якщо держава не ратифікує такий акт, то особа буде фактично позбавлена можливості захищати свої права через міжнародні судові органи, оскільки виконання їхніх рішень не передбачатиметься в національному законодавстві. Таким чином, такі рішення, навіть якщо особа звернеться до міжнародної судової установи, будуть позбавлені дієвості.

Так, наприклад, Конвенція 1950 року ратифікована Верховною Радою України в 1997 році відповідним Законом України «Про ратифікацію Конвенції про захист прав людини і основоположних свобод 1950 року, Першого протоколу та протоколів № 2 ,4, 7 та 11 до Конвенції», згідно з яким Україна повністю визнає на своїй території дію ст. 25 Конвенції про захист прав людини і основоположних свобод 1950 року щодо визнання компетенції Європейської комісії з прав людини приймати від будь-якої особи, неурядової організації або групи осіб заяви на ім'я Генерального Секретаря Ради Європи про порушення Україною прав, викладених у Конвенції, та ст. 46 Конвенції про захист прав людини і основоположних свобод 1950 року щодо визнання обов'язковою і без укладення спеціальної угоди юрисдикцію Європейського суду з прав людини в усіх питаннях, що стосуються тлумачення і застосування Конвенції [4].

Щодо цього С. В. Шевчук зазначає, що кожна чинна правова норма має бути промульгована «сувереном правової системи», а її авторитет базуватись на авторитеті суверена. Саме тому судове рішення, зокрема ЄСПЛ, в якому подано офіційне тлумачення, сформульовано новий правовий принцип або судовий прецедент, не вважається формою права і обов'язкове тільки для сторін у справі, але через те, що стороною в справі, що розглядається в ЄСПЛ, є Україна, а Верховна Рада ратифікувала Конвенцію 1950 року, виконання рішення ЄСПЛ визначено як обов'язкове, а саме рішення – це умовне джерело права, оскільки є підставою для внесення відповідних змін до чинного національного законодавства [5, с. 47–52].

В цьому простежується правоустановчий елемент механізму реалізації права на справедливий судовий розгляд.

На етапі звернення особи до міжнародної судової інстанції вступає в дію одразу два елементи механізму реалізації права: правоустановчий та матеріально-технічний.

Перший уособлюється в закріпленні та гарантуванні особі права звернення до такої інстанції, встановленні форми та порядки подання звернень тощо. Відповідно другий елемент уособлюється через способи забезпечення процедури подання заяви. Від дієвості поєднання цих двох елементів напряму залежить оперативність та повнота реакції міжнародної судової інстанції на звернення особи. Йдеться насамперед про належність і відповідність форми та змісту заяви міжнародноправовим нормам, які передбачають можливість її подання, а також про забезпечення функціонування суду через інструмент

сплати судового збору.

Матеріально-технічний елемент аналізованого механізму є надзвичайно важливим для подальшого розгляду та вирішення проблемного питання, вказаного в заяві, оскільки міжнародні судові інстанції, як правило, відправляють правосуддя в класичний спосіб, так само, як і національні суди, але витрати, пов'язані з їхньою діяльністю, значно вищі.

Крім того, завантаженість міжнародних судових інстанцій більша, ніж національних, а тому важливими є деталізація та конкретизація вимог особи, що викладаються в заяві, їхня умотивованість тощо. Це дасть змогу скоротити проміжок часу, необхідний для попереднього розгляду заяви, та підвищити можливість її прийняття до розгляду безпосередньо в судовому порядку.

На етапі розгляду заяви особи та вирішення справи задіяні одразу два елементи: процесуальний та матеріально-технічний. Процесуальний є головним елементом механізму реалізації права на справедливий судовий розгляд, оскільки саме в процесі розгляду та вирішення справи відбувається безпосереднє відновлення порушених особою прав, а також розробляються заходи для уникнення в майбутньому подібних, порушених через усунення суперечностей або недоліків національного законодавства країни, щодо якої розглядається заява особи. Відповідно матеріально-технічний елемент забезпечує належний організаційний і технічний супровід процесу розгляду справи.

У процесі розгляду заяви міжнародна судова інстанція виконує також правотворчу функцію, оскільки в її рішеннях часто міститься припис органам держави щодо необхідності вжиття конкретних заходів із метою вдосконалення національного законодавства або підвищення ефективності діяльності судової системи чи системи правозахисних органів.

Логічним продовженням етапу розгляду заяви та вирішення справи є етап винесення рішень, а процесуального елементу механізму реалізації права на справедливий судовий розгляд – правотворчий елемент. Рішення будь-якої судової інстанції за суттю є джерелом права, оскільки імперативно визначають поведінку суб'єктів суспільних відносин. Проте може постати питання щодо допустимості використання такого рішення як прямого джерела права, тобто чи таке рішення має бути в певний спосіб легалізоване в національному законодавстві.

Останнім, але надзвичайно важливим елементом міжнародного механізму реалізації права на справедливий судовий розгляд, є правозастосовний або правореалізаційний акт. Йдеться про безпосереднє виконання рішень міжнародних судових інстанцій. Без такого виконання самі собою рішення є недоцільними, а процедури розгляду заяви та вирішення справи – марними [6, с. 51].

Виконання рішення є безпосереднім практичним втіленням процесу відстоювання особою своїх прав загалом. Лише в такий спосіб право може бути поновлене. Виконання рішень міжнародних судових установ, як і можливість звернення особи до них, має гарантуватися державою, а засоби та інструменти його виконання, закріплені у відповідних міжнародно-правових актах, мають бути належним чином імплементовані в законодавство конкретної держави.

Отже, сама собою реалізація права на справедливий судовий розгляд не гарантує відновлення порушених прав особи, а лише демонструє декларацію, умовне визнання такого права державою та міжнародними інституціями.

Отже, підсумовуючи викладене, приходимо до висновку, що право на справедливий судовий розгляд – своєрідна додаткова модель соціальної поведінки особи, яка об'єктивно існує, але реалізація котрої відбувається лише за певних умов [7, с. 201–202] – гарантування особі даного права паралельно із закріпленням відповідного механізму його реалізації, що на сьогодні є найбільш актуальним завданням не лише для України, а й для багатьох інших держав та міжнародних правозахисних чи судових інстанцій через відсутність єдиного методологічного підходу до визначення змісту такого механізму.

Таким чином, міжнародний механізм реалізації права на справедливий судовий розгляд є надзвичайно складним структурним втіленням закріпленого в міжнародному праві порядку відновлення порушених прав особи та сукупністю взаємопов'язаних елементів правоустановчого, процесуального, матеріально-технічного та правозастосовного характеру, послідовність яких уособлює процес вирішення справи та встановлення істини міжнародною судовою інстанцією.

Список літератури:

1. Прокопенко О.Б. Право на справедливий суд: концептуальний аналіз і практика реалізації [Текст]: моногр. / О. Б. Прокопенко; – Національний університет «Юридична академія України ім. Ярослава Мудрого». – Х. : ФІНН, 2011. – 247 с.
2. Девятова О. В. Решения Европейского суда по правам человека в механизме уголовно-процесуального регулирования [Текст] / О. В. Девятова; науч. ред. Л. Г. Татьянина. – М. : Юрлитинформ, 2010. – 200 с
3. Зайчук О. В. Загальна теорія держави і права: (основні поняття, категорії, правові конструкції та наукові концепції) : навч. посіб. / за ред. : О. В. Зайчука, Н. М. Оніщенко, О. Л. Копиленко. – К. : Юрінком інтер, 2008 – 400 с.
4. Шевчук С. Європейська конвенція про захист прав людини та основних свобод: практика застосування та принципи тлумачення у контексті сучасного українського право розуміння [Електронний ресурс] / С. Шевчук // Видання Української правничої фундації «Практика Європейського Суду з прав людини. Рішення. Коментарі» – Режим доступу : http://eurocourt.in.ua/Article.asp?AIdx=416.
5. Європейська конвенція з прав людини: основні положення, практика застосування, український контекст [Текст] / за ред. О. Л. Жуковської. – К. : ВІПОЛ, 2004. – 960 с.
6. Коруц У. Міжнародно-правовий механізм реалізації права на справедливий судовий розгляд. // Актуальні проблеми правознавства. Випуск 2. – 2016 р. – С. 46-51.
7. Касумова А. П. Міжнародно-правовий аспект реалізації права особи на скаргу [Текст] / А.П.Касумова // Вісник Київського національного університету імені Тараса Шевченка: юридичні науки. – 2011. –№ 88. – С. 83–89.

РЕЗОЛЮЦІЯ

Міжнародної науково-практичної конференції «Інформаційна безпека в умовах гібридної війни»

16-17 листопада 2017 року на базі Національної академії Державної прикордонної служби України імені Богдана Хмельницького проходила Міжнародна науково-практичної конференція «Інформаційна безпека в умовах гібридної війни».

Метою конференції стало обговорення стану інформаційної безпеки та перспектив розвитку комунікацій як невід'ємної частини управління в системі Міністерства внутрішніх справ України, що дозволяють спрогнозувати та реалізувати стратегічні цілі щодо інформування та впливу на цільові аудиторії в умовах гібридної війни. Конференція проходила у формі пленарного засідання.

Загалом у конференції взяли участь понад 150 науковців і практиків, керівників інформаційних служб апарату Міністерства внутрішніх справ, центральних органів виконавчої влади, діяльність яких спрямовується та координується Міністром внутрішніх справ України, із них 9 докторів наук та 17 кандидатів наук.

Під час конференції розглянуто комплекс актуальних проблем управління інформаційною безпекою в сучасних умовах, за результатами якого учасники конференції констатували:

1. Застосування країною-агресором щодо України технологій гібридної війни, насамперед в інформаційній сфері, сформувало нові виклики і загрози інформаційній безпеці держави. Саме проти України та інших європейських країн Російська Федерація використовує найновіші технології інформаційно-психологічного впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності.

2. Комплексний характер викликів і загроз національній безпеці в інформаційній сфері потребує ефективної державної інформаційної політики та політики забезпечення інформаційної безпеки, узгодженої стратегії розвитку інформаційної галузі, консолідованих дій та спільного бачення засобів реагування на сучасні виклики і загрози, визначення інноваційних підходів до формування загальнодержавної системи захисту інформації з обмеженим доступом, забезпечення інформаційної та кібербезпеки України в умовах гібридної війни.

3. В Україні прийнято низку нормативно-правових актів стратегічного рівня з питань захисту національних інтересів в інформаційній сфері. Водночас актуальним залишається питання визначення шляхів їх реалізації в сучасних умовах.

Учасники конференції рекомендують:

у процесі реформування правоохоронних органів України чітко визначити їх компетенцію в інформаційному просторі з метою усунення паралелізму в діяльності різних правоохоронних підсистем, а також для організації їх діяльності відповідно до змін, які відбулися у суспільстві, впровадження європейських стандартів, нової системи оцінки ефективності роботи, раціоналізації як окремих служб, так і підрозділів;

розробити дієві механізми виявлення, фіксації, блокування та видалення з національного інформаційного простору, зокрема з українського сегмента мережі Інтернет, інформації та ресурсів, які створюють загрози життю і здоров'ю громадян України, пропагують війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

спрямувати зусилля суб'єктів центральних органів виконавчої влади, діяльність яких спрямовується та координується Міністром внутрішніх справ України на розвиток системи забезпечення інформаційного суверенітету, управління ризиками і новими можливостями в інформаційній сфері, розбудову інформаційно-комунікаційної інфраструктури, формування національного інформаційного простору, оптимізації взаємодії та комунікаційного процесу між державними органами й органами місцевого самоврядування та споживачами інформаційної продукції і послуг;

продовжити заходи щодо впровадження стратегічних комунікацій як скоординованого і належного використання комунікативних можливостей правоохоронних органів, спрямованих на реалізацію цілей України;

сприяти організації спільних заходів з громадськістю, засобами масової інформації, громадянським ініціативам, спрямованим на захист прав людини та зміцнення законності;

удосконалити комплекс заходів із протидії негативним інформаційним впливам, донесення оперативної, достовірної й об'єктивної інформації про події в Україні до міжнародної спільноти та громадян України, розробки та впровадження програм медіаосвіти населення;

забезпечити наповнення інформаційного простору України національним продуктом, здатним конкурувати із зарубіжними аналогами; сприяти розробці та впровадженню вітчизняних засобів обробки й передачі інформації та програмного забезпечення;

вжити необхідних заходів щодо захисту інформації з обмеженим доступом, насамперед державної таємниці та персональних даних, що обробляються в єдиних державних реєстрах та інших інформаційних системах і базах даних;

продовжити розбудову системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямів з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці;

забезпечити активне залучення наукового експертного середовища до розробки та опрацювання проектів нормативно-правових актів в інформаційній сфері;

модернізувати комплексну систему підготовки та перепідготовки фахівців з інформаційної та кібернетичної безпеки для центральних органів виконавчої влади, діяльність яких спрямовується та координується Міністром внутрішніх справ України з урахуванням досвіду проведення АТО та кращих практик зарубіжних країн;

запровадити програми, спрямовані на стимулювання участі молодих учених, курсантів та студентів у наукових дослідженнях із проблем управління інформаційною безпекою держави;

сприяти розвитку та активізації міжнародного співробітництва з питань протидії негативним інформаційно-психологічним впливам та кібернетичній злочинності.

ВІДОМОСТІ ПРО АВТОРІВ

Андреєв Дмитро Володимирович – доктор юридичних наук, доцент
Національна академія внутрішніх справ, м. Київ.

Андрощук Олександр Степанович – доктор технічних наук, професор
Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький.

Андрощук Олена Юріївна – кандидат психологічних наук, старший науковий співробітник
Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький.

Біленчук Петро Дмитрович – кандидат юридичних наук, доцент
Київський університет права Національної академії наук України, м. Київ.

Бурак Марія Василівна – кандидат юридичних наук
Національна академія внутрішніх справ, м. Київ.

Бутенко Володимир Анатолійович – заслужений журналіст України
журнал «Енергозбереження Поділля» Фонду наукового і економічного розвитку «Наука і Життя», м. Хмельницький.

Грицяк Наталя Вітіславна – заслужений діяч науки і техніки України, доктор наук з державного управління, професор
Національна академія державного управління при Президентові України, м. Київ.

Дем'янюк Юрій Анатолійович – кандидат педагогічних наук, доцент
Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький.

Єременко Сергій Анатолійович – кандидат технічних наук, доцент
Інститут з навчальної та методичної роботи Інституту державного управління у сфері цивільного захисту.

Іляшко Олександр Олександрович – кандидат юридичних наук
Навчально-науковий гуманітарний інститут Таврійського національного університету імені В. І. Вернадського, м. Київ.

Калайда Ангеліна Василівна
Національна академія внутрішніх справ, м. Київ.

Катеринчук Іван Степанович – доктор технічних наук, професор
Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький.

Копан Олексій Володимирович – доктор юридичних наук, професор
Національна академія внутрішніх справ, м. Київ.

Корчев Володимир Борисович – кандидат військових наук, старший науковий співробітник
Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький.

Кудлай Аліна Олександрівна
Національна академія внутрішніх справ, м. Київ.
Кулик Володимир Миколайович – кандидат технічних наук, доцент
заступник директора
Філія Донецького національного університету імені Василя Стуса «ДонНУ-Поділля», м. Хмельницький.
Купрієнко Дмитро Анатолійович – доктор військових наук, доцент
Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький.
Левченко Юрій Олександрович – кандидат юридичних наук, доцент
Національна академія внутрішніх справ, м. Київ.
Малик Ярослав Васильович
Національна академія внутрішніх справ, м. Київ.
Маркевичус О. М.
Донецький національний університет імені Василя Стуса.
Нічепорук Андрій Олександрович
Хмельницький національний університет, м. Хмельницький.
Поліщук Геннадій Сергійович – кандидат юридичних наук, доцент
Національна академія внутрішніх справ, м. Київ.
Савенко Олег Станіславович – кандидат технічних наук, доцент
Хмельницький національний університет, м. Хмельницький.
Ставицький Олег Миколайович – доктор педагогічних наук, доцент
Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький.
Табенська Ілона Ярославівна
Управління патрульної поліції у м. Хмельницькому.
Табенський Сергій Миколайович
Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький.

ЗМІСТ

СЕКЦІЯ № 3. КРИЗОВІ КОМУНІКАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ