Збірник наукових праць науково-практичної конференції професорсько-викладацького складу Полтавської державної аграрної академії за підсумками науково-дослідної роботи в 2018 році (м. Полтава, 16-17 травня 2019 року). – Полтава: РВВ ПДАА, 2019. – 309 с.

АНАЛІЗ ЗАГРОЗ В ІНФОРМАЦІЙНІЙ СФЕРІ ДЕРЖАВИ

Івко С.О.
кандидат технічних наук
Черноног О.О.
офіцер Генерального Штабу Збройних Сил України
Копішинська О.П.
кандидат фізико-математичних наук, доцент

Стрімкий розвиток інформаційних технологій сьогодення та засобів масової інформації, на їх основі, дав початок появі нових технологій впливу на вирішення міждержавних конфліктів. Розвиток інформаційно-комунікаційних технологій надає можливість використовувати їх для вирішення політичних чи соціокультурних завдань завдяки прихованого впливу на підсвідомість людей та масштабного маніпулювання суспільною думкою. Це призвело до появи нових форм і методів, завдяки яким світові держави намагаються досягти своїх зовнішньополітичних цілей і владнати міждержавні розбіжності. Суть використання даних методів полягає в зміщенні центру зусиль з фізичного знищення супротивника в рамках масштабної війни до вживання засобів «м'якої сили» проти країни-супротивника з метою дезінтеграції та зміни її керівництва, включення до сфери свого впливу.

Таким чином, перехід до інформаційного суспільства обернувся для людства тотальною катастрофою, оскільки гібридне протистояння, породжене цим

суспільством, є дієвим інструментом політики, а його розгортання означає існування однієї держави ціною виключення іншої.

Протидія держави деструктивному впливу на інформаційному просторі є задачею з багатьма невідомими тому що інформація циркулює сучасними інформаційними каналами практично вільно, незважаючи на обмеження владних структур (не беручі до уваги тоталітарні та диктаторські режими) у центрі уваги яких контроль над інформаційними потоками. Достеменно підтверджено, що контролюючі інформаційні потоки можна нівелювати на виході негативну або небезпечну інформацію, яка в процесі її поширення набуде протилежного значення. Коли збільшується обсяг інформації, що вільно циркулює, на перше місце висувається приховування та дозування інформації [1].

Ефективне поводження з інформацією надасть можливість змінити на свою користь навіть ті інформаційні потоки, які на перший погляд невигідні. Таким чином, потрібен в першу чергу на просторовий контроль, а інформаційний. Отже, отримати перевагу у гібридному протистоянні можливо тільки засобами ефективних і стрімких інформаційних технологій, які будуть адаптовані до власних умов та цілей.

Проведення аналізу впливу, яку здійснює РФ у межах довготривалої інформаційної кампанії проти України, дає змогу виокремити основні напрями та методи здійснення заходів, що зачіпають основні сфери національної безпеки України та становлять загрозу національним інтересам у:

зовнішньополітичній сфері – перешкоджання євроінтеграції України у спосіб формування упередженого ставлення світової спільноти до української влади;

внутрішньополітичній сфері – формування образу ворога – українця серед російськомовних громадян України та росіян;

сфері державної безпеки – посягання на державний суверенітет і територіальну цілісність України у спосіб порушення питань про приналежність АР Крим;

воєнній сфері – витіснення України зі світового ринку зброї у спосіб низької якості української військової техніки тощо;

економічній сфері – перешкоджання реалізації та дискредитація здійснених заходів Україною щодо зниження енергетичної залежності від РФ;

соціальній та гуманітарній сферах – протидія переосмисленню власної історичної спадщини, нівелювання українських культурних цінностей, ставлення під сумнів права української нації на самовизначення й утворення національної держави.

Аналіз негативних інформаційно-психологічних впливів, які здійснює РФ на Україну, вказує на їх плановість, системність і координованість на найвищому державному рівні.

З метою протидії вказаним факторам, в інформаційному просторі, та з урахуванням вимог [2], до основних напрямів удосконалення засад державної політики інформаційної безпеки необхідно віднести:

забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії;

створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них [3];

протидію інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей;

створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики демократичних держав.

Список використаних джерел

1. Пузиренко О.Г., Івко С.О., Лаврут О.О. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем // Системи обробки інформації. 2014.- Вип.8 (124) С. 128-134.

2. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України" № 240/2016 від 06.06.2016: [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/240/2016/page.

3. Пузиренко О.Г., Івко С.О., Лаврут О.О. Напрям вдосконалення нормативно-правового забезпечення системи захисту інформації Збройних Сил України // Науково-практична конференція "Наукове супроводження службово-бойової діяльності сил охорони правопорядку та військових формувань" НА НГ України. 2014.- С.57.