Черноног О.О.
ГУЗІС ГШ ЗСУ
Івко С.О., к.т.н.
ВІТІ

АНАЛІЗ ЗАГРОЗ В ІНФОРМАЦІЙНІЙ СФЕРІ ЯК ЕЛЕМЕНТ ПРОТИДІЇ «ГІБРИДНІЙ ВІЙНІ» В УКРАЇНІ

Глобальний розвиток інформаційних технологій та засобів масової комунікації дав початок появі нових технологій впливу на вирішення різноманітних конфліктів. Розвиток інформаційного суспільства дозволяє використовувати для вирішення політичних чи соціокультурних завдань можливості прихованого впливу на підсвідомість людей та масштабного маніпулювання суспільною думкою. Це призвело до появи нових форм і методів, завдяки яким провідні держави намагаються досягти своїх зовнішньополітичних цілей і владнати міждержавні розбіжності. На зміну суто військового аспекту війни приходять так звані «гібридні війни». Новий спосіб має суто прихований характер і використовується для досягнення цілей у політичній, економічній, інформаційній і соціальній сфері. Суть використання даного методу полягає в зміщенні центру зусиль з фізичного знищення противника 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.

Росія веде проти України «гібридну війну», в якій широко використовується інформаційний чинник, що є не менш важливим, ніж військовий. Зазначене стало можливим за рахунок недосконалості державної політики України у сфері інформаційної безпеки.

Проведення аналізу „гібридної війни”, 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, а також виробити ефективні методи протидії.

З метою протидії агресії Росії в інформаційному просторі, на основі отриманого аналізу та з урахуванням вимог Стратегії національної безпеки України, попередньо до основних напрямів удосконалення засад державної політики інформаційної безпеки у воєнній сфері в умовах „гібридної війни” пропонується:

-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;

-протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства;

-виявлення суб’єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

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

Важливим фактором в умовах інформаційної війни є підготовка та ведення інформаційних операцій. Тому авторами запропоновані деякі підходи до ведення інформаційної операції, розвиток яких доцільно віднести до основного напряму удосконалення засад державної політики інформаційної безпеки у воєнній сфері в умовах „гібридної війни”.