У сучасному світі традиційні концепції ведення війни набувають суттєвих змін. Стратегії ведення війни на знищення уходить в минуле, сьогодні, їм на зміну приходять концепції непрямих дій, гібридної війни, стратегічного паралічу тощо. В даних концепціях виділяють три основні сфери ведення війни: фізична, ментальна та моральна. В умовах глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень національних інтересів держав стає інформаційний простір. Сучасні інформаційні технології дають змогу використовувати власні інтереси без застосування воєнної сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не володіє дієвою системою захисту від загрозливих негативних впливів інформаційної атаки.

Досвід провідних країн світу показує прогрес у формуванні координуючих органів, які контролюють створення та застосування інформаційної зброї, забезпечення інформаційної безпеки суверенітету своєї держави, приділяють значну увагу розробці юридичної бази у сфері забезпечення інформаційної безпеки. Значна увага приділяється розробці питань інформаційно-психологічного впливу. Експертні оцінки фахівців НАТО, найбільш розвинені країни світу в найближчі два-три роки дістануть можливість вести повномасштабні війни в інформаційній сфері з використанням сучасних інформаційних технологій.

Застосування Російською Федерацією технологій гібридної війни проти України поставила перед нашою державою нові виклики у сфері інформаційної безпеки.

Актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

- здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, розпалювання міжетнічних конфліктів в державі;
- поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні;
- використання державою-агресором спеціальних інформаційних прийомів в інших державах з метою створення негативного іміджу України у світі;
- спотворення та домінування інформації країни-агресора на тимчасово-окупованих територіях тощо.

Антиукраїнська пропаганда, відверті фейки, постановчі новинні сюжети, які поширює російські медіа та соцмережі, зумовило необхідність розробки сучасної нормативно-правової бази для ведення інформаційної боротьби.

В Україні концептуальним документом щодо протидії російським інформаційним загрозам стала Доктрина інформаційної безпеки, ухвалена Радою національної безпеки та оборони у грудні 2016 р. і введена в дію Указом Президента Петра Порошенка 25 лютого 2017 року. Доктрина базується на принципах додержання прав і свобод людини і громадянина, поваги до гідності особи, захисту законних інтересів суспільства і держави, забезпечення суверенітету і територіальної цілісності України. Важливі терміни у Доктрині:

Стратегічні комунікації - скоординоване і належне використання комунікативних можливостей держави – публічної демократії, 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.

Доктрина інформаційної безпеки України визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері.

Державна політика в інформаційні сфері спрямована на:

1. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

- створення інтегрованої системи оцінки інформаційної загрози та оперативне реагування на неї;

- своєчасне виявлення, фіксація, блокування та видалення з інформаційного простору держави інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, насилля, національну та міжетнічну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, містить пропаганду комуністичного чи нацистського режиму та їх символіку;

- захист технологічної інфраструктури, регулювання роботи телекомунікацій, телерадіоорганізацій, поліграфічних видавництв, засобів масової інформації, радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед населення та війська держави;

- заборони роботи приймально-передавальних радіостанцій особистого та колективного користування і передачі інформації через комп'ютерні мережі в умовах запровадження правового режиму воєнного стану;

- врахувати практику держав-членів НАТО щодо створення структур, які відповідатимуть за інформаційно-психологічну безпеку, передусім у Збройних Силах України;

- забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах і тимчасово окупованих територіях;

- створення законодавчих механізмів для боротьби з дезінформацією та деструктивною пропагандою з боку Російської Федерації;

- зміцнення сектору безпеки і оборони протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності, підрив обороноздатності України, загострення суспільно-політичної ситуації;

- виявлення та притягнення до відповідальності суб'єктів українського інформаційного простору, що створені або використовуються державою-агресором для ведення інформаційної війни проти України з метою унеможливлення їхньої підривної діяльності.

2. ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ І РОЗВИТКУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ, А ТАКОЖ КОНСТИТУЦІЙНОГО ПРАВА ГРОМАДЯН НА ІНФОРМАЦІЮ

- пропагування цінностей свободи, демократії, патріотизму, національній єдності;

- задоволення потреб населення тимчасово окупованих територій в об'єктивній, оперативній і достовірній інформації.

3. ВІДКРИТІСТЬ ТА ПРОЗОРІСТЬ ДЕРЖАВИ ПЕРЕД ГРОМАДЯНИНОМ

- сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних

- інформування громадян України про діяльність органів державної влади.

4. ФОРМУВАННЯ ПОЗИТИВНОГО МІЖНАРОДНОГО ІМІДЖУ УКРАЇНИ

- розвиток публічної дипломатії, у тому числі культурної та цифрової;

- систематичний моніторинг пропаганди держави-агресора, розроблення та оперативна реалізація адекватних заходів протидії.

м. Чернівці, 2017

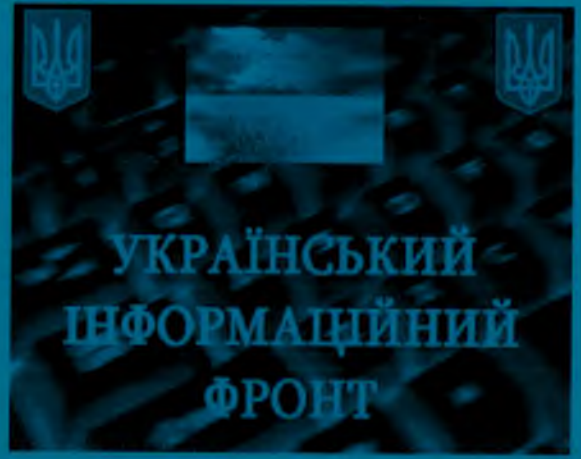
Управління реєстрації нормативно-правових актів, правової роботи та правової освіти Головного територіального управління юстиції у Чернівецькій області

ЮРИДИЧНА ПАМ'ЯТКА

на тему:

ДОКТРИНА інформаційної безпеки

ЗАХИСТ ІНФОРМАЦІЙНОГО ПРОСТОРУ ЗАКОНОДАВСТВОМ УКРАЇНИ



м. Чернівці,
2017 рік