ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут міжнародних економічних відносин

ім. Б.Д. Гаврилишина

КАФЕДРА МІЖНАРОДНИХ ЕКОНОМІЧНИХ ВІДНОСИН

МІЖДИСЦИПЛІНАРНА КУРСОВА РОБОТА

на тему:

«ІНФОРМАЦІЙНІ ВІЙНИ СУЧАСНОСТІ ТА ЇХ ВПЛИВ НА НАЦІОНАЛЬНИЙ СУВЕРЕНІТЕТ»

Студента 4 курсу групи МІ-41
Галузі знань
0302 Міжнародні відносини
Напряму підготовки
6.030204 Міжнародна інформація
Трофимчука А. А.

Керівник к. екон. н., доцент Дем'янюк О. Б.

Національна шкала _____

Кількість балів: _____Оцінка: ECTS _____

Члени комісії _____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали

Тернопіль - 2017

ЗМІСТ

ВСТУП

Актуальність теми. З приходом ери інформаційних технологій людству довелося зіткнутися з безліччю проблем. Однією з таких проблем постала загроза інформаційній безпеці держав та її громадян зокрема. На сьогодні, у світі і досі не існує ефективної системи захисту сфери інформації. В умовах максимальної інформатизації суспільства, жодна держава не може почуватися у безпеці, адже її громадяни у будь-який момент можуть піддатися впливу ворожої інформаційної атаки. Відомо, що у наш час чимало держав розглядають інформаційну війну як ефективний інструмент реалізації власної зовнішньої політики. До таких країн можна віднести і Україну, яка за виняткових обставин вимушена була розпочати ведення інформаційної війни проти Російської Федерації.

На сьогоднішній день традиційні концепції ведення війни набувають глибоких змін. Йдуть в минуле стратегії ведення війни на виснаження та знищення. Їм на зміну приходять концепції непрямих дій, паралельної війни, стратегічного паралічу та інші, які враховують нові фактори уразливості сторін. В цих концепціях виділяються три сфери ведення війни: фізична, ментальна і моральна. В цих умовах інформаційне протиборство набуває нової форми боротьби сторін, у якій використовуються спеціальні засоби, що впливають на інформаційне середовище і психологічний стан противника і захищають свої інформаційні ресурси і особовий склад в інтересах досягнення стратегічних цілей воєнного конфлікту. Дана тенденція є однією з найголовніших у сучасній збройній боротьбі. Інформаційне протиборство вже стало основним змістом воєнних конфліктів, як в період їх підготовки, так і в ході їх ведення.

Інформаційно-психологічна війна здатна негативно впливати на різні процеси всередині суспільства на всіх рівнях у кожній країні чи регіоні. У сучасному світі іноді достатньо керувати засобами масової інформації (далі – ЗМІ) задля управління величезними масами людей (яскравими прикладом служать події «арабської весни»). Тому у даному дослідженні порушено та

розглянуто питання державної протидії операціям інформаційно-психологічної війни.

Наявна ще одна проблема, яка розглянута в дослідженні: цілеспрямований інформаційно-психологічний вплив на людину. Цей вплив є різновидом соціальних відносин, у яких таїться надзвичайна небезпека, і вона потребує більш детального розгляду, і цим зумовлює актуальність дослідження.

Дослідженням проблеми інформаційних війн займаються такі вчені, як С. Гріняєв, О. Калиновський, А. Крутських, І. Панарін, Г. Почепцов, М. Лібікі, Е. Тоффлер, Г. Кіссінджер.

Мета роботи - дослідити вплив інформаційної війни на основні сфери функціонування держави для зміцнення її безпеки та суверенітету.

Для досягнення поставленої мети потрібно розглянути такі *завдання*:

- дослідити сутність та поняття інформаційної війни;
- яку небезпеку несе інформаційна війна для суверенітету країн;
- розглянути стратегії ведення інформаційної війни у сучасному світі;
- проаналізувати інформаційне протистояння України та РФ.

Об'єкт дослідження - інформаційне суспільство, як основа виникнення інформаційних конфліктів.

Предмет дослідження - ведення інформаційної війни в умовах інформаційного суспільства.

Практичне значення дослідження необхібне для управлінської еліти держави, так і для її населення, з метою захисту власного інформаційного простору та відстоювання власних позицій у глобальному інформаційному просторі.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ СФЕРИ ІНФОРМАЦІЙНИХ ВІЙН

1.1. Інформаційна війна та її сутність.

Аналізуючи історію людства, а зокрема історію війн між народами та їх державами, можна виявити, що інформаційна війна існувала завжди. Звичайно, вона не набувала таких масштабів як сьогодні, однак значно впливала на перебіг того чи іншого військового конфлікту.

З завершенням технологічної революції наше життя заполонили інформаційні системи. «Інформаційна ера» подарувала військово-промисловому комплексу країн небачені досі можливості: генерали негайно отримують інформацію про перебіг того чи іншого конфлікту і можуть миттєво реагувати на ситуацію, що склалася. Разом з цим, якість інформації значно покращилася, що дозволило перешкоджати маніпулюванню даними зі сторони супротивника. Таким чином, достовірність інформації є основною зброєю та силою у інформаційній війні.

Сьогодні Україна стала відкритою в інформаційному відношенні державою, уже сьогодні вона підключилась до Глобальної інформаційної інфраструктури (системи Інтернет, Глобалстар, GSM та інші), володіє замкнутими інформаційними системами низького рівня. Вказане робить Україну особливо вразливою до інформаційної зброї. Тому створення та безперервне вдосконалення систем та засобів захисту інформаційної інфраструктури України, створення оборонної інформаційної інфраструктури, є першочерговим завданням для сучасного уряду, вирішення якого забезпечить національну безпеку України.

Перш ніж серйозно аналізувати різні визначення інформаційної війни, відзначимо її важливу властивість: ведення інформаційної війни не буває випадковим чи відособленим, а передбачає узгоджену діяльність із використанням інформації, як зброї для ведення бойових дій як на реальному полі бою, так і у економічній, політичній, соціальній сферах.

Тож у ролі основного і найбільш загального визначення ІВ запропонуємо таке:

Інформаційна війна - це всеосяжна цілісна стратегія, обумовлена зростанням значимості і цінності інформації у питаннях командування, управління та політики [3].

Поле дії інформаційних війн в такому визначенні можна виділити наступним чином [10, с 45-46]:

1) інфраструктура систем життєзабезпечення держави - телекомунікації, транспортні мережі, електростанції, банківські системи й т.п.;

2) промислове шпигунство - розкрадання патентованої інформації, спотворення або винищення особливо важливих даних, послуг; збір інформації розвідувального характеру про конкурентів і т.п.;

3) зламування особистих паролів VIP-персон, ідентифікаційних номерів, банківських рахунків, даних конфіденційного плану, виробництво дезінформації;

4) електронне втручання у процеси командування та управління військовими об'єктами і системами, "штабна війна", виведення з ладу мереж військових комунікацій;

5) всесвітня комп'ютерна мережа Інтернет, у якій, за деякими оцінками, діють 150.000 військових комп'ютерів, і 95% військових ліній зв'язку проходять по відкритим телефонним лініям.

Звичайно, який би зміст у поняття "інформаційна війна" не вкладався, воно зародилося серед військових і позначає, передусім, жорстку, рішучу і небезпечну діяльність, порівняну з реальними діями. Військові експерти, що сформулювали доктрину інформаційної війни, чітко уявляють собі окремі її межі: це штабна війна, електронна війна, психотропна війна, інформаційно-психологічна війна, кібернетична війна тощо.

Отже, інформаційна війна - це така форма конфлікту, у якій відбуваються прямі атаки на інформаційні системи супротивника[10].

До складових частин інформаційної війни відносять [5]:

1) психологічні операції. Використання інформації для порушення психологічного стану солдатів ворога (деморалізація);

2) електронна війна. Не дозволяє ворогу отримати точну інформацію;

3) дезінформація. Надає ворогу неправдиву інформацію про наші сили та наміри;

4) фізична руйнація. Метою є вплив на елементи інформаційних систем і виведення їх з технічної справності;

5) заходи для безпеки. Заходи, що мають на меті уникнення здобуття ворогом реальних даних про можливості і наміри;

6) прямі інформаційні атаки. Пряме спотворення інформації.

Мартін Лібікі – один із провідних теоретиків у галузі інформаційних війн – у своїй книзі «Що таке інформаційна війна?», визначає 7 форм інформаційної війни [9]:

- командно-управлінська (націлена на знищення каналів зв'язку між командуванням і виконавцями);
- розвідувальна (збір важливої і захист власної інформації);
- психологічна (пропаганда, інформаційна обробка населення, деморалізація);
- хакерська (диверсійні дії та атаки проти ворога шляхом створення спеціальних програм);
- економічна (інформаційна блокада й інформаційний імперіалізм);
- електронна (спрямована проти засобів електронних комунікацій – радіозв'язку, радарів, комп'ютерних мереж);
- кібервійна.

На думку Мартіна Лібікі «…спроби повною мірою зрозуміти всі грані поняття інформаційної війни схожі на зусилля сліпих зрозуміти, наприклад, природу слона: один, торкнувшись його ноги, каже, що це дерево, інший – на хвіст каже мотузка і т.д. Чи можна так одержати правильне уявлення?

Можливо, й немає слона, а є лише дерева і мотузки. Одні готові піднести під це поняття дуже багато, а інші – трактують виключно один аспект. Так само сприймаються й прояви інформаційні війни…» [9].

Тепер розглянемо визначення поняття «інформаційна зброя». Під інформаційною зброєю необхідно розуміти сукупність організаційних та організаційно-технічних впливів на інформаційні системи, системи автоматизованого та автоматичного керування, системи та мережі зв'язку, тощо, здійснених з використанням [6, 16]:

- систем та засобів знищення, викривлення, розкриття, крадіжки, створення хибної інформації;
- систем та засобів подолання систем захисту;
- засобів обмеження або розширення доступу до інформації та ресурсів законних користувачів;
- систем та засобів протидії та дезорганізації роботи технічних засобів, комп'ютерних систем;
- систем та засобів управління ресурсами інформаційних систем.

Аналіз досліджень проведених науковцями демонструє, що інформаційна зброя, створена в вигляді програмних або програмно-апаратних систем та засобів, може бути економічною, легко замаскованою під засоби захисту, може діяти анонімно без оголошення війни, володіючи в той же час такими властивостями як універсальність застосування, багатоваріантність побудови та використання, латентність та радикальність дії (у розумінні заподіяння максимальної шкоди) [4,6,8,16].

Основними складовими захищеного інформаційного простору держави можуть бути [4]:

- національна інформаційна інфраструктура (НІІ) з відповідними показниками захищеності;
- національна оборонна інформаційна інфраструктура (НОІІ);

- елементи та засоби глобальної інформаційної інфраструктури (ГІІ).

Очевидно, що основними об’єктами інформаційної війни, по суті мішенню інформаційної зброї є і будуть НІІ та ГІІ. Під удар інформаційної зброї можуть потрапити виробництво, засоби масової інформації, зв’язок, силові відомства, транспорт та енергетика, наука та освіта, фінанси та інше. Але в першу чергу інформаційна зброя буде націлюватись на збільшення суперечок в економічній, політичній та ідеологічній областях держави-суперника. Ця зброя буде націлюватись на збройні сили, підприємства оборонного комплексу, силові структури відповідальні за безпеку держави. При цьому, найімовірніше, що найбільший розвиток та використання інформаційна зброя знайде в економічній області – шпигунство через електронні системи, знищення та підробка інформації, введення в оману та інше – реалії сьогоднішнього дня. В таких складних умовах вижити може тільки держава, яка створить і буде повсякчасно покращувати якість національної оборонної інформаційної інфраструктури.

На Рис.1.1. схематично відображено види інформаційної зброї, які використовуються вже сьогодні.

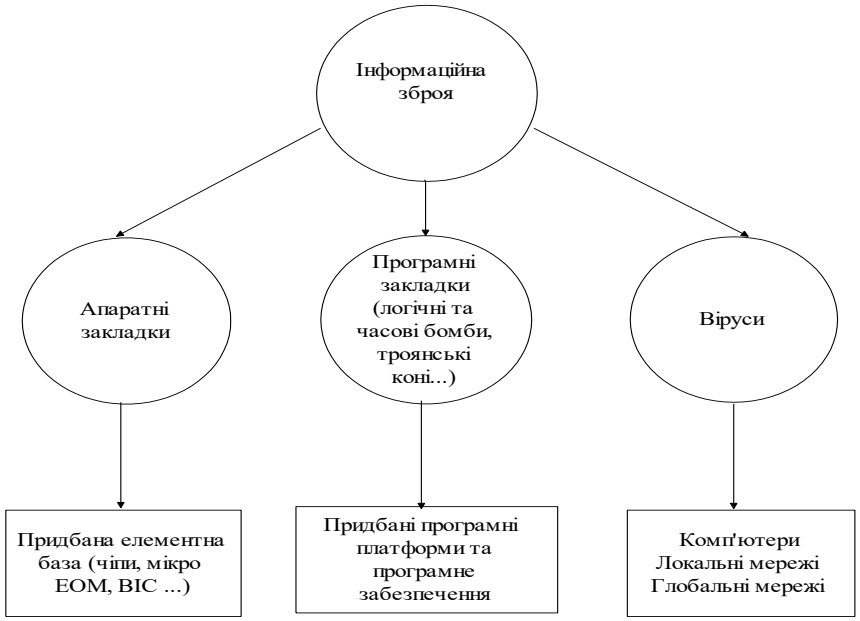

Рис. 1.1. Види інформаційної зброї

Примітка. Розроблено автором.

Приведемо приклад успішного використання інформаційної зброї. Таким прикладом послужить операція "Буря в пустелі" проведена США на Близькому Сході. Операція є досить вдалим прикладом психологічного впливу, коли американські військові, використовуючи "м'яку цензуру", фактично вилучили з інформаційного поля повідомлення, в яких виправдовувалась протилежна сторона. Окрім того, ця операція стала першою в історії війною в прямій телетрансляції. У даному випадку психологічний вплив здійснювався за допомогою висвітлення потрібної інформації у ЗМІ [15].

1.2. Особливості інформаційної безпеки на сучасному етапі розвитку суспільства.

Процеси, що відбуваються в сучасному суспільному житті, можна охарактеризувати як посилення ролі інформації як в суспільстві, так і в житті кожної людини зокрема. Інформація отримує реальне матеріально-енергетичне, соціально-економічне, політичне і вартісне вираження. За цих умов одним із першочергових завдань, що постають перед правовою державою, є вирішення суперечності між реально існуючими і зростаючими потребами особистості, суспільства і держави в якісних інформаційних ресурсах, продуктах та послугах і необхідністю забезпечення їх інформаційною безпекою, що спрямована на досягнення такого рівня духовного та інтелектуального потенціалів країни, який є достатнім для розвитку державності і соціального прогресу.

Визнання проблеми інформаційної безпеки на міжнародному рівні обумовлюється такими чинниками глобалізації [14, с.15]:

- у більшості розвинутих країн проводяться дослідження і розроблення нової інформаційної зброї, що дозволяє здійснювати безпосередній контроль над інформаційними ресурсами потенційного противника, а в необхідних випадках впливати на них. За даними аналітичних центрів США, розроблення такої зброї ведеться в 120-ти країнах

світу. У деяких країнах завершено розроблення засобів інформаційного протиборства з можливим противником як в умовах воєнних конфліктів різної інтенсивності, так і в мирний час на стратегічному, оперативному, тактичному рівнях. Практика міжнародних, регіональних та етнічних конфліктів виявила унікальність застосування інформаційної зброї для впливу на міжнародне співтовариство та для боротьби за геополітичні інтереси;

- кардинально змінилася оцінка доктрини інформаційної безпеки в цілому і позиції більшості країн світу, які усвідомили потенціал інформаційних загроз і необхідність створення відповідного міжнародного механізму для контролю інформаційного протиборства.

Політичні дискусії на Міжнародному семінарі з проблем інформаційної безпеки (Женева, 1999 р.), підтвердили актуальність проблеми та своєчасність її розгляду в рамках ООН. У визначенні підходів до її вирішення виявилися різні позиції, котрі відповідали стратегічним інтересам учасників дискусії.

Позиція розвинутих країн передбачала визнання проблеми міжнародної інформаційної безпеки як [14, с. 22]:

- гіпотетичного силового протистояння;
- перенесення концепції міжнародної інформаційної безпеки на регіональний або тематичний рівень;
- виділення з комплексної проблеми міжнародної інформаційної безпеки таких складових, як кримінальні та терористичні міжнародні інформаційні загрози і створення міжнародного механізму контролю подібних інформаційних злочинів.

Позиція країн, які не належать до західної моделі цивілізації, передбачала такі пропозиції [14, с. 23]

- встановлення міжнародно-правової норми про заборону застосування засобів впливу на інформаційні ресурси та інформаційний потенціал міжнародного, регіонального та національного призначення;

- створення спеціального Міжнародного суду з інформаційної злочинності;
- спільне розроблення технології глобального захисту від інформаційної агресії.

Концепція міжнародної інформаційної безпеки визначає критичні структури, які насамперед зазнають впливу в умовах інформаційного протиборства. Найбільш вразливими вважаються політична, суспільна, економічна, військова, науково-технологічна, духовна сфери життєдіяльності суспільства, а саме [6]:

- у політичній сфері інформаційна безпека стосується всіх елементів політичної структури держави та суспільства: структур підготовки та прийняття політичних рішень, структур управління місцевої та регіональної влади, структур виборчих систем, інформаційно-телекомунікаційних урядових систем спеціального призначення;
- для економічної сфери критичними вважаються системи загальноекономічного аналізу та прогнозування економічного розвитку, структури прийняття рішень та координації управлінських дій в економічній сфері, зокрема, в умовах надзвичайного стану, інфраструктури банківських мереж і систем, системи управління в критично важливих для функціонування держави структурах (енергетика, транспортні комунікації, телекомунікаційні та інформаційні мережі);
- у військовій сфері вразливими в умовах інформаційного протиборства вважаються інформаційні ресурси збройних сил, військово-промисловий комплекс, системи управління військами, системи контролю і постійного спостереження, канали надходження інформації стратегічного, оперативного, розвідувального характеру;
- глобальними загрозами в науково-технологічній сфері є феномен транскордонного переміщення інтелектуальних ресурсів, тобто вивезення інформації унікального науково-технологічного характеру на біологічних

носіях до міжнародних систем спостереження, аналізу і прогнозування тенденцій науково-технологічного розвитку в різних країнах з метою доступу до конфіденційних баз і банків даних; критичними для безпеки у сфері науки і технологій є структури накопичення науково-технічної інформації, інструкції та структури фундаментальних і прикладних досліджень, об’єкти інтелектуальної власності, ноу-хау;

- суспільна сфера є найбільш вразливою для інформаційних впливів, оскільки включає системи формування громадської думки, структури засобів масової комунікації, інформаційно-організаційні структури політичних партій, громадських рухів, національно-культурних та релігійних інституцій, структури забезпечення основних прав і свобод, плюралізму і незалежності виявлення поглядів, вільного обміну ідеями та інформацією;
- становище в духовній сфері стає критичним в умовах конфесійного протистояння, релігійного фанатизму, трансформації духовних ідеалів та морально-етичних цінностей. Так, проявом критичності ситуації в духовній сфері (Ірландія, Алжир, Ізраїль, Афганістан, Китай, Іран) на міжнародному рівні стала проблема, пов'язана з рішенням керівництва ісламського радикального руху «Талібан» (Афганістан), ІДІЛ (Сирія, Єгипет) про руйнування неісламських релігійних пам'яток, що внесені до глобальної культурної спадщини і перебувають під охороною ЮНЕСКО.

Доктрина інформаційної безпеки України спрямована на забезпечення необхідного рівня інформаційної безпеки України в конкретних умовах даного історичного періоду і є основою для формування державної політики у сфері інформаційної безпеки України [5].

Метою інформаційної політики держави має бути створення умов для:

- побудови в державі інформаційного суспільства як органічного сегмента глобального інформаційного співтовариства;
- забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури;
- впровадження новітніх інформаційних технологій;

- захисту національних моральних і культурних цінностей;
- забезпечення конституційних прав на вільний доступ до інформації [15].

Якщо Україна хоче стати незалежною державою, вийти на рівень європейських держав, то вже сьогодні необхідно вирішувати ряд проблем у галузі інформаційної безпеки. Головними з них, на наш погляд, є:

- створення системи підготовки та перепідготовки кадрів, включаючи кандидатів та докторів наук;
- організація та координація наукових та дослідно-конструкторських робіт в галузі інформаційної безпеки;
- створення національних стандартів та контролю якості діючих стандартів, включаючи криптографічні системи;
- розгортання національної конкурентоспроможної промислової бази в галузі захисту інформації;
- створення системи експертизи та сертифікації систем та засобів захисту інформації тощо.

РОЗДІЛ 2
ВПЛИВ ІНФОРМАЦІЙНОЇ ВІЙНИ НА НАЦІОНАЛЬНУ БЕЗПЕКУ

2.1. Інформаційна війна у XXI ст.

Інформаційна війна (далі - ІВ), ведеться не тільки в мережевому електронному просторі і охоплює не лише інтернет, але і закриті державні, військові, корпоративні та приватні мережі. Для ІВ властиві свої інструментарії, методи, стратегії і тактики ведення, закономірності ескалації, можливості попередження і т.п. ІВ тісно пов'язані з кібершпигунством, кіберзлочинністю і кібертероризмом (див. Додаток А). При цьому, слід зазначити, що так само як і в матеріальному світі, в електронному просторі всі ці феномени тісно переплетені і взаємодіють між собою. Ця взаємодія характерна як для взаємної переплетеності атакуючих суб'єктів, так і об'єктів, що піддаються атакам. Ці види злочинної поведінки використовують найчастіше схожі програмні засоби, мають подібні режими їх застосування, тощо. Є всі підстави вважати, що протягом найближчих двох-трьох років сформуються інструментарії та технології для електронних воєн третього типу, основа яких полягатиме в об'єднанні інформаційної та кібервійни. Йдеться про те, що в лабораторіях вже пройшли практичну апробацію апаратні і програмні засоби, що забезпечують прямий і зворотний зв'язок між змінами психіки (або як ще кажуть ідеального або суб'єктивного), спотворення реального світу, матеріальних об'єктів, їх систем, мереж і т.п. Перші публікації з цього приводу з'явилися в США і Росії в 2014 році. У них йдеться про псі-війни, нейровійни і т.п. Але це тема окремого дослідження.

Основною метою інформаційної війни є послаблення моральних та матеріальних сил супротивника та посилення власних; порушення обміну інформацією у опонента. Інформаційна війна включає заходи пропагандистського впливу на свідомість людини, що безпосередньо не призводять до війн в традиційному її розумінні, проте порушують державний

механізм управління. Це так звана прихована, латентна війна, наслідки якої призводять до руйнування держави.

У XXI столітті інформаційна війна являє собою одну з найважливіших проблем в міжнародних відносинах. Масштаби її впливу безперервно збільшуються. Однією з основних загроз є відсутність будь-яких заборон і обмежень в міжнародному праві щодо ведення інформаційної війни. Крім того, необхідно звернути увагу на той факт, що в локальних конфліктах вона поєднується з збройною агресією, що підкреслює необхідність регулювання даного явища на міжнародному законодавчому рівні [17].

У XXI столітті все більшого значення набуває виконавча влада, що здатна контролювати інформацію. Завдяки появі Інтернету було створено єдиний інформаційний простір, монополією на який на даний момент жодна держава не може володіти, але багато країн прагнуть до цього.

Згідно експерту в області інформаційних воєн, А.В. Манойло, можна виділити 3 основні політичні завдання інформаційної війни, а саме: зміна структури економічних, політичних, інформаційно-психологічних систем будь-якої держави у відповідність з інтересами того, хто здійснює інформаційну атаку; досягнення військово-політичної переваги на міжнародній арені; досягнення цілей інформаційно-психологічної експансії [11].

Інформаційна або Кібервійна, що сприймалася до останнього часу деякими політиками і аналітиками у всьому світі як якась екстравагантна тема для «дискурсу», набула в серпні 2013 року реальне втілення. Пов'язано це з документами, які виявилися доступними для журналістів і аналітиків, завдяки Едварду Сноудену. Йдеться зовсім не про програми Prism і XKeyskore, або тотальне прослуховування мобільних операторів, і навіть не про доступ АНБ до серверів Google, Microsoft, Facebook, Twitter, міжнародної мережі банківських транзакцій SWIFT, процесингових систем Visa, MasterCard і т.п. Найцікавішими і поки недостатньо оціненими стали документи в складі досьє Сноудена, що отримали назву - «файли чорного

бюджету американського розвідувального співтовариства». ЗМІ, та й експертне співтовариство обмежилися обговоренням наступальної кібероперації і «шалених» цифр: 500 млрд.доларів витрат на розвідку в США за 2001-2012 рр. Ці документи, опубліковані газетою Washington Post, дають величезний матеріал для по-справжньому серйозного аналізу.

На відміну від слайдів презентацій і мало кому цікавих списків IP-адрес, аналітики отримали в своє розпорядження безліч сухих бюджетних цифр і супроводжуючі їх пояснювальні документи, що бюрократичною мовою демонструють факти, зауваження та пропозиції, що стосуються справжніх, а не медійних секретів американської розвідки і армії. Аналіз цих документів дозволяє зробити висновок, що в світі вже ведеться неоголошена, великомасштабна цифрова або кібервійна. І тільки питання часу, коли в цій війні з'являться перші людські жертви.

Відомий американський аналітичний центр RAND Corp., у своєму дослідженні інформаційної війни у сучасному світі, охарактеризував стратегію ведення ІВ і виділив наступні її риси [3]:

- Низька вартість ресурсів: на відміну від традиційних технологій, зброї, розробка методів ведення війни за допомогою інформації не потребує значних фінансових ресурсів або потужної підтримки зі сторони держави. Інформаційні системи, експертизи та доступ до важливих мереж - ось все, що потрібно для початку розробки наступальних інформаційних дій.
- Розмитість кордонів: географічні кордони між країнами тепер лише на мапі. Зростаюча взаємодія в рамках інформаційної інфраструктури, дозволяє отримувати доступ до будь-якої інформаційної системи іншої країни. Яскравим прикладом може служити втручання російських хакерів у вибори Президента США-2016.
- Розширення ролі управління сприйняттям: нові технології, засновані на інформації можуть істотно збільшити масштаби обману. Наприклад, обробка зображень є маніпуляцією дійсності, що значно

ускладнює роботу уряду зі створення політичної підтримки ініціатив пов'язаних з безпекою.

- Нові можливості розвідки: вже сьогодні, завдяки ІТ, розвідка кожної країни поступово переходить на новий формат ведення своїх розвідувальних дій. Причому протистояти цьому практично неможливо: виявити під чиїм ім’ям ведеться робота в мережі є надзвичайно важким завданням.
- Відсутність договорів по веденню ІВ: на сьогодні, не існує жодної системи договорів, що попереджували би інформаційні бої між державами. Це відкриває величезні можливості для ведення бойових дій у мережевому просторі, для атак у кіберпросторі, для шпигунства і навіть тероризму. Особливо небезпечним залишається тероризм. Кожна країна залишається сам-на- сам у боротьбі з ним у інтернет-просторі. США та РФ одні з перших активно впроваджують технології по боротьбі з загрозою ІДІЛ, яка активно і небезпечно діють в кіберпросторі. Залишається сподіватися, що країни в рамках ООН таки зможуть дійти згоди і розпочати спільну координацію по боротьбі проти цих жахливих проявів інформаційної війни.
- Складність створення і підтримки коаліцій: звертаючи увагу на попередню рису ІВ, не менш важливим залишається питання як довго країни зможуть перебувати в стані коаліції проти світових інформаційних загроз. Загальновідомий факт, що США з одного боку та РФ і Китай з другого, перебувають в доволі напружених, часом войовничих відносинах. І кожна з цих країн сподівається отримати свою вигоду у інформаційних атаках на інфраструктуру свого опонента (-ів). Те, як вони дійдуть згоди у створенні нового мирного інформаційного простору залишається загадкою.

2.2. ЗМІ та інформаційна війна

Необхідно також відзначити роль ЗМІ у веденні інформаційно-психологічних кампаній, які надають пропагандистський вплив на інтелектуальний та емоційний аспекти життя суспільства. Засоби масової

інформації є головним засобом інформаційних воєн. Вони застосовують асиметричну інформацію (дезінформацію) в якості одного із способів впливу на населення. Це поняття отримано в результаті досліджень взаємин між інформацією та економікою експертами Гюльшах Башлар і Кетрін Тернер. У статті «Вплив засобів масової інформації на реконструкцію соціальної реальності за допомогою асиметричної інформації» Гюльшах Башлар пише, що концепція дезінформації - це концепція, розроблена в області економіки та інформаційних відносин [3]. У багатьох сферах життя інформація є асиметричною. Коли одна зі сторін володіє їй в більшій кількості, ніж інша, відбувається обмін асиметричною інформацією між ними.

ЗМІ часто збільшують інформаційну асиметрію в суспільстві, що можна спостерігати в основному в сфері новин. Дезінформація є цілеспрямованою і навмисною, пов'язаною з прагненням заплутати людей і ввести їх в оману. Поширення неправдивих відомостей в суспільстві включає в себе намір змусити громадян будь-якої держави повірити в недостовірну інформацію і прийняти невірні рішення. Дезінформація - це метод, який політично впливові групи використовують, щоб вплинути на громадську думку через ЗМІ. Таким чином, засоби масової інформації, володіючи асиметричною інформаційною перевагою, в будь-який момент можуть ввести в оману громадськість, дезінформуючи її, якщо в цьому є необхідність. Приведемо приклад маніпулювання свідомістю.

Рис. 2.1. Фейк у соцмережі

На Рис. 2.1. у лівій частині відображено скріншот посту одного з твіттер-акаунтів бойовиків ОРДЛО у 2014 р. Фото підписано як «Смерть в Україні», однак насправді фото було зроблено в 1995 році у Чечні фотографом Пітером Тернлі.

Отже, влада може генерувати реальність, представляючи інформацію у вигідному для неї світлі. Повний контроль над ЗМІ дає можливість формувати громадську думку в своїх інтересах. Таким чином, політичні, економічні інститути можуть всіляко маніпулювати суспільством за допомогою ЗМІ. Дезінформовані, необізнані в певних сферах і питаннях люди мають ризик здійснення несприятливого відбору інформації. Таким чином, засоби масової інформації можуть змінювати соціальну реальність і трансформувати її. Замість виявлення реальності, ЗМІ в більшості випадків приховують її.

РОЗДІЛ 3
ІНФОРМАЦІЙНА ВІЙНА ПРОТИ УКРАЇНИ

Політична криза, що наступила в Україні в кінці 2013 – початку 2014 рр. мала масу негативних наслідків. Найжахливішим її результатом стала маса людських жертв під час Майдану-2014. Однак, окрім внутрішніх проблем, Україні, що вступала в новий етап свого розвитку, довелося зіткнутися із проблемами зовнішніми. Вперше за 22 роки свого існування, країні довелося зіткнутися з однією з найнебезпечніших форм війни: інформаційною. Інформаційний тиск на Україну відбувався як зі сторони Заходу, так і пострадянських країн, однак основним супротивником у інформаційному протистоянні, що вже триває понад 3 роки стала РФ.

Росія розпочала використання просунутої форми гібридної війни в Україні з початку 2014 року, що в значній мірі опирається на елемент інформаційної війни, що називають «рефлексивний контроль».

Рефлексивний контроль є одним із трьох найбільш популярних методів інформаційної війни, розробка якого була розпочата ще в часи СРСР. Російські фахівці розглядають як мету дезорганізацію ворога, що в свою чергу веде до інформаційної переваги. Рефлексивний контроль супротивника полягає в тому, щоб противник прийняв правильне з точки зору комунікатора рішення, яке потрібно не супротивнику, а комунікатору. Американський аналітик Стів Тетем зазначає, що рефлексивне управління було використано в ситуації з псевдореферендумами в Криму. Зокрема, мова про використання хорошого розуміння трьох цільових аудиторій: російськомовної більшості Криму, української влади та міжнародної спільноти, особливо ЄС і НАТО. Було спрогнозовано їх можливу поведінку, що говорить про акцент саме на поведінці.

Москва використовувала цю техніку вміло, щоб переконати США і їхніх європейських союзників у своїй непричетності до внутрішніх хвилювань в Україні. Можна частково погодитися з тим, що ця модель ІВ принесла РФ певні успіхи на міжнародній арені: в основному, країни Заходу

залишаються нейтральними до конфлікту Україна-РФ. Захід повинен бути готовим до протистояння з рефлексивним методом ІВ і знайти способи боротьби з ним, якщо він хоче домогтися успіху в епоху інформаційних війн.

Рефлексивний метод і інформаційна війна Кремля в цілому, не є результатом яких-небудь теоретичних інновацій. Основні поняття та методика була розроблена ще в 70-х рр. в Радянському Союзі. Російські інформаційні операції в Україні не є новими, хоча й вони спрямовані на те, щоб створити саме таке враження.

Основними елементами рефлексивного методу ведення ІВ Росією проти України, на нашу думку є:

- заперечення військових операцій, аби приховати присутність російських сил на Донбасі, в тому числі відправки «зелених чоловічків» в Крим в уніформі без знаків відмінності;
- приховування реальної мети і завдань РФ в конфлікті всередині України;
- доведення законності дій Росії у міжнародних організаціях, насамперед в ООН. Москва повністю заперечує визнання себе стороною конфлікту на сході України та вимагає від міжнародного співтовариства визнати себе лише зацікавленою у вирішенні конфлікту стороною, вказуючи на аналогічні західні дії, такі як одностороннє проголошення незалежності Косово в 1990-х роках і вторгнення в Ірак в 2003 році;
- погрози НАТО та їх союзникам у формі постійних військових навчань;
- розгортання великомасштабної пропаганди не тільки серед свого населення але й закордоном.

Результати російських зусиль є неоднозначними. Росія таки домоглася від Заходу його максимального невтручання в події в Україні, здобувши собі час для створення і розширення своєї військової участі в конфлікті. Також РФ вдалося посіяти розбрат в НАТО та ЄС і створити напруженість всередині урядів цих країн, особливо у питанні антиросійських санкцій.

Однак, створити максимально комфортні умови для ведення діалогу з Заходом, незважаючи на український конфлікт, РФ так і не вдалося.

Дезінформація є одним із засобів ІВ РФ проти України. Це збиває з пантелику супротивника. Це дозволяє Росії заперечувати, що її сили присутні в Україні, тому що її бойові операції приховані під активною пропагандистською кампанією. Також, Росія забезпечила потужним дипломатичним прикриттям своїх військових і замаскувала свою зовнішньополітичну діяльність, тим самим зберігаючи для себе свободу дій.

Активна дезінформація дає Росії велику гнучкість у виборі методів для загострення конфлікту в Україні і розширює спектр можливих дипломатичних рішень на міжнародній арені на свою користь. Однак, поряд із цим варто відзначити практичну бездіяльність України у боротьбі на інформаційному фронті. Так, програвши судовий позов до Міжнародного суду ООН у Гаазі у справі фінансування РФ тероризму на сході України, представники української делегації продемонстрували свою неспроможність зібрати факти, що підтверджували б це.

У сьогоднішніх умовах прямої загрози національній безпеці України, яка розширюється, зокрема у зв’язку із посиленням пропаганди в іноземних телерадіопрограмах, є особливо актуальним створення ефективного і швидкого механізму реагування на подібні факти. З метою завдання конкретних матеріальних і нематеріальних збитків у певних сферах діяльності, встановлення власної інформаційної переваги, маніпулювання свідомістю, волею та почуттями громадян російські засоби масової інформації поширюють не лише недостовірну, неповну інформацію про Україну, а й відверту неправду.

Ведення антиукраїнської інформаційної війни стало масованим посяганням не лише на інформаційний, а й на державний суверенітет України. Тепер основною формою ведення цієї інформаційної війни є психологічна агресія, що здійснюються шляхом керованого інформаційного впливу на індивідуальну, групову або масову свідомість, волю громадян, їхні

почуття, дезінформування суб’єктів прийняття політичних, економічних та інших рішень, підрив інформаційної інфраструктури супротивника.

Головними завданнями таких інформаційних психологічних операцій є деморалізація населення України, особового складу Збройних Сил України, а також спонукання їх до державної зради й переходу на бік супротивної сторони; формування у громадян України та Росії викривленого бачення подій; створення вигляду масової підтримки дій Російської Федерації з боку населення Південно-Східних регіонів нашої країни; психологічна підтримка українських прихильників радикального зближення регіонів Сходу й Півдня України з Росією.

Розглянемо методи та прийоми, що застосовуються в інформаційній агресії проти України, та цільові групи, які стали об'єктами інформаційних атак.

Можна виокремити такі основні методи інформаційної агресії проти України [12]:

1) дезінформування та маніпулювання;

2) пропаганда;

3) диверсифікація громадської думки;

4) психологічний та психотропний тиск;

5) поширення чуток.

Дезінформування та маніпулювання інформацією – метод, який передбачає обман чи введення об'єкта спрямувань в оману щодо справжності намірів для спонукання його до запрограмованих суб'єктом дій.

На думку Валентина Петрика, кандидата наук з державного управління, доцента Київського націо-нального лінгвістичного університету, найчастіше у світовій практиці застосовуються такі форми дезінформування та маніпулювання інформацією:

- тенденційне викладення фактів – форма дезінформування, яка полягає в упередженому висвітленні фактів або іншої інформації щодо подій за допомогою спеціально підібраних правдивих даних. Як правило, за

допомогою цього методу спеціально сформована інформація подається дозовано, до постійно зростаючого напруження;

- дезінформування «від зворотного», що відбувається шляхом надання правдивих відомостей у перекрученому вигляді чи в такій ситуації, коли вони сприймаються об'єктом спрямувань як неправдиві. Внаслідок ужиття подібних заходів виникає ситуація, коли об'єкт фактично знає правдиву інформацію про наміри чи конкретні дії протилежної сторони, але сприймає її неадекватно, не готовий протистояти негативному впливу;
- термінологічне «мінування», яке полягає у викривленні первинної правильної суті принципово важливих, базових термінів і тлумачень за- гальносвітоглядного та оперативно-прикладного характеру;
- «сіре» дезінформування, що передбачає використання синтезу правдивої інформації з дезінформацією;
- «чорне» дезінформування, яке передбачає використання переважно неправдивої інформації [12].

Наслідки гібридної війни проти України відчутні вже сьогодні [1]:

- Розрив науково-технічних і оборонно-промислових зв’язків між Україною та Росією, в умовах якого вкрай важливим і критично необхідним є завдання створення власних пунктів виробництва основних типів зброї та військового обладнання. Це призведе до оновлення технологічної інфраструктури на існуючих, так і створення нових оборонних підприємств, у тому числі в кооперації із західними та іншими країнами.
- Поширення фактів злочинного «державного мародерства» Російської Федерації на окупованих територіях Криму, окремих районів Донецької і Луганської областей з вивезення в Росію обладнання та технічної і технологічної документації високотехнологічних (науковоємних) оборонних підприємств та об’єктів електротехнічної, металургійної і хімічної промисловості, а також транспорту та енергетики.

- Використання Росією широкого спектру проблемних питань щодо постачання енергоносіїв в Україну, перш за все природного газу (обсяги, терміни, цінова політика, кабальні умови передоплати та оплати) — в якості чинника тиску на Україну, а також постачання енергоносіїв в Європу транзитом через Україну (обсяги, транзитна політика, маршрути постачання) — в якості чинника тиску на Європу та Україну.
- Посилення торговельно-економічного тиску на Україну, як однієї із форм економічної війни Росії проти України.

Основним висновком і уроком з інформаційно-пропагандистської війни Росії проти України як важливої складової «гібридної війни» є її безпрецедентний характер за своїми змістом, масштабами і спрямованістю[1]:

- по-перше, інформаційна війна розпочалась задовго до військової агресії Росії проти України і продовжує супроводжувати її на всіх етапах, завчасно адаптуючись під поточні цілі і задачі;
- по-друге, інформаційно-пропагандистські та дезінформаційні проекти, операції і заходи спрямовані на всі верстви населення і всі регіони України, а також населення Росії і країн Заходу — відповідно, з різними цільовими установками і задачами;
- по-третє, головна мета інформаційної війни в Україні — ліквідація державності України; в Росії — отримання підтримки населення для виправдання дій керівництва Росії; для країн Заходу — дискредитація дій керівництва України та її Збройних Сил.

Інформаційна війна, яка сьогодні здійснюється проти України, може бути спрямована і проти будь-якої держави Європи. Ця війна є викликом усій міжнародній спільноті, супроводжується наростанням інформаційних загроз світовому порядку.

Грунтовною основою протидії антиукраїнській інформаційній війні має стати єдина комплексна система захисту суспільної моралі, яка сприяла б

реалізації права на інформаційний простір, вільний від матеріалів, що становлять загрозу фізичному, інтелектуальному, морально-психологічному стану населення.

Слід визнати, що Україна, її державні органи влади, громадянське суспільство та ЗМІ не були готові до такої масованої військової та інформаційної агресії, що в експертному середовищі отримала назву «гібридна війна». Саме тому першочерговим завданням усіх державних, громадських, наукових, експертних, журналістських інституцій є розробка термінових ефективних заходів щодо нейтралізації інформаційно-диверсійної діяльності Російської Федерації проти України та протидії її подальшому розгортанню. Крім того, виклики, що постали перед Україною, потребують вжиття негайних заходів щодо розробки нової Доктрини національної безпеки України, модернізації всієї системи інформаційної безпеки держави.

Тому, Указом Президента України введено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2014 року “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” у якому передбачається вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, у тому числі [14]:

– визначення механізму протидії негативному інформаційно-психологічному впливу;

– розробка проекту Стратегії розвитку інформаційного простору України, в якому, зокрема, визначити мету, завдання, структуру та режим функціонування національної системи забезпечення інформаційної безпеки держави та проекту Стратегії кібернетичної безпеки України;

– розробка проекту Закону України про кібернетичну безпеку України. Для запобігання хибним інформаційно-психологічним впливам потрібно дотримуватися низки правил:

– критично відноситись до будь-якої пропаганди зарубіжних засобів масової інформації, а більш довіряти інформації з офіційних джерел та видань;

– перевіряти та порівнювати інформацію від декількох джерел;

– не драматизувати обставини, які відбуваються навколо та в інформаційному середовищі;

– бути пильними та протистояти ворожим пропагандистам, завданням яких є створення у вашій свідомості бажаного для них уявлення про поточну ситуацію.

ВИСНОВКИ

Отже, в даному дослідженні було вивчено та опрацьовано відповіді на наступні питання:

- Мета інформаційної війни - послабити моральні і матеріальні сили супротивника або конкурента та посилити власні. Вона передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях. Очевидно, що інформаційна війна - складова частина ідеологічної боротьби. Вона не призводять безпосередньо до кровопролиття, руйнувань, при її веденні немає жертв, ніхто не позбавляється їжі, даху над головою. І це породжує небезпечну безпечність у ставленні до неї. Тим часом, руйнування, які завдають інформаційні війни психології суспільства, психології особи, за масштабами і за значенням цілком співвідносяться, а часом і перевищують наслідки збройних воєн.
- Питання формування понятійного апарату у сфері інформаційних відносин ще остаточно не вирішене. І передусім це пов'язано із недостатнім застосуванням методології теорії національної безпеки та її понятійного апарату. Можна наголосити на тій обставині, що чисельність трактувань поняття інформаційна війна, має більш глибинні коріння, ніж це здається на перший погляд. Йдеться про несформованість загальної теорії національної безпеки, а отже і базового вихідного алгоритму забезпечення безпеки країни.
- У сучасних умовах безперервний розвиток техніки сприяє послідовному підвищенню обсягу і швидкості поширення інформації. Удосконалюються можливості інформаційного охоплення великих територій та мас людей у найкоротші терміни. Разом із позитивними явищами глобальної інформатизації, чіткіше проступають контури нових міжнародних проблем. Передусім це стосується сфери інформаційної безпеки та інформаційного протиборства. По наявним на сьогодні розсекреченим документам, вже сьогодні у світі ведеться великомасштабна інформаційна та кібервійна.

- Маніпулювання свідомістю за допомогою ЗМІ є основним способом ведення ІВ, прямим вторгненням у психічне життя людей. При цьому маніпулятивний вплив організовується таким чином, щоб думка, уявлення, образ безпосередньо входили у сферу свідомості та закріплювалися в ній як дані безперечні й уже доведені. Подібне завдання ставиться перед ЗМІ, які часто є підконтрольними урядам держав.
- Глобальні соціальні зміни, події у світі в кінці ХХ ст. потребують об’єктивного аналізу інформаційного середовища світової спільноти. До цього проблема забезпечення інформаційної безпеки в нашій державі не лише не розглядалася, але й фактично ігнорувалася. При цьому вважалося за можливе її вирішення шляхом введення тотальної таємності, різних обмежень. Однак вже в 2014 році Україні довелося зіткнутися з інформаційною агресію збоку РФ. Виклики, що постали перед Україною, потребують вжиття негайних заходів щодо розробки нової Доктрини національної безпеки України, модернізації всієї системи інформаційної безпеки держави.

ДОДАТКИ

ДОДАТОК А

Термінологічний словник

Інформаційна безпека - стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Інформаційна війна - використання і управління інформацією з метою набуття конкурентоздатної переваги над супротивником.

Інформаційна зброя - сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виводу з ладу функцій і служб інформаційної інфраструктури в цілому або окремих її елементів.

Інформація - це нові відомості, які прийняті, зрозумілі і оцінені її користувачем як корисні.

Кібершпигунство - термін, що позначає, як правило, несанкціоноване отримання інформації з метою отримання особистого, економічного, політичного чи військової переваги, здійснюваний з використанням обходу (злому) систем комп'ютерної безпеки, з застосуванням шкідливого програмного забезпечення, включаючи "троянських коней" і шпигунських програм.

Пропаганда - форма комунікації, спрямована на поширення фактів, аргументів, чуток та інших відомостей для впливу на суспільну думку на користь певної спільної справи чи громадської позиції.

Фейк - підробка, фальсифікація. Спершу даний термін почав вживатися в мережі інтернет, а потім почав широко використовуватись і у повсякденному житті. Так, наприклад, поряд з часто вживаними виразами «фейкова сторінка», «фейковий аккаутн», «фейковий сайт» також можна почути вирази «фейкові продукти», «та він фейк» (про людину) та інші.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2016 році». – К. : НІСД, 2016. – 688 с.

2. Başlar M. A. The Influence of Media on the Reconstruction of Social Reality Through Asymmetric Information [Електронний ресурс] / Başlar. – 2014. – Режим доступу до ресурсу: http://cicr.blanquerna.url.edu/congres_vi/actas/dades/ambit2/2.%20Gulsah.pdf.

3. Strategic Information Warfare: A New Face of War [Електронний ресурс] // RAND Corp.. – 2014. – Режим доступу до ресурсу: http://www.rand.org/pubs/monograph_reports/MR661/index2.html.

4. Бой без поля боя – война в 21 веке. (По материалам корпорации RAND). [Електронний ресурс] // RAND Corp.. – 1995. – Режим доступу до ресурсу: http://csef.ru/ru/oborona-i-bezopasnost/265/boj-bez-polya-boya-vojna-v-xxi-veke-843.

5. Галатенко В. Г. Информационная безопасность. / В. Г. Галатенко. // Компьютерное обозрение. – 20 – №36. – С. 20–25.

6. Доктрина інформаційної безпеки України [Електронний ресурс]: Затв. указом Президента України від 8 лип. 2009 р. № 14/2009. — Режим доступу: http://zakon.rada.gov.ua/laws/show/514/2009

7. Завадский И. И. Информационная война – что это такое? / И. И. Завадский. // Конфидент. – 2012. – №4. – С. 13–20.

8. Зубарев Е. А. Обыкновенный фапсизм / Е. А. Зубарев. // Час Пик. – 2012. – №168. – С. 35–42.

9. Кузнецов П. А. Информационная война и бизнес. / П. А. Кузнецов // Конфидент. – 2012. – № 4. – С. 21-24.

10. Лібікі М. Що таке інформаційна війна? [Електронний ресурс] / М. Лібікі. – 2014. – Режим доступу до ресурсу: http://viysko.com.ua/texnologiji-voyen/martin-libiki-shho-take-informacijna-vijna/.

11. Малькова Т. В. Маси. Еліта. Лідер. / Т. В. Малькова. – М.: Яуар, 2015. – 232 с.

12. Манойло А. В. К вопросу о содержании понятия “информационная война”. [Електронний ресурс] / А. В. Манойло. – 2012. – Режим доступу до ресурсу: http://ashpi.asu.ru/ic/?p=1552.

13. Петрик В. І. Сутність інформаційної безпеки держави, суспільства і особи [Електронний ресурс] / В. І. Петрик. – 2015. – Режим доступу до ресурсу: http:// justinian.com.ua/article.php?id=3222.

14. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" [Електронний ресурс]: Затв. указом Президента України від 1 травня 2014 р. № 449/2014. – Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/449/2014.

15. Рижиков М. М. Міжнародна інформаційна безпека: Сучасні виклики та загрози / М. М. Рижиков. – К.: Центр вільної преси, 2015. – 916 с.

16. Рибак М. К. Війна у зоні Перської затоки: застосувапння нових методів збройної боротьби та їх вплив на розвиток воєнного мистецтва [Електронний ресурс] / М. К. Рибак // Військо України. – 1999. – Режим доступу до ресурсу: http://www.middleeast.org.ua/articles/17.htm.

17. Стратегія національної безпеки Україні «Україна у світі, що змінюється» [Електронний ресурс] : Затв. указом Президента України від 12 лют. 2007 р. Ns 105. — Режим доступу: http://zakon2.rada.gov.ua/laws/show/389/2012. — У ред. від 8 черв. 2012 р. № 389/2012.

18. Черешкин Д. С. Реалии информационной войны. / Д. С. Черешкин, Г. Л. Смолян, В. Н. Цыгичко. // Конфидент. – 2012. – №4. – С. 9–12.