DOI: 10.18372/2225-5036.22.11102

АНАЛІЗ СУЧАСНИХ ТЕОРІЙ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ В АСПЕКТІ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Андрій Гізун, Владислав Гріга

Національний авіаційний університет, Україна

ГІЗУН Андрій Іванович, к.т.н.

Рік та місце народження: 1987 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Національний авіаційний університет, 2010 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, управління інцидентами інформаційної безпеки, комплексні системи захисту інформації, штучні імунні системи, управління безперервністю бізнесу та правове забезпечення захисту інформації.
Публікації: більше 60 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях, авторські свідоцтва.
E-mail: andriy.gizun@gmail.com

ГРІГА Владислав Сергійович

Рік та місце народження: 1995 рік, м. Старокостянтинів, Хмельницька область, Україна.
Посада: студент, Голова Студентського науково-технічного товариства «CyberTag».
Наукові інтереси: інформаційна безпека, інформаційно-психологічна безпека, психологічні операції, інформаційна війна.
Публікації: 1 наукова стаття у фаховому журналі, матеріали та тези доповідей на конференціях.
E-mail: gsmgrey1@gmail.com

Анотація. *У даній статті розглядаються дослідження з теорії інформаційного протиборства та інформаційно-психологічного впливу з практичної точки зору. Дана тема є досить поширеною серед науковців у всьому світі. Проаналізовано моделі та концепції здійснення інформаційно-психологічного впливу, захисту від нього, моделі виявлення психологічних та інформаційних атак, життєві цикли інформаційного протиборства. Під час дослідження розглядалися наукові праці південноафриканських вчених Б. Ван Нікерка та М. Махараджа, що дослідили життєвий цикл інформаційно-психологічного впливу, фінів Й. Йормакка та Я. Молса, які розглянули інформаційне протиборство зі сторони теорії ігор, австралійців Б. Хатчисона та М. Уорена, що розробили та описали тактики проведення інформаційного протиборства, американця С. Джонсона і його модель інформаційної атаки, Науково-дослідної Ради США, проект моніторингу та виявлення інформаційно-психологічного впливу CEPA. Варто відзначити й українських вчених А. Шияна, що представив метод виявлення інформаційно-психологічного впливу та способи протиборства, та Р. Грищука, що розглянув технологічні аспекти інформаційного протиборства. Вищенаведені дослідники зробили вагомий внесок у практичні дослідження інформаційно-психологічного впливу. Аналітичне дослідження дозволить розробити формалізовану модель інформаційно-психологічного впливу, визначити його базові характеристики та розробити метод, а на його основі систему виявлення та ідентифікації інформаційно-психологічного впливу.*

Ключові слова: *інформаційне протиборство, інформаційна війна, інформаційно-психологічний вплив, інформаційно-психологічна безпека, психологічні операції, теорія інформації, модель.*

Вступ

Інформаційний вплив стає дедалі більш важливим у сучасному світі. Цьому процесу сприяє глобалізація та перехід до інформаційного суспільства. Саме цей чинник впливає на більш широке застосування інформаційних засобів впливу задля отримання власної вигоди. Найпоширенішими сферами їхнього застосування є військова, політична та економічна. Під час військових дій важливими аспектами є позитивна підтримка населенням дій військовослужбовців, погіршення морально-психологічного стану противника, його дезорганізація, у політичній – це створення підтримки населенням влади, наса-

дження ідеології, а в економічній – отримання переваги над конкуруючою компанією чи державою в цілому. Одним із основних методів досягнення цього є інформаційно-психологічний вплив.

Інформаційно-психологічний вплив (ІПВ) – це вплив на свідомість особи і населення з метою внесення змін у їх поведінку та (або) світогляд [1]. Звідси виникає потреба у забезпеченні інформаційно-психологічної безпеки.

Інформаційно-психологічна безпека особи (у вузькому розумінні) – це стан захищеності психіки людини від негативного впливу, який здійснюється шляхом упровадження деструктивної інформації у свідомість і (або) у підсвідомість людини, що призводить до неадекватного сприйняття нею дійсності [2].

Особливої актуальності забезпечення інформаційно-психологічної безпеки в Україні набуло у зв'язку з агресією Росії проти України, коли гостро постало питання щодо формування підтримки частиною населення територіальної цілісності України, підтримання на високому рівні морального бойового духу військовослужбовців сил АТО.

Застосування інформаційно-психологічного впливу та забезпечення інформаційно-психологічної безпеки неможливе без детального розгляду його теорії та методів реалізації. Тому надалі більш детально це й розглянемо.

Аналіз існуючих досліджень і постановка завдання

У роботі проведено аналіз сучасних досліджень інформаційно-психологічного впливу. Важливість інформаційного протиборства доводив китайський воєначальник Сунь-Цзи у своєму Трактаті «Мистецтво війни» ще у IV ст. до н. е. Першим документально засвідченим дослідженням з теорії інформаційного протиборства є робота М. Лібікі «Що таке інформаційна війна?», яка була опублікована в серпні 1995 року Національним інститутом оборони США. У ній автор намагався розкрити суть інформаційного протиборства та інформаційної війни, а також визначив основні її форми. Вперше термін «інформаційна війна» увів в обіг китайський теоретик Шень Веньгуань [3, 4]. Значних успіхів досягли американські дослідники Дж. Стейн і Р. Шафранскі, російський С. Расторгуєв, українські Я. Жарков, В. Петрик, М. Присяжнюк. Крім того, серед українських дослідників чиї роботи мають практичне значення, варто відзначити А. Шияна, В. Гумінського, Р. Грищука та інших [5, 6]. Тому дана стаття направлена на вивчення основних досліджень з питань інформаційно-психологічного впливу вітчизняних та зарубіжних науковців.

Метою даної роботи є аналітичне дослідження основних теоретичних та практичних теорій і моделей інформаційно-психологічного впливу, базових положень концепцій інформаційного протиборства.

Основна частина дослідження

Проведемо аналіз відомих публікацій в сфері інформаційно-психологічного впливу, виділимо ключові особливості відомих методів, моделей та теорій інформаційно-психологічного впливу.

Модель Шияна. Базові положення концепції інформаційного протиборства та війни були закладені в основному в роботах закордонних вчених, в першу чергу з США та Китаю, проте суттєвий внесок був внесений і вітчизняними науковцями. Зокрема, активно методами захисту від негативного інформаційно-психологічного впливу займається український вчений Шиян А. А. Він, з метою використання інформаційного середовища для підвищення захищеності людини та соціальної групи від негативного інформаційно-психологічного впливу, розглядає кортеж, який описує результат інформаційного простору:

$$IS =< DB, G, d_1, d_{1u}, d_{1d}, d_2, C_1, ..., C_8 >,$$

де DB – база даних, яка описує задачу; G – характеристика мети діяльності; d_1, d_{1u}, d_{1d}, d_2 – оператори дихотомічного поділу; $C_1, ..., C_8$ – вісім компонентів інформаційного простору [5]. Згідно даного дослідження інформаційно-психологічний вплив може бути здійснено щодо кожного елементу вищенаведеного кортежу або на певну його сукупність, а його здійснення на довільний елемент – можна описати оператором А:

$$A : IS_k \rightarrow IS_k^a .$$

У вищенаведеній формулі індексом «а» позначено один із елементів кортежу, що змінився.

Важливим із точки зору теорії інформаційно-психологічного впливу є розгляд науковцем двох випадків:

$$\exists is_j (is_j \in IS_k : is_j \notin IS_k^a).$$

Перший випадок відповідає ситуації, під час якої через зовнішній інформаційно-психологічний вплив із елементу кортежу інформаційного середовища вилучається одна із його «правильних» складових. Внаслідок цього інформаційний простір стає неповним. У другому випадку – внаслідок зовнішнього інформаційно-психологічного впливу до елементу кортежу додається нова «неправильна» складова. Внаслідок цього інформаційний простір перестає відповідати своєму функціоналу. Випадок, коли одна «правильна» складова елементу кортежу замінюється на «неправильну» зводиться до послідовного застосування вищенаведених операцій [5].

Шиян А. А. запропонував метод протидії інформаційно-психологічному впливу, згідно якого певні дії можна взагалі ідентифікувати саме як процес інформаційно-психологічного впливу. Метод базується на формуванні адекватної цілі діяльності інформаційного простору, який можна представити у вигляді кількох етапів.

Етап 1. Створюється база даних еталонних інформаційних просторів $IS_e(G,SA)$, які відповідають цілі діяльності G та предметним областям діяльності SA.

Етап 2. Здійснюється визначення поточних станів інформаційного простору із часом, у результаті якого будується інформаційний простір задачі $IS(t)$ в момент часу t.

Етап 3. Здійснюється порівняння по компонентам кортежу еталонного інформаційного простору IS_e із $IS(t)$.

Якщо в результаті порівняння отримана рівність $IS(t)_k - IS_e = \varnothing$, то акт негативного інформаційно-психологічного впливу не мав місця. У даному випадку рівень захищеності суб'єкту інформаційної безпеки є достатнім.

Якщо ж має місце таке співвідношення $IS(t)_k - IS_e = \Delta IS(t) \neq \varnothing$, то це означає, що потрібно приступати до захисту інформаційного простору [5].

Технологічні аспекти інформаційного протиборства. Значних успіхів у дослідженні інформаційного протиборства досягли українські науковці Р. Грищук, І. Канкін та В. Охрімчук. Згідно їхнього дослідження, суб'єктами інформаційного протиборства є вище політичне та військове керівництво держави, органи місцевого самоврядування та власне населення [6]. Виходячи з цього, вплив зловмисників направлений на дестабілізацію обстановки всередині країни. Також вони відзначили, що методи інформаційного протиборства ґрунтуються на психічних процесах людини. Науковці розглядають ознакову класифікацію методів інформаційного протиборства. Вона має п'ять характеристик: за типом протиборства, за метою, за характером впливу, за джерелом розповсюдження, за цільовою аудиторією. Згідно з цією класифікацією, за типом протиборства (ТС) суб'єктами захисту (або впливу) при інформаційно-психологічному протиборстві є:

– системи прийняття політичних рішень;

– системи формування громадської думки;

– системи формування суспільної свідомості (книги, фільми, телевізійні програми, друковані ЗМІ);

– психологічний вплив на психіку осіб, що приймають рішення (дискредитація лідерів) тощо [6].

За метою (АЕ) розрізняють методи пропаганди та контрпропаганди [6]. Пропаганда направлена на те, щоб поширити у свідомості визначеної групи людей необхідну інформацію. Контрпропаганда направлена на припинення поширення в інформаційному просторі повідомлення.

За джерелами розповсюдження (SD) різниця методів проявляється в способах їх реалізації [6]. Визначальна роль належить засобам масової інформації (ЗМІ): телерадіомовлення та друковані видання. В останнє десятиліття відбувається небувалий розвиток Інтернет-ресурсів. Проте, більш традиційні ЗМІ мають ряд переваг. Передусім це аудиторія: частка населення, яке дивиться телебачення значно більша, ніж та, яка читає електронні ЗМІ. Іншою перевагою є те, що телебачення сильніше у фоновому та наведеному інформаційних впливах.

За цільовою аудиторією (РА) при виборі методів, способів та прийомів інформаційного впливу обов'язково необхідно враховувати характер цільової аудиторії [6]. Передусім, необхідно враховувати такі характеристики як вік аудиторії, соціальний статус та рівень обізнаності.

Дослідники представили схему «Технологічні аспекти інформаційного протиборства на сучасному етапі», де детально наведено кожний аспект та зв'язок між ними (рис. 1) [6].

Модель життєвого циклу інформаційного протиборства. Південноафриканські науковці В. Нікерк та М. Махарадж дали визначення інформаційній війні як комплекс наступальних і оборонних операцій із використання інформаційних ресурсів. В. Нікерк та Махарадж визначили, що вона проводиться через зростаючу цінність інформації для людей. Наступальні операції направлені на збільшення цього значення. Оборонні – на потенційні втрати.

Із вищевказаного визначення вони зробили висновок, що використання інформаційної війни є спробою отримати перевагу над конкурентом або противником завдяки використанню власних або блокування інших інформаційних ресурсів. Вони довели, що інформаційна війна може вестися у фізичній, інформаційній і когнітивній області – це показує, що інформаційне протиборство може включати як традиційне фізичне знищення інформаційних ресурсів противника, так і виконання дій, направлених на людський розум.

В. Нікерк та Махарадж зазначають, що інформаційна війна ведеться проти трьох основних характеристик інформації: цілісності, доступності та конфіденційності. Виходячи з цього ставляться задачі щодо проведення дій:

– порушити та погіршити доступ до інформації або знищити інформацію;

– перехоплення інформації;

– погіршення інформації шляхом зміни змісту, вставка додаткової «брехливої» інформації, зміна контексту, у якому проглядається інформація і зміна сприйняття її людьми [7].

Дослідники визначають, що інформаційно-психологічний вплив здійснюється під час психологічної війни та розглядають модель Л. Кокса (рис. 2) [8].

Дана модель приймає форму потоку повідомлень. Вона побудована таким чином, що надає стимул для цільової аудиторії щодо дій. Відправник доставляє повідомлення за допомогою інструментів ЗМІ, що забезпечує певну реакцію аудиторії і можливість спостерігати за нею. Так, цільові спільноти реагують на повідомлення своєю підтримкою або байдужістю до нього, відправник потім повторно його оцінює на цій основі.

Південноафриканськими науковцями було запропоновано модель життєвого циклу інформаційного протиборства (рис. 3). Ними було розроблено дворівневий цикл. Цикл високого рівня містить основні блоки циклу (контекст, напад і захист, наслідки, реакції, відновлення і впливу на контекст). Це поєднується з більш детальним циклом, який показує застосування кількох понять високого рівня, наприклад, планування операцій буде виконуватися із урахуванням контексту і може проводитися до початку нападу або контрдій. Блок «АТАКА» містить кілька детальних інструкцій. Блок «ЗАХИСТ» має

захисні методи та інструменти. Блок «СУСПІЛЬСТВО» має 4 концепції на високому рівні [7].

Моделі інформаційно-психологічного впливу НДР США. Дослідження Національної дослідницької ради США вказує на те, що роль інформаційно-психологічного впливу є дуже вагомим під час сучасних конфліктів. Вони вбачають, що вплив, який направлений на соціальні процеси противника, базується лише на психології і розглядають 4 напрями: математичні моделі формування переконання у відповідь на передачу повідомлень, переконання мереж, моделі обробки соціальної мережі та транзактивна пам'ять.

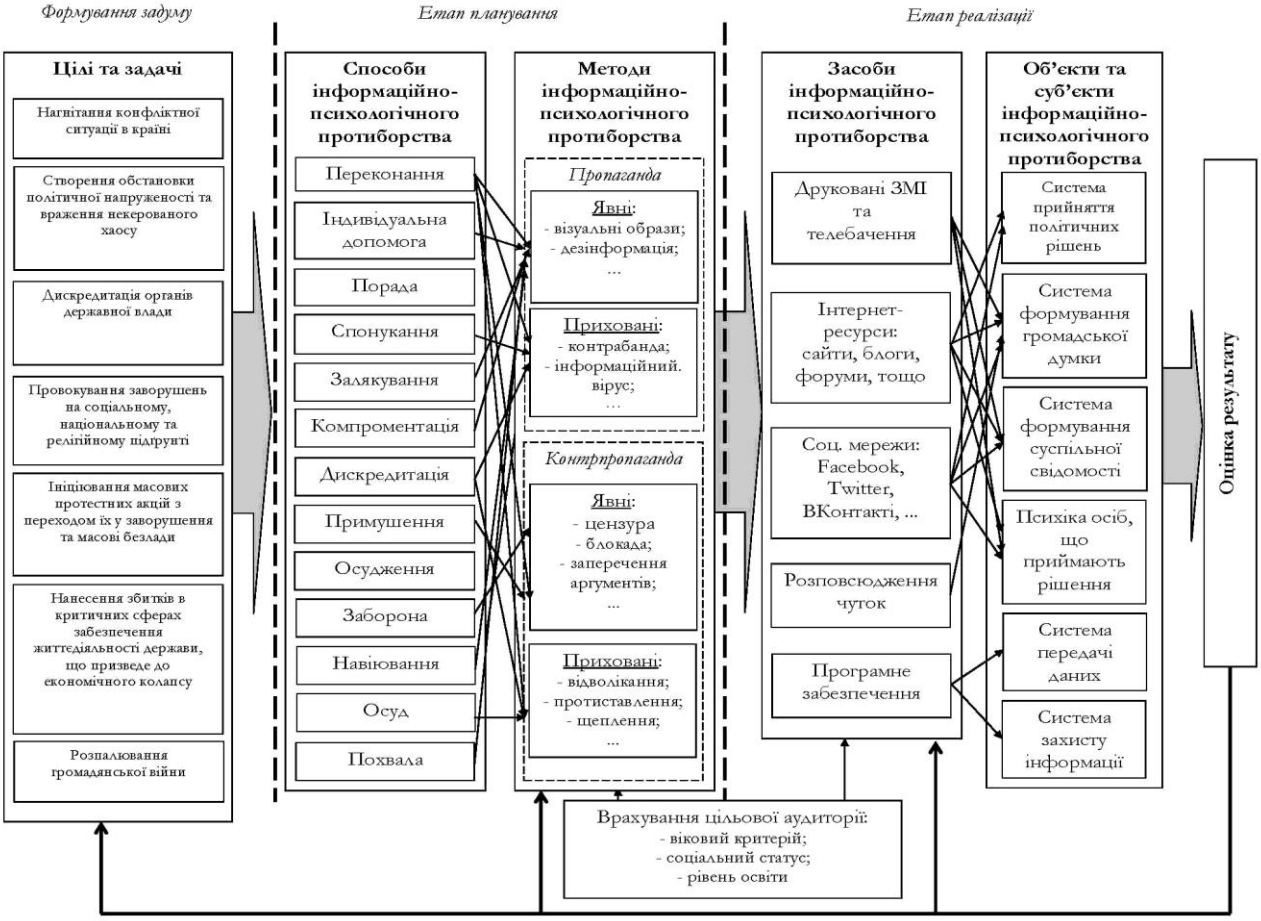

Рис. 1. Технологічні аспекти інформаційного протиборства на сучасному етапі

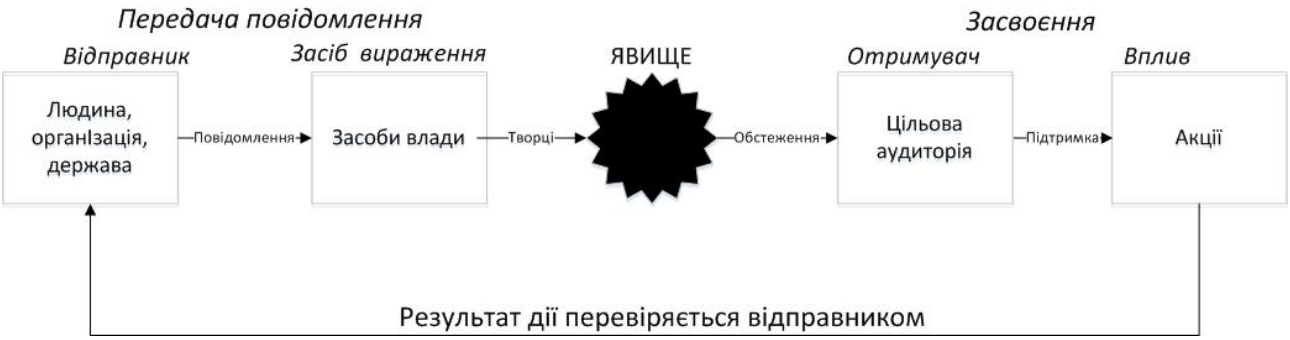

Рис. 2. Модель Л. Кокса

Більша частина соціальної роботи по формуванню психології переконань фокусується на тому, як повідомлення впливає на переконання. Розроблено важливі теоретичні поняття щодо цього: теорія підкріплення та теорія обробки інформації. На відміну від них, моделі соціальної мережі переконань зосереджені на тому, що положення індивіда в соціальній мережі та переконання інших членів групи впливають на переконання індивіда. Дані моделі називають моделями соціального впливу [9].

Багаточисельні емпіричні дослідження показали, що установлені переконання важче змінити. Крім цього доведено, що переконання, засновані на малій кількості інформації менш стійкі до змін. Таким чином, давно установлені переконання будуть стійкі до змін у тому ступені, у якому людина має найбільше аргументів для їх підтримання (ві-

рить у них через факти пов'язані із переконанням). Таким чином, дані твердження доводять ідею, що існує від'ємна кореляція між здвигом віри і теперішнього переконання незалежно від змісту повідомлення [9].

Дослідники виявили, що одним із найбільш перспективних підходів до розуміння інформаційної війни на локальному рівні є гібридні моделі, які використовують моделі визначеного інформаційного простору та моделі соціальної мережі. Дана гібридна модель включає в себе організаційні та когнітивні моделі. У даній моделі інформація зменшується і перетворюється у вузлах та із затримкою через обмеження зв'язку між вузлами. Така модель може об'єднати аналіз соціальних мереж для оцінки аспектів комунікації та ієрархії із переконанням мереж для оцінки аспектів індивідуальної обробки інформації. Тобто в них використовують соціальні мережі, для того, щоб зробити переконання мережі динамічними.

Соціальна обробка інформації передбачає введення у дію моделей структурних процесів, які впливають на переконання. Сучасні моделі зазвичай стимулюють процес, за допомогою якого люди взаємодіють з невеликою групою інших. Типова модель виглядає наступним чином:

$$T = Y + AWY + XB + E \ ,$$

де Y – представляє собою вектор власної особистості і відношення до друга або віра у певний момент; X – представляє собою матрицю із екзогенних факторів; W – вагова матриця, яка взаємодіє або проводить/спричиняє вплив, є постійною; B – представляє собою вектор розвитку певного інформаційного середовища; E – вектор (вектори) помилок [8].

Більш конкретно моделі вагомо відрізняються тим, як вони будують матрицю W .

Одне з ключових понять у даній моделі є транзактивна пам'ять, що полягає у здатності груп мати систему пам'яті. Ідея заключається у тому, що знання зберігаються стільки, скільки перебувають у динамічному використанні. Модель Вегнера транзактивної пам'яті заснована на представлені людської пам'яті у вигляді комп'ютерної системи.

Проект CEPA. У Європейському союзі було утворено проект CEPA задля виявлення інформаційно-психологічного впливу, контролю, збору, аналізу, даванню відсічі і виведенні на чисту воду російських пропагандистів у країнах Центральної та Східної Європи. Програма об'єднує провідних журналістів, активістів і аналітиків ЗМІ із держав Європи та використовує свій досвід для розробки аналітичного інструменту для ефективного рішення проблем із російською дезінформації на інституціальному, стратегічному і концептуальному рівнях [10]. Програма включає семінари, регулярний моніторинг програм російського змісту для конкретних країн і методів пропаганди.

Інформаційне протиборство зі сторони теорії ігор. Фінські науковці Йорма Йормакка та Ярмо Молса розглядають інформаційне протиборство та інформаційно-психологічний вплив з боку теорії ігор. Вчені доводять, що теорія ігор є однією з можливих шляхів вивчення математичних моделей інформаційної війни та інформаційно-психологічного впливу. У дослідженні також розглянуто мета стратегії, метою яких є зміни затрат на «гру». Такого роду управління громадською думкою тісно пов'язані з петлями спостереження (петлі Бойда, OODA) – кібернетичний самостійний і саморегулюючий цикл, що має в своїй структурі 4 процеси: спостереження, орієнтація, рішення і дія. Моделювання інформаційного протиборства та інформаційно-психологічного впливу як гри передбачає наявність двох гравців: злодія та захисника [11]. Всі гравці, як очікується, будуть раціональними. Виграш для зловмисника – це втрати жертви. Можливі чотири сценарії для моделювання:

1. Напад противника на командування, управління та системи зв'язку і намагання відключити їх.

2. Група нападників здійснює масовану атаку проти критичних інформаційних ресурсів.

3. Здійснення цільових, добре спланованих та скоординованих атак за допомогою кіберзброї, таких як нові віруси, хробаки та DoS-інструменти.

4. Група нападників проводить довгострокову інформаційна війну, щоб викликати економічні втрати і сповільнити технічний розвиток.

Розглядається кілька стратегій. Однією з них є «терористичні ігри». Терористична гра є статичною грою для двох гравців, де обидва гравці раціональні. Терористи (T) захопили заручників і загрожують їх підірвати, якщо вимоги терористів не приймаються. Уряд (G) пропонує, що терористи повинні здатися і сісти до в'язниці. Обидва гравці мають дві стратегії p_1 і p_2 . Стратегія p_1 означає прийняття умов одного з гравців у повному обсязі: терористи віддають заручників або уряд приймає вимоги (наприклад, платить викуп). гія p_2 означає, що виконується лише одна умова, і гравець повністю відкидає інші [10]. Виграшем є наступні ситуації:

– якщо обидва гравці грають p_1 , то вони разом отримують -1: G приймає вимоги, T здається і йде до в'язниці, але отримує вигоду згідно допустимих вимог;

– якщо обидва гравці грають p_2 обидва гравці, то отримують -10: G відкидає вимоги, T вбивають заручників і отримують вигоду сам;

– якщо один з гравців обере стратегію p_1 , то він отримує 0: Т грає p_1 , а інший гравець грає p_2 , то T отримує -5 і G відкидає умови, T здається та йде до в'язниці [11].

Припустимо, що G відіграє p_2 . Тоді G говорить, що він не буде вести переговори з T , T може не вірити, що G так зіграє і може спробувати стратегію p_2 скінченим числом раз, але якщо G грає p_2 , врешті-решт, і T доведеться почати грати p_1 для того, щоб звести до мінімуму втрати. Дану гру можна так проаналізувати, якщо T приймає, що G завжди відіграє p_2 і буде приймати рішення

або в підірвати заручників або прийняти вимоги уряду [11]. Потім раціональний гравець T завжди повинен грати p_1. Сміливий раціональний гравець виграє завжди над менш сміливим раціональним гравцем в довгостроковій перспективі, коли терористична гра повторюється.

Тактики проведення інформаційного протиборства. Австралійські науковці Біл Хатчисон та Мет Уорен визначили та дослідили тактики проведення інформаційного протиборства, одним із інструментів здійснення якого є інформаційно-психологічний вплив. Дослідження окреслює можливі режими інформації атаки, використовуючи модель життєздатності системи інформаційного протиборства як структуру для їх проведення. Це спроба використовувати засіб системного аналізу уразливостей інформаційної інфраструктури в усіх організаціях. Його акцент робиться на процес атаки, а не на контрнаступ.

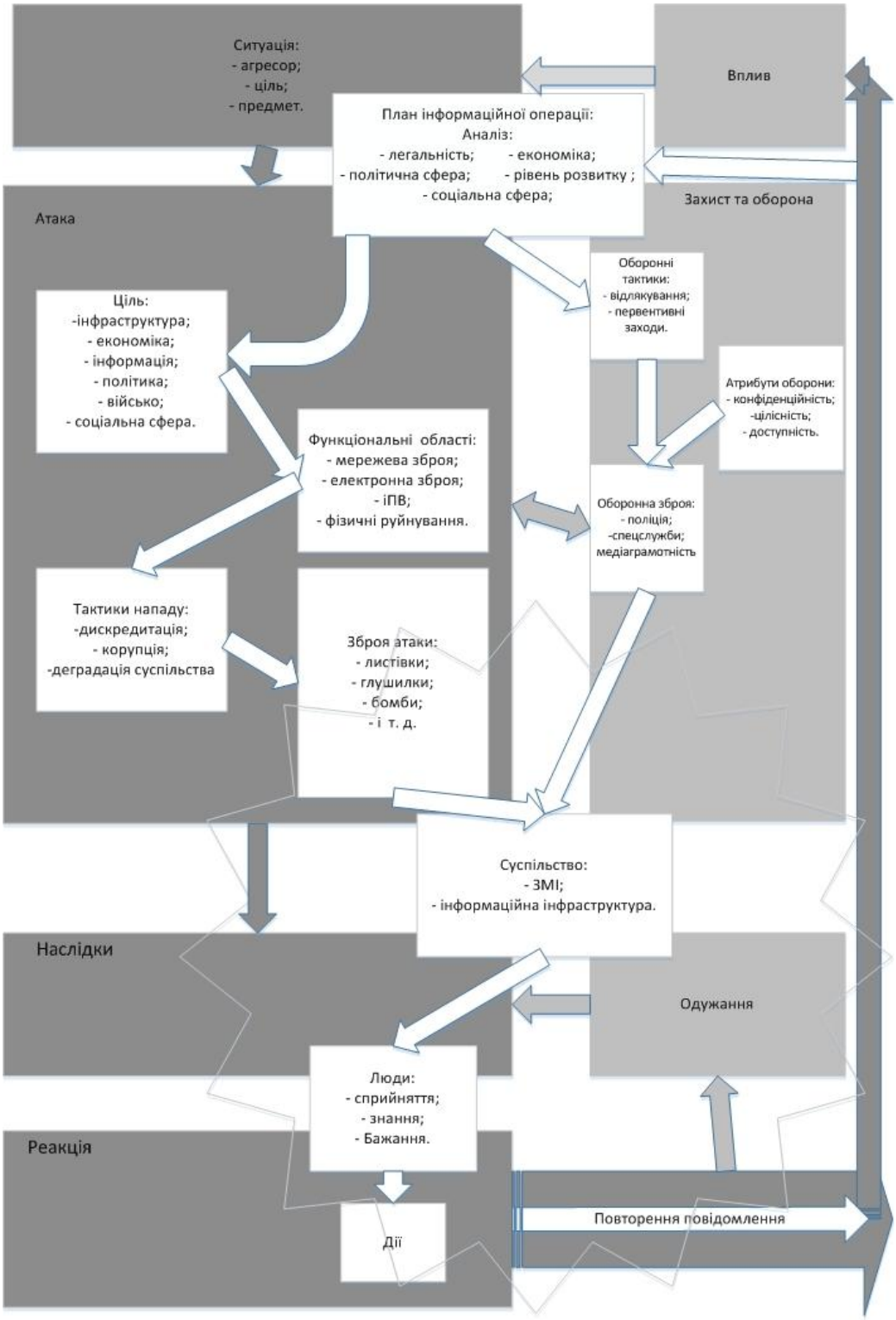

Рис. 3. Модель життєздатності системи інформаційного протиборства

Є кілька способів як інформація або інформаційні системи можуть бути використані для проведення інформаційного протиборства. Нижче перераховані деякі агресивні тактики, які є авторськими розробками дослідників:

– інформацією можна маніпулювати або дезінформувати. На одному рівні це може розглядатися як реклама, а на іншому – як навмисний обман;

– інформація може бути перехоплена, таким чином даючи перехоплювачу уявлення про сильні чи слабкі сторони противнику;

– інформаційні потоки в цільовій аудиторії можуть бути порушені, або зупинитися, тим самим виробляючи перевагу для нападника;

– цільовій аудиторії може бути «залита» інформація, яка сповільнить переробку або аналіз вхідних даних;

– інформація може бути недоступною або блокованою для аудиторії;

– порушення інформації або інформаційних потоків призводить до зниження достовірності інформаційної системи;

– розголошення конфіденційної та таємної інформації призводить до незручного становища органів влади [12].

Мотивацією для атак можуть бути певні організаційні цілі або зловмисні. Напади можуть здійснюватися організацією або окремими особами. Деннінг виділив п'ять класів ресурсів, задіяних у інформаційній війні. Це:

– контейнери, наприклад, комп'ютери і людські спогади;

– транспортери, наприклад, люди, телекомунікаційні системи.

– датчики, наприклад, сканери, камери, мікрофони, людські почуття.

– реєстратори, наприклад, принтери, людські процеси, що показують характеристики інформаційного середовища.

– процесори, наприклад, мікропроцесори, люди, програмне забезпечення [13].

Кожен з цих елементів, або їх компоненти, можуть бути середовищем атак. Таким чином, коло об'єктів може варіюватися від громадської думки до мікрохвильового посилання. Дослідники описують життєздатну модель інформаційного протиборства (VSM) Стафорда Біра (рис. 4) [14].

Модель складається з п'яти підсистем, які мають такі функції [12]:

1. Реалізація ($S1$): ця функція складається з напівавтономних одиниць, які виконують оперативні завдання у системі. Це функції, які є основою для існування системи. Вони взаємодіють з їх місцевим середовищем і один з одним. Кожен блок має своє власне локальне управління, яке підключається до ширшого управління вертикальних інформаційних потоків. Ця функція є частиною «роботи» організації.

2. Координація ($S2$): ця функція координує $S1$ для того, щоб кожна одиниця $S1$ діяла в інтересах всієї системи, а не своєї власної. Це може бути представлено як простий графік, або мораль серед працівників.

3. Внутрішній контроль ($S3$): ця функція обробляє інформацію політики з «вищої» функції ($S4$) і «нижчої» функції. Даний процес є функцією, яка контролює оперативний рівень. Його роль полягає в тому, щоб не створювати політику, але реалізувати її.

4. Розвідка та розробка ($S4$): ця функція діє як фільтр інформації від S3 і зовнішнього середовища.

5. Стратегія і політика ($S5$): ця функція є відповідальною за напрямок всієї системи. Вона повинна збалансувати внутрішні і зовнішні чинники.

Дослідники розглядають атаки на кожні функції більш детально:

Атака на основні діючі енергоблоки ($S1$)

Діючі енергоблоки можуть бути порушені:

– припинення їх експлуатації у локальному середовищі;

– відключення їх з іншими підрозділами $S1$;

– відділення їх від функції управління.

Інформація може бути використана для дезінформації локального середовища. Після цього окремі одиниці починають погано взаємодіяти одне з одним і значно погіршується управління ними. Дані напади мають на меті знизити ефективність організації порушуючи функції оперативного реагування [12].

Атаки на координаційну функцію ($S2$)

Мета атак на функцію узгодження ($S2$) полягає у знищенні згуртованості діючих енергоблоків. Метою, яку переслідують нападники є маніпулювання, заміна або заперечення інформації для того, щоб зробити функцію узгодження неефективною. Таким чином, діяльність $S1$ одиниць була б неузгодженою і працювали один проти одного до точки повного зриву під час успішної атаки. Прикладом може бути поширення неправдивої інформації задля дезінформування, що може призвести до втрати морального духу противником. Під час цих атак широко використовується інформаційно-психологічний вплив, який допомагає частково змінити характеристики середовища проведення операції [12].

Атаки на контролюючі функції ($S3$)

Головним для атак на функції контролю є використання інформації щодо порушення сприйняття політики. Таким чином, інструкції, що передаються з $S1$ будуть пропорційними з намірами політики, створені у $S5$. Зміна інформації в $S3$ і $S1$ впливає на зміни характеристик $S4$. На даному етапі формується вплив на політику, внаслідок якого вона буде змінена або деформована.

Атаки на $S3$ повинні порушити або знищити ефективне співробітництво між плануванням політики інформаційного середовища і її виконанням. Тому основною метою є зменшення ефективності взаємодії усіх ланок інформаційного середовища [12].

Знищення «мозку» і почуття організації ($S4$ / $S5$)

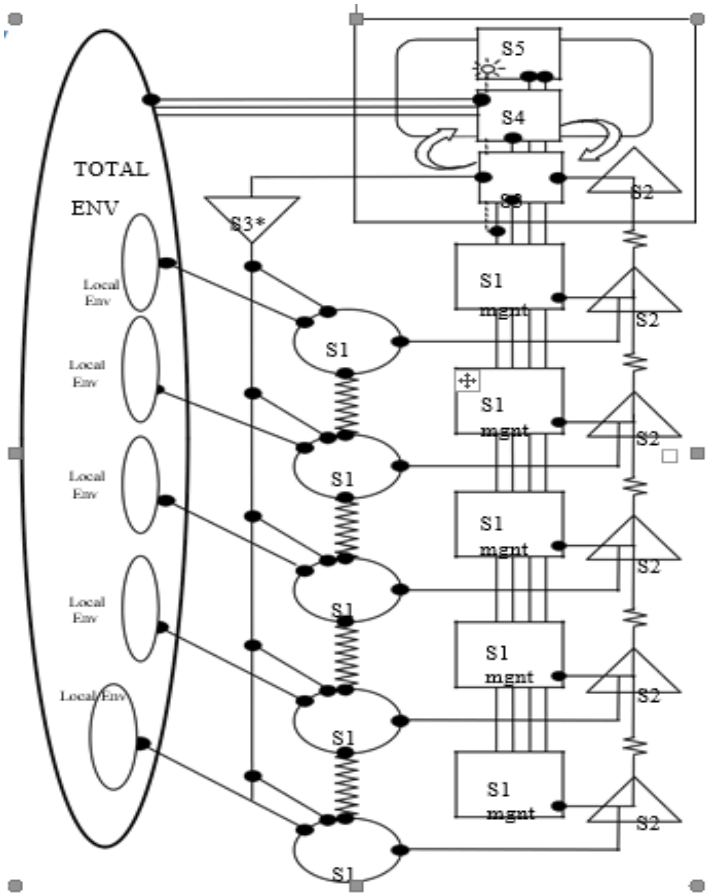

Рис. 4. Життєздатна модель інформаційного протиборства

Метою *S4* є динамічний зв'язок між зовнішнім і внутрішнім середовищем шляхом обробки і об'єднання інформації *S5* і *S3*. *S5* виробляє політику з даних, які надсилаються з *S4*.

Ці дві функції можуть розглядатися як «мозок» середовища. Таким чином, метою атаки є створення хибних уявлень внутрішнього і зовнішнього середовищ, тобто створення такої політики та стратегії, які не підходять середовищу. Кінцева мета передбачає знищення визначеного інформаційного середовища. *S4* також може бути переповнений неправдивою інформацією, яка викликає плутанину та недовіру до неї. Згідно дослідження, основними завданнями інтелектуальних систем (*S4*) є збір, обробка, аналіз та поширення інформації.

Класифікується рівень «Інформація» як: дані (вимірювання і спостереження); інформація (контекст, проіндексовані і організовані дані); знання (розуміння інформації); мудрість (знання ефективно застосовані).

Таким чином, завдання атак є порушення, маніпуляції з інформацією задля зміни цілі визначеного середовища Після отримання цільовою аудиторією інформації, нападники нею маніпулюють у раніше визначеному контексті. Класичним прикладом цього є кампанія з дезінформації німецьких військ британською владою до висадки військ союзників у Нормандії в 1944 році. На більш пізніх стадіях зловмисник має заперечувати ефективне застосування знань мети.

Модель інформаційної атаки Джонсона. Американський дослідник Скот Джонсон визначає, що інформаційне протиборство відбувається власне інформаційною атакою, комп'ютерною атакою та психологічною операцією. При чому усі компоненти часто взаємодіють між собою. Ці форми як правило використовуються на тактичному рівні, і вони потребують знання технічних характеристик мішені та експлуатаційних процедур. За нормальних умов вони є незалежними та ізольованими. Науковець розробив трирівневу цільову модель інформаційного протиборства. Вона складається з таких рівнів [15]: рівень інформаційної системи – фізичні елементи, які генерують, передають або зберігають інформацію. Атаки на інформаційні системи створюють технічні ефекти; рівень управління інформацією – процеси для обробки і розповсюдження інформації. На цьому рівні атаки створюють функціональний ефект; рівень прийняття рішення – інтелектуальні процеси для інтерпретації та використання інформації. На такому рівні атаки створюють експлуатаційні ефекти.

С. Джонсон представив використання моделі для атаки під час інформаційного протиборства.

Рівень інформаційної системи. Передусім атаки здійснюється на інформаційну систему. У багатьох, але не у всіх випадках, ця система є початковою метою атаки, і технічні ефекти від їх реалізації призначені для перевантаження приймача, порушення цілісності даних, виключення комп'ютера, стирання

даних, фізичного знищення носіїв інформації і т. д. [15].

Рівень управління інформацією. Управління інформацією означає передачу інформації, поширення, зберігання, злиття і перетворення. Ці функції виконуються інформаційними системами, і вони являють собою логічний рівень, накладеного на фізичному, інформаційних систем. Прикладами функціональних ефектів є зміна потужності передачі інформації, затримки продуктивності і перевантаження інформацією. Відбувається поширення дезінформації або розкручення певними фактами задля підривання довіри до органів влади, збройних сил. Ще більш серйозною проблемою є військова неправдива інформація, що передбачає ще й мережеву вразливість. Це викликано мінливими вимогами для проведення спільних операцій, в поєднанні з величезним збільшенням кількості систем зв'язку і передачі даних, які мають жорсткі вимоги до сумісності. Традиційні УКВ голосові радіостанції , що працюють на стандартних каналах можуть бути використані ким-небудь; інші передавачі можуть бути використані тільки якщо одержувач має сумісне обладнання. Противник може використовувати цю вразливість шляхом виявлення і орієнтації критичних вузлів, де виконується перетворення даних, або скориставшись плутаниною або проведенням атак. Якщо інформаційні управлінці звикли бачити нечитабельні дані, вони можуть не визнати той факт, що деякі дані були зіпсованими або пошкоджені, приписуючи порушення функціонування системи до її недоліків. Таким чином, планувальник атак повинен розуміти процеси управління інформацією ворога [15].

Процес прийняття рішення. Кінцевою метою інформаційної атаки є процес прийняття рішень. Дані ефекти можуть бути непрямими, для маскування та більш пізнього виявлення та прийняття контрдій противником. Багато чи більшість успішних командирів і лідерів на протязі всієї історії мали інтуїтивне розуміння своїх супротивників на цьому рівні; вони часто застосовували його в своїх інформаційних тактиках, маневрах і психологічних операціях (табл. 1) [15].

Інформаційні атаки — Таблиця 1

Вид атаки	**Цільовий рівень**	**Технічний ефект**	**Функціональний ефект**	**Операційний ефект (приклади)**
Глушіння систем звязку	Інформаційні системи	Блокування сигналу	Втрата інформації	Затримка або помилкове вирішення
Вторгнення у системи звязку	Управління інформацією	Лінії звязку перестають працювати	Втрата інформації, самогенеруючі перевантаження	Затримка
Компютерні віруси	Інформаційні системи	Параліч системи	Втрата даних, втрата функціональних властивостей	Затримка або помилкове вирішення
Мережеві черви	Управління інформацією	Лінії звязку перестають працювати	Затримка або перевантаження, що спричиняють втрату даних	Затримка вирішення, навмисне згортання вузлів
Інформаційно-психологічний вплив	Процес вирішення	Немає	Немає	Вирішення впливу
Інформаційно-психологічний вплив під час бойових дій	Процес вирішення	Немає	Немає	Сприйняття маніпуляції

Джонсон визначає основні елементи інформаційного протиборства (табл. 2). Елементи ІВ виходять за рамки методів і можливостей для традиційних форм інформаційної атаки. Беручи буквальне уявлення терміну «війна» необхідними елементами для інформаційного протиборства є: первинна атака і обороноздатність. Підтримка полягає в наступних задачах: збір розвідки для таргетингу інформації – розташування (яке, для інформаційного протиборства, може бути фізичним або логічним), сильні і слабкі сторони; збір розвідки для оцінки збитку битви (BDA); збір розвідки для свідчень атаки і попередження (I & W).

Основні елементи інформаційного протиборства — Таблиця 2

Цільові елементи						*Атака/захист*	
Логічний				Фізичний			
Інтелект		Інформація		Примітки	Посилання		
Фізичний	Операційний	Дані	Контроль			Наступ	Підтримка
місцезнаходження; параметри; функціональна архітектура; мережа.	користувачі; потік даних; терміни.	відео; текст; голос; картинки; цифровий.	головний канал сигналу.	ресурси даних; дані процесу зберігання даних; дані конвертації.	дані; комп'ютер.	блокування інформації; «продажна» інформація; затримка інформації; знищення інформації.	використання інтелекту; використання інформації.

Висновок

Дослідники у багатьох країнах світу широко описали процеси та створили моделі інформаційно-психологічного впливу. Враховуючи сучасну ситуацію із інформаційного протиборства, актуальність даних досліджень буде лише зростати. Зведена інформація про розглянуті моделі показана у табл. 3.

Ключові особливості моделей ІПВ Таблиця 3

Назва	Особливості
Модель Шияна	Виявлення інформаційно-психологічного впливу через зміну однієї із характеристик або всього інформаційного простору
Технологічні аспекти інформаційного протиборства	Розгляд ознакової класифікації методів інформаційного протиборства. Вона має п'ять характеристик: за типом протиборства, за метою, за характером впливу, за джерелом розповсюдження, за цільовою аудиторією
Модель життєвого циклу інформаційного протиборства	Дворівневий цикл: «АТАКА» і «ЗАХИСТ» із власним набором методів
Моделі інформаційно-психологічного впливу НДР США	Розгляд чотирьох складових: математичні моделі формування віри у відповідь на передачу повідомлень, переконання мереж, моделі обробки соціальної інформації та транзактивна пам'ять
Проект CEPA	Аналіз інформаційного середовища по ключовим словам, виявлення та ідентифікації інформаційно-психологічного впливу по контексту
Інформаційне протиборство зі сторони теорії ігор	Передбачається, що інформаційне протиборство – це гра з двома раціональними гравцями, для яких можливі кілька сценаріїв. Суть гри полягає у виборі кращого сценарію
Тактики проведення інформаційного протиборства	Представлення інформаційного простору як 5 підсистем: реалізація, координація, внутрішній контроль, розвідка та обробка, політика і стратегія, побудова тактик атак та захисту на них
Модель інформаційної атаки Джонсона	Визначення, що атаки може відбуватися як в цілому на інформаційне середовище, так і на окремі його рівні

Як бачимо наукові розробки із питання інформаційного протиборства є досить поширеними та ґрунтовними. Було проведено дослідження із інформаційно-психологічного впливу на формування української нації, яке довело дану дію зі сторони географічних сусідів на Україну [15]. Проте, існує проблема побудови формалізованої моделі інформаційно-психологічного впливу. Тому, отримані результати дозволять чіткіше визначити власне функцію та процес інформаційно-психологічного впливу. Це допоможе розробити нові кращі або покращити наявні методи захисту від нього, дозволить створити ефективні методи контрдій під час атаки.

Література

[1] Історія інформаційно-психологічного протиборства : підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш]; за заг. Ред. д.ю.н., проф., засл. юриста України Є.Д. Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2012. – 212 с.

[2] Інформаційна безпека: Підручник / [Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін.]; за заг. ред. Є.Д. Скулиша. – К. : КНТ, 2010. – 776 с.

[3] Бєльська Т. В. Інформаційно-психологічна війна як спосіб впливу на громадянське суспільство та державну політику держави / Т.В. Бєльська. – Технології та механізми державного управління. – 2014. - №3. – С. 49-56.

[4] Гріга В. С. Характеристика базових складових інформаційного протиборства/ В. Гріга, А. Гізун, І. Іванченко// Матеріали Другої всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації». – Одеса, 2016. – С. 22-25.

[5] Бурячок В. Л. Можливість забезпечення захисту від інформаційно-психологічного впливу на основі універсального методу онтологій / В.Л. Бурячок, А.А. Шиян // Сучасний захист інформації. – 2013. - №4. – С.57-67.

[6] Грищук Р. В. Технологічні аспекти інформаційного протиборства на сучасному етапі / Р.В. Грищук, І. О. Канкін, В. В. Охрімчук // Захист інформації. – 2015. – Том 17. – № 1 – С. 80–86.

[7] Van Niekerk B. The Information Warfare Life Cycle Model / B. Van Niekerk, M.S. Maharaj // SA Journal of Information Management – 2011. - Vol 13. - № 1–9 p.

[8] Cox L. Planning for psychological operations: a proposal / L. Cox. – Air Command and Staff College, Maxwell Air Force Base, Montgomery, Alabama, 1997. – 89 p.

[9] Pew R.W. Modeling Human and Organizational Behavior: Application to Military Simulations / Richard W. Pew and Anne S. Mavor. – Washington, D.C. : National Academy Press, 1998. – 418 p.

[10] CEPA [Електронний ресурс]. – Mode of Access URL: http://infowar.cepa.org/ – Дата звернення: 14.11.16.

[11] Jormakka J. Modelling Information Warfare as a Game / Jorma Jormakka, Jarmo V. E. Mölsä // Journal of Information Warfare. – 2005. – Vol 4 (2). – №12. – 25 p.

[12] Hutchinson B. Information Warfare: Using the Viable System Model as a framework to attack organizations / B. Hutchinson, M. Warren. // Australasian Journal of Information Systems. – 2002. - Vol 9. - № 2. – 10 p.

[13] Denning D.E. Information Warfare and Security / D.E. Denning. - Reading : Addison-Wesley, 1999. – 544 p.

[14] Beer S. The Viable System Model: its provenance, development, methodology and pathology / S. Beer; Espejo R, Harnden R. (eds.). – Chichester, John Wiley & Sons, 1984. – PP. 211-270.

[15] Johnson L. S. Toward a Functional Model of Information Warfare / L. S. Johnson // Center for the Study of Intelligence. CIA. – 8 p.

[16] В. Грига. Информационно-психологическая безопасность общества, как средство сохранения народа/ В. Грига, С. Гнатюк, А. Гизун// Безпека інформації. – 2015. – Том 21, 2. – С. 179-191.

УДК 003.26:004.056.55 (045)

Гизун А.И., Грига В.С. Анализ современных теорий информационно-психологического воздействия в аспекте информационного противоборства

Аннотация. *В данной статье рассматриваются исследования по теории информационного противоборства и информационно-психологического воздействия с практической точки зрения. Данная тема является достаточно распространенной среди ученых во всем мире. Проанализированы модели и концепции осуществления информационно-психологического воздействия, защиты от него, модели выявления психологических и информационных атак, жизненные циклы информационного противоборства. В ходе исследования рассматривались научные работы южноафриканских ученых Б. Ван Никерка и М. Махараджа, исследовавших жизненный цикл информационно-психологического воздействия, финнов И. Йормакка и Я. Молса, которые изучали информационное противоборство со стороны теории игр, австралийцев Б. Хатчисона и М. Уоррена, что сформулировали и описали тактики проведения информационного противоборства, американца С. Джонсона и его модель информационной атаки, Научно-исследовательского Совета США, проект мониторинга и выявления информационно-психологического воздействия CEPA. Стоит отметить и украинского ученого А. Шияна, который представил метод выявления информационно-психологического воздействия и способы противоборства ему, и Р. Грищук, рассмотревшего технологические аспекты информационного противоборства. Вышеприведенные исследователи внесли весомый вклад в практические исследования информационно-психологического воздействия. Аналитическое исследование позволит разработать формализованную модель информационно-психологического воздействия, определить его базовые характеристики и разработать метод, а на его основе систему обнаружения и идентификации информационно-психологического воздействия.*

Ключевые слова: *информационное противоборство, информационная война, информационно-психологическое воздействие, информационно-психологическая безопасность, психологические операции, теория информации, модель.*

Gizun A., Griga V. Analysis of modern information-psychological influence theories in aspect of information confrontation

Abstract. *This paper reviewed studies on the information warfare theory and information-psychological influence from a practical point of view. This subject is widespread among scientists in the whole world. Models and implementation concepts of the information-psychological influences, security from it, models of detection psychological and information attacks, lifecycles of information warfare were analyzed. During this research were examined the scientific works of South African scientists B. Van Niekerk and M. Maharaj, in which studied the lifecycle of information and psychological warfare, Finns Yormakka I. and J. Mols, in which studied the information warfare from the perspective of game theory, Australians B. Hutchison M. Warren in which identified and described the tactics of information warfare, American S. Johnson with his information attack model, and US Council Scientific Research of monitoring and information-psychological influence detection project CEPA. Also studied works of Ukrainian scientists: A. Shiyan, who presented method of detection information-psychological influences and confrontation methods and R. Grischuk, who considered the technological aspects of information influences. Above-mentioned researchers have made a significant contribution in practical research of information-psychological influences. In this study developed a formalized informational-psychological influence model, define basic characteristics and design the method, and based on it the detection system and the identification information-psychological influences.*

Key words: *information confrontation, information warfare, information-psychological influence, information-psychological security, psychological operations, information theory, model.*

Отримано *12 вересня 2016 року*, затверджено редколегією 26 *вересня 2016 року*