1 Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації

УДК 355.405.1

КОНЦЕПЦІЯ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ ТА ПРОТИДІЯ ІНФОРМАЦІЙНІЙ ЗБРОЇ

***Хорошко Володимир; Хохлачова Юлія; Прокофьєв Михайло*[1]**
Національний Авіаційний Університет;
[1]Національний технічний університет України «Київський політехнічний інститут»

CONCEPT OF INFORMATION IMPACT AND RESPONSE INFORMATION WEAPONS

***Khoroshko Vladimir; Hohlacheva Yulia; Prokofiev Mykhailo*[1]**
National Aviation University;
[1]The National Technical University of Ukraine «Kyiv Polytechnic Institute»

Анотація: **Проведено аналіз загальнотеоретичної суті інформаційних впливів і протидії інформаційній зброї. У ході проведеного дослідження було сформовано рекомендації щодо протистояння інформаційній війні.**
Ключові слова: **Інформаційна війна, інформаційний вплив, інформаційна зброя, протидія.**
Abstract: **This paper analyzes the essence of general theoretical information influence and information counter weapons. In the course of the study was formed recommendations on information war confrontation.**
Keywords: **Information war, information influence, information weapons, counteraction.**

Вступ

Досвід існуючих в останній час збройних конфліктів показує, що одними з найважливіших механізмів війни стають не тільки зміни у військовій справі, але й інформаційна революція, яка наразі переживає стадію формування. Перший досвід ведення інформаційної боротьби в оперативному масштабі, як однієї із складових військових протиборств, був започаткований у війні в зоні Перської затоки у 1991 році. Успіх застосування інформаційної зброї не тільки окрилив США в розумінні ролі інформаційної боротьби, але надав приклад іншим державам – як її застосувати. Прикладом її масштабного використання є інформаційна війна, яка ведеться Росією проти України.

На сьогодні є безліч визначень інформаційної війни. Визначення терміну інформаційної війни є у роботах М. Лібікі [M. Libiki], зокрема у [1], в якій автор визначив сім різновидів інформаційної війни: командно-управлінська, хакерська, економічна, психологічна, розвідувальна, електронна та кібервійна**.**

Найбільш важливими, на наш погляд, є електронна та психологічна війни. Електронна війна об'єктом свого впливу має засоби електронних комунікацій – радіозв'язку, телевізійних і комп'ютерних мереж.

Психологічна війна – здійснюється шляхом пропаганди, «промивання мозку» і іншими методами інформаційної обробки населення.

Мартін Лібікі виділяє чотири складові психологічної війни: підрив громадського духу, деморалізація збройних сил, війна культур, дезорієнтація командування.

Безліч визначень інформаційної війни пов'язано, мабуть, із складністю і багатогранністю такого явища, труднощами побудови аналогій з традиційними війнами. Якщо спробувати трансформувати визначення в поняття «інформаційна війна», то навряд чи щось конструктивне вийде. Це пов'язано з рядом особливостей інформаційної війни [2].

Для інформаційної війни зазвичай чітко визначена оборона, поняття початку і закінчення можна застосувати лише для окремих операцій інформаційної війни, лінія фронту не визначена, а наступ описується різними моделями. Успіх проведених інформаційних операцій не має прямого зв'язку з співвідношенням військових потенціалів сторін. Забезпечення інформаційної безпеки в сфері державного та муніципального управління ґрунтується на детальному аналізі структури та змісту управління, а також інформаційних процесів і використання при управлінні відповідних технологій.

При цьому визначальними факторами при розробці засобів інформаційної зброї [3] стають саме індивідуальні особливості людини та соціуму. Для того, щоб змоделювати поведінку людини (суспільства), необхідно знати саме її (його) індивідуальні особливості та переваги.

Зрозуміло, що інформаційна боротьба стає тим фактором, що впливає на саму війну, її початок, хід і результат. Це підтверджується агресією Росії проти України. Тому розробка концепції захисту системи інформаційно-аналітичного забезпечення завдань інформаційної боротьби є актуальною проблемою безпеки України.

Аналіз публікацій. Тема інформаційної зброї, інформаційного впливу на суспільство та формування ідеологічних особистостей у різних сферах його життя не є новою, адже чимало дослідників розкрили основні механізми інформаційних впливів. Проте вони постійно удосконалюються в різних напрямках і завдяки цьому з'являється безліч нових і неврахованих аспектів, дослідження яких має на меті їх виявлення, подальший розвиток, структуризацію і поширення у суспільстві.

Інформаційний вплив – це поширення певних ідей, поглядів чи ідеології, є засобом певної політики. Головним інструментом його реалізації є засоби масової інформації (ЗМІ) та різні комунікації.

У [4] визначають інформаційний вплив або пропаганду, як цілеспрямовані, систематичні спроби формувати сприйняття, маніпулювати свідомістю та спрямовувати поведінку суспільства у певному напрямку.

Хоча інформаційний вплив започаткував свою історію з початком історії суспільства, першою науковою школою, що спеціально досліджувала проблему інформаційного впливу, стала американська школа вивчення ЗМІ. Ця школа вивчала його передусім на матеріалі Першої світової війни.

Ця школа, зокрема, виокремлювала три основні типи інформаційних впливів:

1. «Білий» вплив. Його основною характеристикою є те, що журналіст відкрито називає себе і дозволяє пов'язати тексти зі справжнім джерелом. Яскравим прикладом подібної інформації є заяви президента, уряду, офіційного інформаційного агентства.

2. «Сірий» вплив. Журналіст використовує для поширення матеріалів спеціально створені джерела чи забезпечує просування матеріалів у певних незалежних засобах масової інформації. Прикладом подібного «сірого» інформаційного впливу може бути інформація, що поширюється через неурядові ЗМІ, неурядової організації тощо.

3. «Чорний» вплив. Журналіст поширює матеріали від імені третьої

ISSN 2074-9481
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (31), 2016р.

особи, наприклад, підпільної організації [5].

За твердженням французького дослідника другої половини XX ст. Ж. Доменака, під час здійснення інформаційної компанії звичайно застосовуються п'ять основних правил [5]:

1. Правило спрощення. Виходячи з орієнтації матеріалу на найменш досвідченого члена суспільства та її апелювання до емоцій, важливою вимогою є максимальне спрощення об'єкта впливу. Багатозначність, наявність напівтонів принципово не придатні для інформаційного впливу.

2. Правило перебільшення та перекручення. Створення позитивних (негативних) іміджів викликає необхідність гіперболізації певних рис об'єкта, акцентування на подіях, не обов'язково значних, але таких, що працюють на ідею, а за умови недостатньої чіткості матеріалу його перекручування.

3. Правило оркестрування або замовчування. Як визначив Й. Геббельс, «важливо не те, про що пишуть в газетах, важливо те, про що в них не пишуть». За матеріалами Р. Герценштейна, одним із основних прийомів такої пропаганди було саме замовчування. Подібні підходи широко використовують і сьогодні, особливо це стосується російських ЗМІ.

4. Правило переливання. Одне з важливих, проте дуже дискутивних, правил Ж. Доменака полягає у відповідності інформаційного впливу настановам і стереотипам суспільства [5].

5. Правило спільності та зараження. Це правило є повним аналогом деривації В. Парето (звернення до загальновживаного) [4].

Мета роботи. Метою роботи є аналіз загальнотеоретичної суті інформаційних впливів і протидії інформаційній зброї.

Основна частина

Розроблення загальних рекомендацій щодо узагальнення концепції протидії інформаційним впливам для інформаційно-аналітичного забезпечення (ІАЗ) випливає безпосередньо з результатів аналізу цих впливів для протидії зброї. Під інформаційним впливом розуміються цілеспрямовані заходи інформаційного характеру, які спрямовані на зміну поведінки або реакції людини, суспільства або інформаційно-обчислювальних (інформаційно-керуючих) систем (ІОС) в інтересах супротивника.

Розглянемо тільки ті види інформаційного впливу, які безпосередньо впливають на процеси прийняття рішень. Об'єктами впливу в процесі інформаційно-аналітичної діяльності (ІАД) можуть виступати: людина, суспільство, держава або ІОС. Вплив на ІОС є предметом протидії з боку технічного захисту інформації. Підходи до розв'язання проблеми захисту людини або суспільства в процесі ІАД на сьогодні відсутні навіть у постановочному плані.

Запропоновані концепції захисту ІАЗ відбивають технічні аспекти захисту саме людини або суспільства в процесі аналітичного опрацювання нею інформаційного матеріалу. У табл. 1 в узагальненому вигляді наведені фактори впливу на ІАД та можливі заходи щодо захисту від інформаційних впливів.

Часовий інтервал, на якому система намагається здобути перемогу в інформаційній війні (в даному випадку порівняємо з часом життя елементів людини, суспільства або ІАД), незначний з точки зору часу на зміну поколінь. Тому порівнювати час життя елементів з тимчасовим інтервалом активного ведення інформаційної війни не завжди коректно.

Таблиця 1

Узагальнені моделі інформаційних загроз

№	Джерела, канали реалізації загроз	Характер прояву загроз	Заходи із захисту від загроз
1	Інформаційні технології	Занепад власних технологій обробки інформації	Розробка власної інформаційної технології
		Імпортування запозичених інформаційних технологій	
2	Інформаційні ресурси	Перевантаження інформацією	Розробка методів стиснення інформації
		Дезінформування	Розробка методів виявлення дезінформації
		Приховування інформації	Оцінка інформації на повноту
		Тенденціозне подання інформації	
3	Свідомість людини	Суб'єктивність оцінки інформації	Автоматизація ІАД

В першу чергу доцільно відзначити наступне: інтенсивність модифікації навколишнього світу часто не залишає інформаційній системі або суспільству можливості вийти з запропонованих їй сценаріїв поведінки. В умовах, коли час інформаційної протидії між системами (системою, яка підлягається нападу та системаою супротивником, що володіє модельованими базовими елементами) малий (не перевищує середнього часу життя елементів системи), можна запропонувати алгоритм інформаційного впливу, що має назву «алгоритм, який завжди перемагає» [2]:

- визначення базових елементів інформаційного простору систем-супротивників;
- вивчення індивідуальних особливостей і потенційних можливостей базових елементів;
- моделювання різних варіантів поведінки базових елементів при різних вхідних впливах;
- вибір найбільш переважного сценарію поведінки базових елементів;
- підготовка середовища, в якому функціонують базові елементи (громадська думка), та їх самих;
- реалізація алгоритму.

Алгоритм цілеспрямованого інформаційного впливу в зародковому прообразі сьогоднішньої інформаційної війни був викладений майже сто років тому в [5]. Не вдаючись у суперечки про причини і джерела [5] хотілося б відзначити, що авторів зазначених положень безперечно слід назвати серйозними теоретиками в області побудови типових тактик і стратегій ведення інформаційних війн, хоча ці положення носять методичний характер. Вони складені так, що їх може використовувати будь-хто, розуміючий значимість таємної війни, і зовсім не обов'язково обмежувати їх застосування тільки мудрецями і тільки тим далеким часом. З точки зору значимості для теорії інформаційної війни дані протоколи, в чомусь аналогічні першим боязким дослідженням з теорії ядерної зброї.

Коротко та точно в [5] сказано практично про всі аспекти інформаційної війни:

- система управління, тобто контроль владних структур;
- кошти на перепрограмування населення (засоби масової інформацій);
- тероризм;
- економічна війна, засоби економічного управління;
- фінансова програма;
- загальне голосування і т. д.

Що собою представляє конкретний алгоритм інформаційної війни з конкретним супротивником? Дуже схожа

на «алгоритм, який завжди перемагає», та на рекомендації [5] схема дій, описана А. Зінов'євим у монографії «Русский эксперимент» [6] на прикладі інформаційної війни Заходу проти Радянського Союзу:

1. Для вивчення індивідуальних особливостей і потенціальних можливостей «базових елементів» СРСР на Заході була створена ціла наука зі своїми служителями – Кремлінологія.

2. «Кремлінологи найбільш допитливим чином вивчали апарат ЦК. І не тільки вивчали, а чинили на партійних керівників вплив через засоби масової інформації та помічників, радників, через дипломатів, журналістів, агентів КДБ… Можна визнати як факт, що Захід у вісімдесяті роки почав підсилювати певною мірою маніпулювання вищим радянським керівництвом».

3. «Кремлінологи вивчали ситуацію у вищому радянському керівництві ще за часів Брежнєва Л. І. Андропова Ю. В. і Черненко К. У., досконально якості керівників та претендентів на їх посаду. У відповідних службах Заходу вирішили усунути Г. Романова і розчистити шлях М. Горбачову».

4. «У засобах масової інформації було винайдено та оприлюднено наклеп на Г. Романова причому винахідники наклепу були впевнені, що «соратники» Г. Романова його не захистять. Так воно і сталося.

5. «Змінилося багато методів, прийомів і вони отримали наукове обґрунтування. Виникли цілі наукові напрямки: про те, як управляти поведінкою людини, колективом і суспільством. Виробництво та поширення інформації вже поставлено на конвеєр. Всього цього ще не було навіть у минулому столітті – не було достатньо ефективних методів та засобів масової інформації, не було науково обґрунтованих алгоритмів управління соціумом, а виникнути ці алгоритми могли лише з появою теорії програмування для сьогоднішніх засобів обчислювальної техніки. Здійснити інформаційну атаку – це значить так підібрати вхідні дані для системи, щоб активізувати в ній певні алгоритми, а в разі їх відсутності – активізувати алгоритми генерації потрібних алгоритмів.

Наявна на сьогоднішній день теорія алгоритмів цілком дозволяє пояснити, яким чином може здійснюватися автоматичне створення програм для певних предметних областей.

Процес реалізації зомбованого ефекту на окреме суспільство міг би виглядати наступним чином [2]:

1) розслабити суспільство – вселяти через засоби масової інформації, що ворогів немає; обговорювати окремі історичні періоди і інтереси окремих народностей (мета – суспільство як ціле має зникнути як об'єкт свідомості суспільства);

2) змусити суспільство слухати тільки противника, не звертаючи уваги на якість іншої думки або відчуття, наприклад, акцентувати засоби масової інформації на якійсь одній парадигмі суспільного розвитку (наприклад, російський), виключивши будь-який інший досвід, наприклад України, Польщі (мета – процес навантажування свідомості і дії формуючих сил послаблюються);

3) змусити суспільство не розмірковувати над тим, що говорить супротивник, і для цього виключити із засобів масової інформації результати досліджень серйозних аналітичних проблем (мета – сприяти гальмуванню безперервного потоку думок);

4) зосередити увагу суспільства на якомусь предметі окрім вхідного інформаційного потоку, наприклад, внутрішні катаклізми, війни, терористичні атаки (мета – підсистема захисту, відповідальна за обробку вхідної інформації, виявляється не в змозі виконувати свою функцію і як би розбудовується);

5) постійно навіювати, що саме суспільство стає краще і краще, а всі навколишні ставляться до нього краще й краще (мета – подібне навіювання послаблює історичну пам'ять і почуття самоототожнення, якими характеризується нормальний стан суспільства);

6) ЗМІ одночасно повинні переконувати членів суспільства про те, що викликало такий стан – це не зовсім те, що повинно бути (мета – створення пасивного стану свідомості, в якому зберігається можливість залежності від інформаційного впливу супротивника).

Наведений алгоритм в загальних рисах відображає роботу ЗМІ в Росії часів 1990 - 2015 років та в Україні до та під час агресії Росії.

Для дослідження впливу ЗМІ на суспільство застосовуються окремі моделі.

На першому кроці береться модель "S-R" ("стимул – реакція"), що була одним із перших підходів до розуміння впливів ЗМІ [7]. Інформаційний потік, сформований ЗМІ, розглядається як незалежна змінна, а суспільство та його досвід, настанови та поведінка – як залежна змінна.

Ця модель дозволяє лише оцінити кількісну міру впливу "стимулу" на думку суспільства. Співвідношення кількості матеріалів змінної «реакція» до кількості матеріалів змінної "стимул" у розрізі кожного окремого дня дослідження визначає "коефіцієнт корисної дії" впливу ЗМІ на суспільство. Головним прикладним результатом, що дає змогу отримати модель "S-R", є інформація про проміжок часу між піковими значеннями "стимул" та "реакція", тобто затримку реакції суспільства на вплив ЗМІ.

Наступними моделями, що застосовуються на шляху еволюції впливу ЗМІ на суспільство, були:

1) модель "O-S-O-R", що містить етапи взаємодії суспільства та ЗМІ: "Зумовлюючі змінні", "Комунікація мас-медіа", "Проміжні змінні", "Досвід, настанови та поведінка реципієнтів". Ця модель являє собою удосконалення моделі "S-R", що враховує проміжні змінні [7], [8];

2) модель двоступеневого потоку інформації. Згідно з цією моделлю ідеї від ЗМІ спрямовуються до лідерів думок (перший ступінь), а від них вже до ідейних прихильників (другий ступінь) [7], [8]. Таким чином реалізовуються два односторонніх спрямованих потоки: від ЗМІ до лідерів та від лідерів до ідейних прихильників;

3) модель двоциклічного потоку інформації враховує недоліки, що наявні в попередній моделі. ЇЇ концепція полягає в тому, що інформаційний потік дорівнює одноступеневому потоку інформації, а процес впливу – двоступеневому потоку інформації:

- інформація від ЗМІ надходить відразу до всіх членів суспільства, що сприймають її з однаковою уважністю;
- ЗМІ можуть впливати лише на настанови лідерів думок, але не на настанови ідейних прихильників;
- ідейні прихильники сприймають інформацію, що несумісна з ними;
- лідери думок звертаються за порадами до інших лідерів думок;
- будь-хто може взяти ініціативу комунікації у свої руки.

Однак отримати підтверджуючі показники для цих моделей за допомогою контент-аналізу неможливо у зв'язку з тим, що не існує можливості відокремити проміжні змінні в моделі "O-S-O-R", а в моделях двоступеневого та двоциклічного потоку інформації – виконати опис процесу інтерпретації інформації ідейними лідерами та її сприйняття суспільством за допомогою вербальних моделей.

Усі зазначені вище моделі не дають змогу оцінити "міру важливості" новин щодо згадувань інших подій у новинах ЗМІ. Для визначення пріоритетності наведених новин порівняно з іншими новинами пропонується виконати побудову інших моделей − моделі важливості та моделі поінформованості [8]. Головна ідея моделі важливості полягає у припущенні, що ЗМІ впливають лише на визначення тем, які мають розглядатися як важливі. Модель базується на тому, що ЗМІ оцінюють теми за рахунок певних технік виконання (частота згадувань, виділення новинарної площі та інше).

Принцип моделі поінформованості: ЗМІ впливають лише на ті теми, які взагалі привернуть громадську увагу. Темами ЗМІ є нові події або нові обставини відомих

справ, а суспільство переймається тими темами, про які вони повідомляють. Найкращим показником у такому випадку слугуватиме відсоткова частка новин, що присвячені досліджуваній тематиці, у загальній кількості статей у щоденному розрізі.

Прикладне застосування отриманих даних за моделями важливості та поінформованості полягає в розрахунку міри поінформованості суспільства певною тематикою.

Крім того, застосовується модель використання та задоволення, яка ґрунтується на припущенні, що люди активно використовують ЗМІ для задоволення своїх власних потреб. Тому в центрі моделі перебувають саме потреби. Головні її положення:

- суспільство використовує засоби масової інформації;
- використання має характер задоволення власних потреб;
- на поведінку, пов'язану з використанням ЗМІ, впливають соціальні та психологічні чинники.

Щодо інтегративної моделі задоволення, то вона враховує існуючу критику щодо розглянутої вище моделі використання та задоволення. У цій моделі чітко розрізняються отримані задоволення, а також врахована зворотна дія від отриманих задоволень на потрібні задоволення [7], [8].

Модель Г. Ласуелла [9] – модель впливу ЗМІ на суспільство, передбачає відповіді на запитання:

1) хто надсилає інформацію?;
2) що міститься в інформації?;
3) якими каналами інформація передається?;
4) кому адресується інформація?;
5) який ефект викликає інформація?

Ця модель є композицією моделей, що перераховані вище. Так, наприклад, модель "S-R" дає відповідь на питання 1 та 4. Відповідь на питання 5 міститься в усіх вище розглянутих моделях, які по-різному інтерпретують отримані результати.

Отримані показники моделі "S-R" та моделі поінформованості дуже добре відображають міру впливу засобів ЗМІ на суспільство. На їх основі можна проаналізувати взаємозв'язок ЗМІ та громадської думки, прогнозувати розвиток ситуації. Однак ці моделі не дозволяють проаналізувати дії у розрізі усіх суб'єктів подій довкола прийняття рішення під впливом ЗМІ.

Будь-яка система, відповідальна за обробку вхідної інформації, повинна споживати енергію для того, щоб проводити в дію закладені в ній алгоритми обробки вхідної інформації та генерувати нові. Базові елементи кожної системи мають певну фізичну природу, яка багато в чому визначає час реакції, а значить, і вибір того чи іншого алгоритму вирішення конкретного завдання.

Задача виявлення дезінформації або інформаційного впливу є складною і багатоаспектною задачею [7], [8], розв'язання якої потребує урахування наступних параметрів:

- визначення якісних показників, які характеризують інформаційний вплив і несуть в собі дезінформацію;
- визначення особливостей організаційної структури проходження інформаційного впливу від джерела до кінцевого користувача (створення маршрутної моделі);
- дослідження кількісних та якісних показників, які характеризують знання про навколишній світ (проблемну область) і є необхідними для залучення при аналізі інформації на достовірність;
- визначення показників зовнішньої характеристики інформаційних впливів (звідки, куди, кому, від кого, коли надійшов певний інформаційний вплив?) та методик їх використання для оцінки достовірності інформації;
- дослідження інформаційних моделей суб'єкта, об'єкта та створювача інформації тощо.

В [6] можна прочитати: «В руках сучасних держав є велика сила, яка створює рух думки в народі - це преса». «Жодне

сповіщення не буде проникати в суспільство без нашого контролю. Це і тепер уже нами досягається тим, що всі новини виходять кількома агентствами, в яких вони централізуються з усіх кінців світу. Ці агентства будуть тоді вже повністю нашими установами і будуть оголошувати тільки те, що ми їм наперед напишемо».

Тобто вплив ЗМІ є дуже різноманітним та виражається в [10]:

– поінформованості суспільства;

– настановах суспільству, поведінці суспільства.

Результатами впливу засобів масової інформації можуть бути [9]:

– зміни в поведінці суспільства;

– зміни в настановах суспільству (бо поведінка і настанови не можуть бути ототожнені);

– зміни в знаннях суспільства, як наслідок зростання поінформованості.

Слід відзначити, що ЗМІ мають дуже великий вплив на суспільство в цілому та на окрему людину.

При аналізі інформаційних джерел можна визначити такі характерні впливові прийоми:

1. Читання думок. Журналіст ніби читає думки пересічних людей, але насправді нав’язує їм свої міркування.

2. Анонімність. Цей прийом ближче до першого типу. Він полягає у використанні анонімного або фактично анонімного джерела повідомлень. Улюблений прийом для введення в оману активно використовується усіма ЗМІ, особливо російськими. Він відноситься до так званого «Сірого» впливу.

3. Вилучення. Суть цього методу полягає у фільтрації думок членів суспільства. Текст журналіста проходить у повідомлення повністю, а текст інтерв’юера подається частинами.

Як зазначено у [11] Е. Ефон виділяє чотири типи вилучень:

– відхилення;

– перспектива;

– підміна;

– останнє слово.

4. Звеличення. Цей тип прийомів спрямований на ідеалізацію, створення позитивного іміджу людини, спільноти або інституту. Визначають шість видів цього прийому:

– похвала;

– придушення негативу;

– найменування і звеличення негативів;

– ігнорування негативних характеристик;

– збільшення значущості;

– атака опонентів як аморальних осіб.

5. Приниження. Дослідження Е. Ефрона доводять, що їх існує сім видів:

– пряма атака;

– непряма атака;

– атака за допомогою подвійного стандарту;

– гумор, сарказм, сатира, іронія;

– аргумент;

– звинувачення за асоціацією;

– код.

6. Підроблений інтелект. Суть цього типу прийомів у штучному створенні враження про нейтралітет комунікатора, який насправді заанагажований однією зі сторін. Він поділяється Е. Ефроном на шість прийомів:

– фальшивий комплімент;

– фальшива критика;

– фальшиві серії;

– фальшивий прототип;

– напівдебати;

– подвійна бесіда.

7. Повна фальсифікація. Досить активно використовуються прийоми, що є повною фальсифікацією. Найчастіше використовується така ситуація як цитування вихопленого з контексту речення, фрази або висловлювання.

8. Редагування структури. Цей тип інформаційних прийомів активно використовує можливості психологічного впливу шляхом структуризації текстів:

– “отруйний сендвіч”;

– “цукровий сендвіч”;

– перебільшення деталей.

9. Інші техніки. Цей тип прийомів зазвичай використовують як додаток, як

додатковий разом з іншими. Слід виділити його чотири основні види:

– суперузагальнення;
– недоведена теорія;
– навідне запитання;
– однослівна журналістика.

10. ”Буденна розповідь”. Цей прийом використовується для адаптації людини до негативної інформації, що викликає заперечення своїм змістом.

11. Голодування. Ефективний прийом емоційного впливу на суспільство та психологічного тиску на владу. Підбирається група добре оплачуваних молодих людей із міцним здоров’ям, які, нічим не ризикуючи, організовують ”курс лікувального голодування” у якому-небудь публічному місці. Навколо цього ЗМІ підіймають неймовірний галас. Проти цього прийому встояти вкрай складно тому, що влада в будь-якому випадку змушена реагувати на висунуті ”борцями” вимоги.

12. ”Тримай злодія”. Мета прийому – змішатися з переслідувачами.

Не має потреби детально зупинятися на досвіді Росії, інформаційний ресурс якої вже давно перетворено на потужну агітаційно–пропагандистську машину Кремля. Це, по-перше, ”нацизм” – визначення просоюзних, прокомуністичних сил у колишньому СРСР протилежною стороною під гаслами: ”Крим наш” та ”Донбас наш”. По-друге, представлення України та інших країн як агресорів, які здійснюють геноцид російськомовного населення.

При цьому слід враховувати, що характерною рисою сучасної цивілізації є її детермінованість інформаційним процесам. Потенційні можливості розвитку основних сфер життя сучасного суспільства залежить від стану цих процесів. На сьогодні інформація вважається стратегічним національним ресурсом та засобом впливу на інші держави. Таку ситуацію важко було передбачити у попередні роки.

Впровадження сучасних засобів обробки і передачі інформації в різні сфери діяльності започаткувало новий еволюційний процес у розвитку суспільства – інформатизацію.

Під впливом інформатизації усі сфери життя суспільства набувають нових якостей – гнучкості, динамічності, але водночас зростає і потенційна вразливість суспільних процесів від інформаційного впливу.

Насамперед величезний потік інформації хлинув на людину не даючи їй змоги сприйняти цю інформацію повною мірою. Внаслідок – настає інформаційна криза або вибух, що має такі прояви:

– з’являються протиріччя між обмеженими можливостями людини щодо сприйняття та переробки інформації й існуючими потоками та чисельністю інформації, що зберігається. Наприклад, загальна кількість знань змінювалася спочатку дуже повільно, але вже з 1900 року вона подвоїлась за 50 років, з 1950 подвоєння відбувалося кожні 10 років, з 1970 року – кожні 5 років, а з 1990 року – щорічно;

– існує чимало зайвої та шкідливої інформації, яка ускладнює сприйняття корисної для споживача інформації;

– виникають певні економічні, політичні й інші соціальні бар’єри, які перешкоджають поширенню інформації. Наприклад, через дотримання режиму таємності часто необхідною інформацією не можуть скористатися працівники інших відомств. Ці причини породили парадоксальну ситуацію: у світі накопичений великий інформаційний потенціал, але люди не можуть ним скористатися сповна через обмеження власних можливостей.

Стрімке зростання обсягів інформації й об’єктивна зміна умов психологічної діяльності людини в сучасному світі привели до перерозподілу ваги даних про оточуючий світ що надходить до індивіда за допомогою різних інформаційних шляхів і в результаті безпосереднього сприйняття дійсності на користь даних, які отримуються ним із ЗМІ.

Розвиток ЗМІ, інформаційних технологій та техніки з інформаційної безпеки

обумовлює масштабність і результативність проведення інформаційних виливів. Поява технічних засобів нового покоління, що здатні ефективно впливати не тільки на психіку і свідомість людей та на нове покоління людства, але й на інформаційно-технічну інфраструктуру держав-супротивників, дала змогу вести інформаційну війну на якісно новому рівні, основними завданнями якої є:

1) здійснення деструктивного ідеологічного впливу;

2) створення атмосфери бездуховності, негативного ставлення до культури та дискредитація фактів історичної, національної самобутності народу противника чи ворога;

3) маніпулювання громадською думкою з метою створення політичного напруження та стану близького до хаосу;

4) формування негативного іміджу держави на міжнародній арені;

5) дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою розпалення конфліктів, стимулювання недовіри, загострення ворожнечі, боротьби за владу;

6) зниження рівня інформаційного забезпечення органів влади та управління, інспірація помилкових управлінських рішень;

7) провокування соціальних, політичних, національно-етнічних і релігійних зіткнень;

8) створення чи посилення опозиційних угруповань чи рухів;

9) зміна системи цінностей, які визначають спосіб життя і світогляд людей;

10) формування передумов до економічної, духовної чи військової поразки, втрати волі для боротьби та перемоги;

11) підрив морального духу населення і, як наслідок, зниження обороноздатності та бойового потенціалу.

Крім того, в системі захисту інформації (протидії) слід враховувати і викривлення інформації (порушення цілісності), яке з’являється в результаті певних дій або помилок її передачі [7], [8]. Передбачається, що об'єктом захисту є зміст мовної інформації, носіями якої виступають фізичні поля і сигнали, які можуть бути перетворені для подання в текстовій формі в ЕОМ. Вибір об'єкта захисту обумовлений такими міркуваннями [7]:

1. Для кінцевого користувача важливо одержати і проаналізувати зміст інформації. Тому особливого значення в цьому випадку набуває проблема захисту цілісності саме змісту інформації. Вона може бути порушена на будь-якій із фаз обробки – передачі, прийому, формування, аналізу, перетворення, відображення та збереження інформації.

2. З точки зору протидії технічній розвідці захист інформації (як мовної, так і текстової) потрібно здійснювати таким чином, щоб був забезпечений необхідний рівень безпеки цілісності її змісту.

3. Аналіз стану теоретичного доробку в області автоматизації обробки мовної та текстової інформації дозволяє стверджувати, що при відповідному їхньому розвитку можна розробити методичні рекомендації та створити програмні засоби оцінки ступеня порушення цілісності її змісту, а також відновлення змісту перекрученої або частково зруйнованої текстової інформації.

4. Необхідний ступінь захисту цілісності саме змісту інформації є основою для розробки методологічних основ і взаємопов'язаного комплексу методичних рекомендацій, для розробки вимог до системи захисту інформації й оцінки ступеня захисту на всіх фазах її опрацювання, контролю за її витоком, а також створення багаторівневої системи захисту.

При цьому необхідно зменшити вплив ЗМІ супротивника (на сьогодні це Росія, на наше суспільство).

Чого лише варті численні російські фільми та серіали, якими були заповнені телеекрани України і нав'язували кремлівський "правильний" погляд на життя. Слід ще враховувати, що сьогодні на

ISSN 2074-9481
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (31), 2016р.

протидію російським ЗМІ Україна нічого не протиставляє. На окупованих територіях Донбасу та Криму немає достатнього обсягу радіо та телемовлення з України. Також дуже мало інформації отримують закордонні слухачі.

Відмітимо, що телеканал Russia Today, який охоплює супутниковим мовленням територію практично усіх континентів, доступний у мережах кабельного телебачення у більшості країн Європи.

Професійні журналісти цього каналу із сучасних телестудій доброю англійською мовою несуть у широкі маси новини, коментарі, аналітику, подані, звичайно, у вигідному для Росії світі.

Повідомлення про вбивства у Росії правозахисників та журналістів, розгін демонстрацій демократичної опозиції чи дебоші неонацистів на екрані там не показують.

Цій пропаганді піддаються в Росії та світі не тільки звичайні люди, а й чимало тих, хто творить громадську думку і впливає на неї: зірки естради та кінематографу, бізнесмени, чиновники та ін. Російська пропаганда має на меті посилити свої моральні позиції, принижуючи українців. Відтак, ситуація складається не на користь України. Адже росіяни, як це ми вже відмічали, висвітлюють події в Україні на користь собі, щоб завоювати якомога більшу частину прихильників так званих "ДНР", "ЛНР" і Криму. А це шлях до розколу країни та пряма загроза нашому іміджу в очах демократичного світу. Росіяни вміло маніпулюють українською аудиторією за допомогою ЗМІ та дезорієнтують суспільство. Російські журналісти сьогодні висвітлюють інформацію про Україну, ігноруючи принципи та етичні засади журналістики, оскільки застосовують прийоми дезінформації та викривлення інформації.

Вразливість українського медіапростору до інформаційної війни з боку Росії породжена такими причинами:

1. В Україні не контролюється виникнення нових електронних ресурсів. Відтак, чи не щодня з'являються нові Інтернет-медіа, спрямування яких досить часто має антиукраїнський, пропагандистський характер.

2. Вільне і досить активне проникнення в супутникові ЗМІ, соціальні мережі та електронну пошту пропагандистських матеріалів.

3. Україна не повною мірою може протистояти вірусам та шкідливому програмному забезпеченню, що поширюється російськими хакерами.

4. У Росії на відмінну від України з'явилося чимало різноманітних розробок, спрямованих на пропаганду та маніпулювання свідомістю. Розвиток цієї сфери у нас на початковому рівні і немає ефективних засобів протидії агресивним сигналам, які використовує Росія.

5. Неналежною є підготовка фахівців до ведення інформаційної війни в ЗМІ. Українські вищі навчальні заклади не готують фахівців з кіберзахисту, а якщо у них навіть і є поодинокі спецкурси з таких дисциплін, то вони викладаються дуже поверхнево і в них мало уваги приділяють підготовці фахівців з технічного і криптографічного захисту інформації.

6. Немає відповідної джерельної бази, яка б надавала доступ до інформації про стратегію і тактику ведення інформаційної війни. Адже якщо проаналізувати наявність відповідної літератури, яка вийшла за часів Незалежної України, то її обмаль, а кількість фахівців з цього питання – мізерна.

У світі останніх подій Україна не має достатніх засобів та ресурсів для ведення у «сучасному форматі» інформаційної війни (протидіяти її впливам).

У ході проведеного дослідження було сформовано рекомендації щодо протистояння у інформаційній війні, а саме:

1) підсилити державний контроль за інформаційним простором України;

2) більш оперативно координувати інформаційний вплив на вразливі елементи інформаційної системи противника;

3) розробляти методи і засоби протистояння інформаційним акціям ворога для зменшення сфери його впливу;

4) використовувати комплексний підхід при формуванні стратегії інформаційної війни, тобто поєднувати суто інформаційні методи впливу з економічними, військовими, політичними і т. д.

Висновки

Аналіз факторів інформаційних впливів та протидії інформаційній зброї дозволяє зазначити наступне:

1. Інформація буває позитивною і негативною. Позитивна (конструктивна) інформація прагне довести до особистості (людини) певні переконання у доступній формі. Вона повинна сприяти соціальній гармонії, злагоді, вихованню людей відповідно до загальноприйнятих цінностей. Позитивна інформація виконує виховну та інформаційну функції в суспільстві. Вона здійснюється в інтересах тих, кому адресована, а не обмеженого кола зацікавлених осіб. Позитивна інформація не переслідує маніпулятивних цілей.

Метою негативної пропаганди інформаційних впливів є розпалювання соціальної ворожнечі, ескалація соціальних конфліктів, загострення суперечок у суспільстві. Це дозволяє роз'єднати людей, зробити їх слухняними волі нападника.

2. Проблема інформаційної війни Росії проти України – питання надзвичайно гостре. На нашу думку, для того, щоб протидіяти російській інформаційній ескалації в Україну слід:

− підвищити ефективність політики інформаційної безпеки в галузі оборони, а відтак вдосконалити і посилити відповідні структури держави;

− перешкоджати маніпулятивним технологіям супротивника, які застосовують для впливу на суспільну свідомість;

− вдосконалювати методи протидії інформаційним впливам та захисту державних інформаційних ресурсів.

3. Українці не мають іншої альтернативи ніж гідно і адекватно відповідати на інформаційні виклики сучасності. Бо лише так в умовах глобальних інформаційних впливів можна відстоювати власні інтереси.

Література

[1] M. Libicki, *Conquest in cyberspace. National security and information warfare*. - Cambridge, 2007. – 207p.

[2] І. С. Іванченко, *Забезпечення інформаційної безпеки держави* / Іванченко І. С., Хорошко В. О., Хохлачова Ю. Є., Чирков Д. В. – К.: ПВП "Задруга", 2013. – 170 с.

[3] В. О. Хорошко, *Особливості застосування сучасної інформаційної зброї* / Хорошко В. О, Козел Т. І., Ярошенко О. О. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. Вип 1(29), 2015. – С. 9-15.

[4] В. В. Бойко, *Устная пропаганда: критерии, показатели, условия эффективности* / Бойко В. В. – Л.:Лениздат, 1983. – 98 с.

[5] С. А. Нилус *Протоколы Сионских Мудрецов: Всемирный тайный заговор*/ изд. Берлинъ, 1922, с. 125.

[6] А. Зиновьев, *Русский єксперемент* / L'Age d'Homme — Наш дом, 1995. — 448 с.

[7] В. В. Балабін, *Концептуальні засади захисту системи інформаційно-аналітичного забезпечення завдань інформаційної боротьби як складової воєнної безпеки* / Балабін В. В., Замаруєва І. В., Пампуха І. В. // Вісник КНУ ім. Т. Шевченка. Військово-спеціальні науки, №22, 2009. – С. 30-33.

[8] А. О. Рось, *Концептуальні засади моделювання інформаційної боротьби* / Рось А. О., Замаруєва І. В., Петров В. Л. // Наука і оборона, 2000, №2. – С. 47-53.

[9] H. Lasswell, A. Kaplan, *Power and Society: A Framework for Political Inquiry*. / New Haven, 1950. P. 75.

[10] В. А. Хорошко, *Кибертерроризм и информационная безопасность* / Хорошко В. А., Шелест М. Е. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, Вип. 1(27), 2014. – С. 9-14.

[11] Е. Ефон [Ел. Ресурс]: old.niss.gov.ua/ book/lity/007_5.html

References

[1] M. Libicki, *Conquest in cyberspace. National security and information warfare*. - Cambridge, 2007. ¬– 207p.

[2] I. S. Ivanchenko, *Zabezpechennia informatsiinoi bezpeky derzhavy* / Ivanchenko I. S., Khoroshko V. O., Khokhlachova Yu. Ye., Chyrkov D. V. – K.: PVP "Zadruha", 2013. – 170 s.
[3] V. O. Khoroshko, *Osoblyvosti zastosuvannia suchasnoi informatsiinoi zbroi* / Khoroshko V. O, Kozel T. I., Yaroshenko O. O. // Pravove, normatyvne ta metrolohichne zabezpechennia system zakhystu informatsii v Ukraini. Vyp 1(29), 2015. – S. 9-15.
[4] V. V. Boiko, *Ustnaia propahanda: kryteryy, pokazately, uslovyia эffektyvnosty* / Boiko V. V. – L.:Lenyzdat, 1983. – 98 s.
[5] S. A. Nylus *Protokolы Syonskykh Mudretsov: Vsemyrnыi tainыi zahovor*/ yzd. Berlynъ, 1922, s. 125.
[6] A. Zynovev, *Russkyi yeksperement* / LAge dHomme — Nash dom, 1995. — 448 s.
[7] V. V. Balabin, *Kontseptualni zasady zakhystu systemy informatsiino-analitychnoho zabezpechennia zavdan informatsiinoi borotby yak skladovoi voiennoi bezpeky* / Balabin V. V., Zamaruieva I. V., Pampukha I. V. // Visnyk KNU im. T. Shevchenka. Viiskovo-spetsialni nauky, #22, 2009. – S. 30-33.
[8] A. O. Ros, *Kontseptualni zasady modeliuvannia informatsiinoi borotby /* Ros A. O., Zamaruieva I. V., Petrov V. L. // Nauka i oborona, 2000, #2. – S. 47-53.
[9] H. Lasswell, A. Kaplan, P*ower and Society: A Framework for Political Inquiry*. / New Haven, 1950. P. 75.
[10] V. A. Khoroshko, *Kyberterroryzm y ynformatsyonnaia bezopasnost* / Khoroshko V. A., Shelest M. E. // Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini, Vyp. 1(27), 2014. – S. 9-14.
[11] E. Efon [El. Resurs]: old.niss.gov.ua/ book/lity/007_5.html.

Реферат

Хорошко Владимир, Хохлачова Юлія, Прокофьєв Михайло

Концепція застосування інформаційних впливів та протидія інформаційній зброї

Розробка концепції протидії інформаційним впливам для інформаційно-аналітичного забезпечення (ІАЗ) випливає безпосередньо з аналізу цих впливів. Запропоновані концепції захисту ІАЗ відбивають технічні аспекти захисту саме людини або суспільства в процесі аналітичного опрацювання нею інформаційного матеріалу.

Інтенсивність модифікації навколишнього світу часто не залишає інформаційній системі або суспільству можливості вийти з запропонованих їй сценаріїв поведінки.

В умовах, коли час інформаційної протидії між системами малий (не перевищує середнього часу життя елементів системи), і є система, яка підлягає нападу, а система-супротивник володіє модельованими базовими елементами, слід запропонувати алгоритм інформаційного впливу, що має назву «алгоритм, який завжди перемагає».

Наявна на сьогоднішній день теорія алгоритмів цілком дозволяє пояснити, яким чином може здійснюватися автоматичне створення програм для певних предметних областей.

Усі зазначені в роботі моделі не дають змогу оцінити "міру важливості" новин щодо згадувань інших подій у новинах ЗМІ. Для визначення пріоритетності наведених новин порівняно з іншими новинами пропонується виконати побудову інших моделей – моделі важливості та моделі поінформованості.

У ході проведеного дослідження було сформовано рекомендації щодо протистояння інформаційній війні: підсилення державного контролю за інформаційним простором України; координація інформаційного впливу проти вразливих елементів інформаційної системи противника; створення методів і засобів протистояння інформаційним акціям ворога для зменшення сфери його впливу; використання комплексного підходу при формуванні стратегії інформаційної війни, тобто поєднання суто інформаційних методів впливу з економічними, військовими, політичними і т. д.

Аналіз факторів інформаційних впливів та протидія інформаційній зброї дозволяє зазначити наступне: інформація буває позитивною і негативною. Для

того, щоб протидіяти російській інформаційній ескалації в Україну, слід:

− підвищити ефективність політики інформаційної безпеки в галузі оборони, а відтак вдосконалити відповідні структури держави;

− перешкоджати маніпулятивним технологіям, які застосовують для впливу на суспільну свідомість;

− вдосконалювати методи протидії інформаційним впливам та захисту інформації.

Хорошко Владимир, Хохлачова Юлия, Прокофьев Михаил

Концепция применения информационных воздействий и противодействие информационной оружия

Разработка концепции противодействия информационным воздействиям для информационно-аналитического обеспечения (ИАО) следует непосредственно из анализа этих воздействий. Предложенные концепции защиты ИАО отражают технические аспекты защиты именно человека или общества в процессе аналитической обработки ею информационного материала.

Интенсивность модификации окружающего мира часто не оставляет информационной системе или обществу возможности выйти из предложенных ей сценариев поведения.

В условиях, когда время информационного противодействия между системами мало (не превышает среднего времени жизни элементов системы), т. е. есть система, которая подвергается нападению и система-противник обладает моделируемыми базовыми элементами, можно предложить следующий алгоритм под названием «алгоритм, который всегда побеждает».

Имеющаяся на сегодняшний день теория алгоритмов вполне позволяет объяснить, каким образом может осуществляться автоматическое создание программ для определенных предметных областей.

Все указанные в работе модели не позволяют оценить "степень важности" новостей относительно упоминания других событий в новостях СМИ. Для определения приоритетности приведенных новостей по сравнению с другими новостями предлагается выполнить построение других моделей – модели важности и модели поинформированности.

В ходе проведенного исследования были сформированы рекомендации по противостоянию информационной войне: усиление государственного контроля за информационным пространством Украины; координация информационного воздействия против уязвимых элементов информационной системы противника; создание методов и средств противостояния информационным акциям врага для уменьшения сферы его влияния; использование комплексного подхода при формировании стратегии информационной войны, то есть сочетание чисто информационных методов воздействия с экономическими, военными, политическими и т. д.

Анализ факторов информационных воздействий и противодействие информационному оружию позволяет сформулировать следующее: информация бывает положительной и отрицательной; для того, чтобы противодействовать российской информационной эскалации на Украине надо:

− повысить эффективность политики информационной безопасности в области обороны, поэтому усовершенствовать соответствующие структуры государства;

− препятствовать манипулятивным технологиям, применяемым для влияния на общественное сознание;

− совершенствовать методы противодействия информационным воздействиям и защиты информации.

Khoroshko Vladimir, Hohlacheva Yulia, Prokofiev Mykhailo

Concept of information impact and response information weapons

Developing the concept of counter information actions for information-analytical software (IAS) follows directly from the analysis of these impacts. The proposed concept of protection IAS reflect the technical aspects of protection is a person or society in the analytical study of its information material.

The intensity of the modification of the world often leaves the public information system or to exit the scripts offered to her behavior.

At a time when time information counter between systems is small (less than the average lifetime of the elements of the system) is a system that subject attack and system-enemy has modeled the basic elements, we propose the following algorithm entitled "algorithm that always wins."

The currently available algorithms theory allows fully explain how the automatic creation can be done for specific subject areas.

All of the models in work do not allow to estimate "as important" news about other events of mentions in the news media. To prioritize these news compared to other news offered to perform the construction of other models - models and models continue the importance of awareness.

In the course of the study was formed recommendations on information war confrontation, strengthening state control over the information space of Ukraine; coordination of information influence against the vulnerabilities of information systems of the enemy; creation of methods and means of information confrontation enemy actions to reduce its sphere of influence; use an integrated approach in shaping the strategy of information warfare, ie the combination of purely informational methods to influence the economic, military, political, etc.

Analysis of the factors and information actions counteracting weapons information allows us to formulate the following: information is positive or negative; in order to counter the Russian news escalation in Ukraine should be:

− increase the effectiveness of information security policy in the field of defense, thus improving the relevant structures of the state;

− prevent manipulative technologies use to influence the public consciousness;

− improve countermeasures informational influences and information security.

Відомості про авторів

Хорошко Володимир Олексійович

Освіта: вища, Київський інститут інженерів цивільної авіації, інженер за фахом «Технічна експлуатація авіаційного радіоелектронного обладнання» (1968).

Місце роботи: Національний авіаційний університет, професор, д.т.н. (1992).

Область знань: захист інформації.

Наукові інтереси: інформаційна безпека, системи захисту інформації.

Хохлачова Юлія Євгеніївна

Освіта: вища, Національний авіаційний університет, спеціаліст за фахом «Захист інформації з обмеженим доступом та автоматизація її обробки» (2004).

Місце роботи: Національний авіаційний університет, професор, к.т.н. (2015).

Область знань: захист інформації.

Наукові інтереси: інформаційна безпека, системи захисту інформації.

Email: *hohlachova@gmail.com*

Прокофьєв Михайло Іванович

Освіта: вища, Київський політехнічний інститут, радіоінженер за фахом «Конструювання та виробництво радіоелектронної апаратури» (1972).

Місце роботи: Національний технічний університет України «Київський політехнічний інститут», директор Науково-дослідного центру «ТЕЗІС», к.т.н. (2014).

Область знань: системи захисту інформації.

Наукові інтереси: інформаційна безпека, системи захисту інформації, проектування радіоелектронної апаратури та систем.

Email: *pmi@tesis.kiev.ua*