УДК 659.3

Л.О. Комарова

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ ЯК ШЛЯХ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ У КРИЗОВИХ СИТУАЦІЯХ

На підставі аналізу факторів інформаційного впливу були висунуті вимоги до системи захисту інформаційно-аналітичного забезпечення. А саме: випереджувальне володіння ситуацією на основі аналізу всієї доступної інформації у порівнянні з існуючими технологіями; орієнтація на обробку знань (тобто змісту інформації), а не текстів (форми інформації); орієнтація на комплексну автоматизацію всіх етапів аналітичного опрацювання інформації;система захисту інформаційного ресурсу має забезпечувати оцінку інформації на достовірність, повноту і об‘єктивність. Розкрито шляхи забезпечення висунутих вимог.

Ключові слова: інформаційно-аналітичне забезпечення; інформаційна боротьба; інформаційний ресурс; інформаційний вплив; інформаційні технології.

Вступ

Досвід останніх збройних конфліктів показує, що одним з найважливіших механізмів війни шостого покоління стає революція у військовій справі, яка завдяки новітнім інформаційним технологіям свідчить про те що інформаційні війни стали категорією воєнного мистецтва. Перший досвід ведення інформаційної боротьби в оперативному масштабі, як однією із складових військового протиборства, був придбаний у війні в зоні Перської затоки в 1991 році. Тоді багатонаціональні сили, використовуючи методи радіоелектронної й вогневої протидії, здійснили блокування практично всієї інформаційної, у тому числі й військової системи Іраку.

Сучасна воєнна доктрина США (концепція Force XXI) до сфер ведення бойових дій крім вже традиційних: землі, моря, повітря та космосу, включає і інформаційний простір, при цьому останній набуває вирішального значення. Стратегічна задача США визначена як досягнення світового лідерства в інформаційній сфері за рахунок розширення можливостей щодо обробки інформації в існуючих та створюваних системах [1]. Основними об‘єктами ураження у війнах майбутнього будуть інформаційна інфраструктура та психологія противника. Фізична окупація території не потрібна. Розгалужується саме поняття перемоги: такою вважається безперечна перевага в управлінні інформаційними ресурсами противника. Перевага над противником буде досягатися через перевагу в одержанні інформації, мобільності, оперативності її обробки та швидкості реакції, у точному вогневому й інформаційному впливі в реальному масштабі часу по численних об'єктах його економіки, військових об'єктах і при мінімально можливому ризику для своїх сил і засобів.

Основна частина

Зараз уже ясно, що інформаційна боротьба стає тим фактором, що вплине на саму війну майбутнього, її початок, хід і результат. Володіння інформаційними ресурсами противника стає таким же неодмінним атрибутом, як у минулих війнах володіння силами й засобами, озброєнням, боєприпасами, транспортом тощо. Перемога засобами інформаційної боротьби у війнах майбутнього фактично приведе до досягнення стратегічних і політичних цілей війни, що буде адекватно розгрому збройних сил противника, заволодінням його територією, руйнуванням його економічного потенціалу й скиненню політичного ладу. Таким чином, розробка концептуальних засад побудови системи інформаційно-аналітичного забезпечення в інтересах безпеки прийняття управлінських рішень у кризовій ситуації є актуальною **науковою** задачею.

Під поняттям **інформаційно-аналітична діяльність** будемо розуміти процес створення нового інформаційного продукту на підставі **аналізу** змісту всієї доступної інформації, **інтегрування знань** про предметну галузь і знань, отриманих із інформаційних джерел, **узагальнення знань** в інтересах прийняття управлінських рішень і синтезу вихідного аналітичного документа.

При цьому інформаційні джерела мають наступні характеристики:

- значні обсяги інформації;
- інформація відносно заданої теми представлена різними мовами;
- інформація містить величезний обсяг фактів, які поступають без будь-якої логічної послідовності відносно вирішуваного завдання;
- факти можуть бути як достовірними, так і містити дезінформацію;
- інформація, як правило, є надмірною з одних аспектів і неповною - з інших.

Умови, в яких працюють фахівці, визначаються:

- обмеженістю часу на підготовку та укладання аналітичних документів;
- великими щодобовими обсягами поточної інформації;
- великими обсягами "накопиченої" інформації;
- різнорідністю джерел інформації;
- надмірністю інформації за одними аспектами й неповнотою за іншими;
- нерівномірністю розподілу інформації за тематичними рубриками;
- невизначеністю інформації;
- наявністю спотвореної й хибної інформації, в тому числі й дезінформації;
- наявністю частково зруйнованої і викривленої інформаціїє

В таких умовах фахівцю-аналітику потрібно отримати найкращу відповідь при певних обмеженнях часу і вхідних даних. Експерти Американського розвідувального співтовариства так оцінюють роботу аналітиків: "Робота аналітика - це: діяти без свідків; робити пропозиції; враховувати думку інших; оцінювати альтернативні сценарії; прогнозувати напрямки і результати; відповідати політикам; оцінювати зацікавленість власної сторони (тобто державні інтереси), бути об'єктивним (давати свій аналіз без політичної забарвленості)".

Кінцевий інформаційно-аналітичний продукт має задовольняти як інформаційним вимогам: своєчасність, достовірність, повнота, адекватність, аргументованість, так і вимогам психологічного сприймання інформації з боку особи, яка приймає рішення: об'єктивність, всебічність, переконливість, ясність, лаконичність.

Етап **аналізу інформації** включає відповіді на питання:

Що нового в цій інформації? Які нові моменти з'явилисяв характеристиці проблеми?

Чому це трапилось?

Які цілі, наміри, мотивація учасників подій?

Які фактори можуть впливати на ситуацію?

Чи усвідомлюють ці фактори учасники подій? Чи є в них програма або стратегія для подолання або використання цих факторів?

Від чого може залежати успіх або провал розвитку подій для учасників?

Які можуть бути наслідки як для учасників подій, так і для власної сторони?

Як сприйметься розвиток подій іншими зацікавленими сторонами?

Яких заходів можуть задіяти основні учасники подій ?

Які можуть бути альтернативні сценарії розвитку подій?

Етап **інтегрування знань** включає:

оцінку інформації на достовірність, яка полягає в оцінці джерела інформації, оцінці збирача інформації, оцінці змісту інформації на протиріччя та наявність дезінформації;

оцінку актуальності інформації, яка полягає виокремленні важливої інформації від другорядної;

оцінку інформації на повноту і змістову цілісність, яка поступає із різнорідних джерел.

Оцінка збирача інформації включає: характеристику робітника; його можливості та здібності; професійні навички; загальнокультурний і мовний рівень; де і яким чином можна перевірити збирача інформації. Оцінка інформації включає:точність інформації; відповідність попереднім повідомленням; відповідність змісту інформації інтересам користувача; повнота (що ще потрібно знати); достовірність (наоснові співставлення з попередніми оцінками щодо джерела і збирача); які висновки та питання випливають з інформації; де можна знайти додаткову інформацію.

Оцінка інформації на достовірність включає виявлення суперечливої інформації, втому числі і дезінформації. Суперечливість інформації може проявлятися в наступних аспектах:

– суперечливість опису множини фактів реальній дійсності;

– суперечливість оцінки фактів різними джерелами;

– суперечливість оцінки подальшого розгортання подій (прогнозування, побудова альтернативних сценаріїв тощо) в процесі узагальнення та інтегрування інформаційного матеріалу.

За словами американського вченого, засновника фреймових структур, з точки зору формальної теорії будь-яка неструктурована інформація (до якої відносять і ПМТ) є надмірною, неповною і суперечливою одночасно. Суперечливості в тексті можуть мати як навмисний, так і ненавмисний характер. Для системи захисту інформації важливим є питання визначення кордонів між природною суперечливістю інформації та навмисним викривленням інформації. Цілеспрямоване викривлення інформації з метою нав‘язування вигідних для протидійної сторони рішень будемо називати ***дезінформацією.*** За функціональним призначенням до дезінформації відносять і тенденційно подану інформацію [2]. З формальної точки зору ця інформація не є суперечливою, але вона однобічно висвітлює певні факти (події). Тобто, формально така інформація є неповною відносно об‘єктивного опису реальної дійсності.

Навмисне викривлення інформації, як правило, базується на методах:

– приховування частини інформації,

– нав‘язування "бажаної" інформації.

Сутність дії першого методу полягає в тому, що ознаки, які дають максимальний внесок в розпізнавання ситуації, пригнічуються. Сутність дії другого методу полягає в тому, що імітуються ознаки, які дають максимальний внесок в розпізнавання хибної ситуації. На рис.1. наведені оцінки умовних кордонів дезінформації та природної суперечливості для системи захисту при розпізнаванні певних ситуацій.

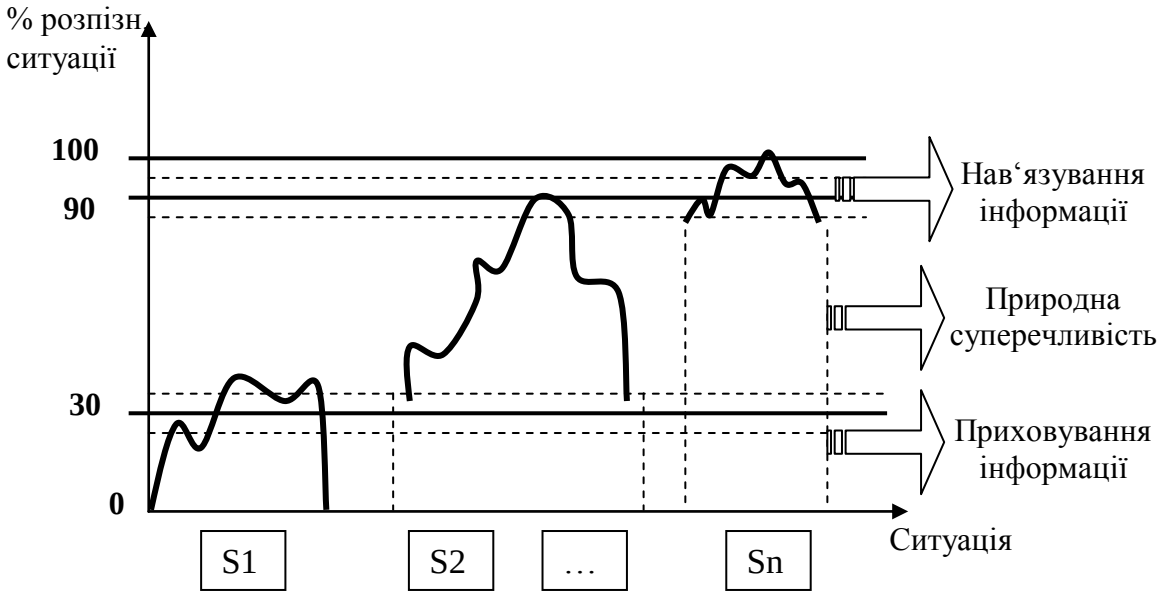

Рис. 1. Оцінки умовних кордонів дезінформації

Оцінка інформації на повноту має включати:

– зовнішню оцінку інформації, яка полягає у перевірці наявності більш ніж одного джерела за певною змістовою інформацією та незалежності цих джерел. Якщо інформація відбивається лише водному джерелі (а це характерно для закритої інформації), або джерела

інформації знаходяться в певній кореляції, то такій інформації має надаватися певний ваговий коефіцієнт дезінформування;

– прагматичну оцінку інформації на повноту, тобто визначення всіх необхідних даних (фрагментів) знань для вирішення певної прикладної задачі.

Задача виявлення дезінформації є складною і багатоаспектною задачею [3], розв‘язання якої потребує урахування багатьох параметрів, серед яких:

– визначення якісних показників, які характеризують дезінформацію;

– визначення особливостей організаційної структури проходження розвідувальних відомостей від джерела до кінцевого користувача (побудова 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 повідомлень (тобто *звідки? куди? кому? від кого? коли?* надійшло певне інформаційне повідомлення) та методик їх використання при оцінці достовірності інформації;

– дослідження інформаційних моделей суб‘єкта, об‘єкта та збирача інформації тощо.

Крім того, в системі захисту інформації слід враховувати і викривлення інформації, яке проявляється в результаті помилок передачі інформації [3].Для цього в системі має бути передбачена процедура відновлення змісту інформації. Передбачається, що об'єктом захисту є зміст природно-мовної інформації (ПМІ), носіями якої виступають фізичні поля і сигнали і яка може бути перетворена до подання в текстовій формі в ЕОМ. Вибір об'єкта захисту обумовлений такими міркуваннями.

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

2. З точки зору протидії технічній розвідці захист ПМІ (як мовної, так і текстової) потрібно здійснювати таким чином, щоб був забезпечений необхідний ступінь безпеки цілісності її змісту. Розрізнене слово або фрагментарні відомості, які змістовно між собою не пов'язані, мало кого цікавлять. З іншого боку, якщо цю розрізнену інформацію накопичувати достатньо довго, то можна скласти змістовно-цілісну інформаційну модель певного об'єкту, події або явища, але для цього буде потрібно час. Останнє може бути чинником для визначення вимог до системи технічного захисту (СТЗ) природно-мовної інформації.

3. Аналіз стану теоретичного доробку в області автоматизації обробки природно-мовної текстової інформації дозволяє стверджувати, що при відповідному їхньому розвитку можна розробити методичні рекомендації і створити програмні засоби оцінки ступеня порушення цілісності її змісту, а також відновлення змісту перекрученої або частково зруйнованої текстової інформації. Програмні засоби відновлення змісту перекрученої текстової інформації в даному випадку розглядаються як засоби технічного захисту інформації.

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

Системність припускає наявність деякого системо твірного фактора, який забезпечує якісне вирішення покладених на систему задач. У даному разі в якості такого фактора пропонується когнітивний підхід, який припускає, що в основу функціонування комплексної СТЗ ПМІ покладено моделювання процесу розуміння людиною (системою) текстової інформації і її аналізу на змістову пов’язаність і повноту. При цьому розуміння текстової

інформації трактується як її інтерпретація людиною (системою) шляхом занурення в систему знань, якою вона володіє. Визначення когнітивного підходу в якості системо твірної основи дозволяє створити єдину методологічну основу й інструментальні засоби для комплексної автоматизації вирішення задач захисту цілісності змісту ПМІ.

Відокремлення актуальної (важливої) інформації від другорядної передбачає відповіді на питання: *Що хоче знати замовник?Що потрібно знати замовнику?*

Етап узагальнення включає: усунення дублюючої інформації; перехід на поняття більш загального значення.

Етап синтезу включає: визначити загальну картину; зробити попередні висновки; побудувати логічну структуру документа; використовувати мовні конструкції відповідно стилю вихідного документа; висловлювати свої думки ясно і лаконічно; використовувати активний залог; самостійно редагувати; знати, що потрібно замовнику.

В технологічному плані система інформаційно-аналітичного забезпечення підтримки прийняття рішенн має забезпечувати наступні функції інформаційно-аналітичної діяльності:

попередній пошук, відбір і класифікація інформації під цільову настонову вихідного аналітичного документа;

автоматичний переклад різномовної інформації українською мовою;

реферування різномовної інформації українською мовою;

інтегрування й узагальнення інформації, отриманої із різних джерел, відносно предметної галузі й цільової настанови вихідного аналітичного документа;

аналіз інформації на цілісність, відновлення її змісту (у разі потреби), виявлення дезінформації.

Автоматизація зазначених функцій на наш погляд має базуватися на принципах, які необхідно покласти в основу розробки системи автоматизації інформаційно-аналітичної діяльності. Під поняттям **принципи автоматизації інформаційно-аналітичної діяльності** будемо розумітизагальні науково обґрунтовані положення, правила щодо автоматичної обробки інформації. Принцип завжди можна висловити формулою — «роби так...».

Принцип універсальності передбачає відкритість системи відносно нових вхідних мов та прикладних задач, забезпечується відокремленням програмного забезпечення від даних (інформаційного забезпечення); відокремленням знань про мову від знань про предметну галузь; відокремленням знань про предметну галузь від знань про вирішувану задачу.

Принцип інтегрованості передбачає сумісну автоматичну обробку різнорідної інформації (дані космічної розвідки, текстову інформацію, аудіо та відеоінформацію тощо), забезпечується модульною організацією програмного забезпечення; єдиною базою знань з предметної галузі для різнорідної інформації; узгодженими протоколами обміну інформації.

Принцип об’єктивності передбачає автоматизацію інтелектуальних функцій офіцера-аналітика, забезпечується знання-орієнтованим підходом до побудови системи автоматизації інформаційно-аналітичної діяльності; побудовою компонентів системи на засадах теорії штучного інтелекту.

Зазначені принципи дозволяють усунути загрози стану інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень, які визначені в таблиці 1.

Таблиця 1

Узагальнена модель інформаційних загроз стану інформаційно-аналітичного забезпечення

№	**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 (неповнота інформації)	Оцінка інформації на повноту
		Тенденціозне подання інформації	
3	Свідомість людини	Суб‘єктивність оцінки інформації	Автоматизація ІАД

На процес аналітичного опрацювання інформаційного матеріалу негативним чином можуть впливати запозичені інформаційні технології. Розробка власної інформаційної технології має задовольняти наступним вимогам: випереджувальне володіння ситуацією на основі аналізу всієї доступної інформації у порівнянні з існуючими технологіями; орієнтація на обробку знань (тобто змісту інформації), а не текстів (тобто форми інформації); орієнтація на комплексну автоматизацію всіх етапів аналітичного опрацювання інформації.

Підсистема ***захисту інформаційного ресурсу*** має включати розвинуті методи:

– стиснення інформаційних потоків на основі їх узагальнення з урахуванням вимог щодо її цілісності;

– виявлення суперечливої інформації, в тому числі і дезінформації;

– оцінки інформації на повноту.

Надмірність інформації виникає за рахунок повторювання однакових фрагментів знань в різних інформаційних джерелах, а також за рахунок “засмічування” корисної інформації купою зайвої. Отже, засоби стиснення інформації мають забезпечувати:

– семантичне стиснення інформації за рахунок усунення повторювальних фрагментів знань в різних джерелах;

– прагматичне стиснення інформації за рахунок відкидання тих фрагментів знань, які не відповідають цільовій настанові вирішення кінцевої прикладної задачі.

Ефективне вирішення цих завдань можливо лише на основі знання-орієнтованої технології.

При розглянутому підході до побудови комплексної системи захисту цілісності змісту ПМІ її ядром, як випливає з вищевикладеного, є система відновлення змісту частково зруйнованої або перекрученої ПМІ. Вона може бути використана не тільки для вирішення задач відновлення інформації, але і для вирішення задач контролю за витоком ПМІ по технічних каналах, для оцінки ступеня захищеності ПМІ і керування рівнем її захисту.

Захист людини (фахівця-аналітика) від перевантаження інформації полягає в автоматизації перелічених функцій стиснення інформації. В американській настанові FM 100-34 [4] зазначається, що основним призначенням автоматизованої інформаційної системи є звільнення командира від купи зайвої інформації. Суб‘єктивність сприймання інформації

можна вирішити за рахунок комплексної автоматизації задач ІАД на єдиній методологічній базі.

Висновки

Аналіз факторів інформаційного впливу дозволяє сформулювати вимоги до системи захисту інформаційно-аналітичного забезпечення завдань: власна інформаційна технологія має забезпечувати: випереджувальне володіння ситуацією на основі аналізу всієї доступної інформації у порівнянні з існуючими технологіями; орієнтацію на обробку знань (тобто змісту інформації), а не текстів (тобто форми інформації); орієнтацію на комплексну автоматизацію всіх етапів аналітичного опрацювання інформації; система захисту інформаційного ресурсу має забезпечувати оцінку інформації на достовірність, повноту і об‘єктивність. Оцінка інформації на достовірність має включати виявлення суперечливої інформації, в тому числі і дезінформації. Оцінка інформації на повноту спирається на: зовнішню оцінку інформації, яка полягає у перевірці наявності більш ніж одного джерела за певною змістовою інформацією та незалежності цих джерел; прагматичну оцінку інформації на повноту, тобто наявність всіх необхідних даних (фрагментів) знань для вирішення певної прикладної задачі. Об‘єктивність інформації має забезпечуватися за рахунок комплексної автоматизації задач інформаційно-аналітичного забезпечення завдань на єдиній методологічній базі; захист людини (фахівця-аналітика) від перевантаження інформацією полягає в автоматизації функцій стиснення інформаційних потоків на основі їх узагальнення з урахуванням вимог щодо її цілісності.

Інструментально-технологічний комплекс автоматизації задач інформаційно-аналітичного забезпечення має забезпечувати реалізацію наступних основних функцій: цілеспрямований пошук потрібної текстової інформації в базі знань; класифікація різномовних текстових документів; інтегрування та узагальнення знань, які містяться в різномовних текстових документах; переклад оригінальних текстів українською мовою; формування рефератів різномовних текстів українською мовою; перевірка знань, які містяться в різномовних текстах та їх сукупності на логічну та семантичну сумісність і суперечливість; виявлення закономірностей і тенденцій в певній предметній області за різномовними текстами; формування аналітичних документів за вимогами користувача щодо їх змісту та обсягу.

Література

1. Воробьев И.Н., Круглов В.В. Основы военной футурологии. – М.: ВАФ, 1998. – 175 с.

2. Плет В. Стратегическая разведка. Основные принципы. – М.: Издательский Дом «Форум», 1997. – 376 с.

3. Комарова Л.О. Математична модель каналу зв’язку [Текст] / Комарова Л.О.// Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2008. –№15. – С. 160-168 .

4. Комарова Л.О. Інформаційне забезпечення комплексного керування захистом складних систем [Текст] / О.Б. Лантвойт, С.П. Гришин, Я.Я. Винярський, Л.О. Комарова // Сучасна спеціальна техніка. – К., 2011. – №2(25). – С.112 -117.

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

6. FM 100-34. Military Department of USA // Field Manual.– June, 1999.

Надійшла 19.04.2016 р. Рецензент: д.т.н., проф. Бурячок В.Л.