ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

В.В. Балабін, канд. філол. наук, доц.,
І.В. Замаруєва, д-р. техн. наук, проф.,
І.В.Пампуха, канд. техн. наук, доц.

КОНЦЕПТУАЛЬНІ ЗАСАДИ ЗАХИСТУ СИСТЕМИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ЗАВДАНЬ ІНФОРМАЦІЙНОЇ БОРОТЬБИ ЯК СКЛАДОВОЇ ВОЄННОЇ БЕЗПЕКИ

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.

On the basis of analysis of factors of information influence were pulled out system requirement security of the information-analytic providing. Namely: passing ahead domain a situation on the basis of analysis of all of accessible information by comparison to existent technologies; orientation on treatment of knowledge (I.e. maintenances of information), but not texts (forms of information); orientation on complex automation of all of the stages of analytical treatment of information; system of security of information resource must provide the estimation of information on validity, plenitude and objectivity. The ways of providing of the pulled out requirements are exposed.

Keywords: information-analitic providing; information warfare; information resource; information influence; information technologies.

Вступ. Досвід останніх збройних конфліктів показує, що одним з найважливіших механізмів війни шостого покоління стає не тільки революція у військовій справі, але й інформаційна революція, яка зараз переживає стадію формування. 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. Цей успіх не тільки окрилив США в розумінні ролі інформаційної боротьби, але й змусив задуматися над тим, як вийти з подібного стану, якщо така боротьба буде нав'язаною їм самим. Були проведені аналітичні дослідження й експерименти під керівництвом агентства інформаційної безпеки міністерства оборони США, які показали, що ступінь уразливості комп'ютерних систем і баз даних військового відомства США винятково висока. Проникнути в мозковий центр Пентагона виявляється не складно, тому що він має безліч виходів в інші інформаційні системи як усередині держави, так і за його межами.

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.

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 захисту системи інформаційно-аналітичного забезпечення завдань інформаційної боротьби є ***актуальною*** проблемою воєнної безпеки держави.

Основна частина. Розробка концепції захисту системи інформаційно-аналітичного забезпечення (ІАЗ) випливає безпосередньо з аналізу інформаційних впливів. Під інформаційним впливом будемо розуміти цілеспрямовані заходи інформаційного характеру, які спрямовані на зміну поведінки (реакції) людини або комп'ютерної системи, в інтересах протидіючої сторони. Зупинимось лише на тих видах інформаційного впливу, які безпосередньо впливають на процес прийняття рішень. Об'єктами впливу в процесі інформаційно-аналітичної діяльності (ІАД) можуть виступати: людина або комп'ютерна система. Вплив на комп'ютерні системи є предметом захисту з боку технічного захисту інформації. Підходи до розв'язання проблеми захисту людини в процесі ІАД на сьогодні відсутні навіть у постановочному плані.

Запропоновані концептуальні засади захисту ІАЗ відбивають технічні аспекти захисту саме людини (фахівця) в процесі аналітичного опрацювання нею інформаційного матеріалу. В табл. 1. в узагальненому вигляді наведені фактори впливу на ІАД та можливі заходи щодо захисту від зазначених загроз.

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.

Оцінка інформації на достовірність включає виявлення суперечливої інформації, в тому 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.

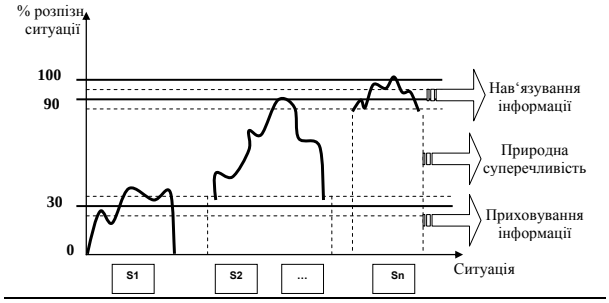

Рис. 1. Оцінка умовних кордонів дезінформації та природної суперечливості для системи захисту при розпізнаванні певних ситуацій

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 в одному 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 системотвірного 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 системотвірної основи дозволяє створити єдину методологічну основу й інструментальні засоби для комплексної автоматизації вирішення задач захисту цілісності змісту ПМІ. Сутність цього підходу полягає в наступному.

Текстова інформація підлягає лінгвістичному опрацюванню в ЕОМ, у процесі якої формується поняттєва структура (ПС) змісту вихідного тексту. Вона представляє собою деяку ієрархічну структуру, на верхньому рівні якої знаходяться найбільше загальні поняття і відношення між ними, кожний рівень, який знаходиться нижче, представлений поняттями і відношеннями, що конкретизують відповідні поняття і відношення вищого рівня. Кожне поняття і відношення в ПС супроводжуються характеристиками, які відбивають їхні властивості, модальності й інші їх аспекти; лінгвістичною інформацією, яка характеризує мовні засоби їх відображення у вихідному тексті; семантичною інформацією, що відбиває їх роль та інші характеристики (об'єкт, суб'єкт, тип відношення, спрямованість дії й ін.). Можливість її формування визначається наявністю відповідних знань у тезаурусі системи. При цьому не має принципового значення мова вихідного тексту тому, що ПС його змісту не залежить від того, якими мовними засобами цей зміст виражений. Природно, що це не стосується безпосередньо методів лінгвістичного аналізу, які враховують закономірності вираження знань засобами конкретної мови. Якщо текст змістово цілісний, тоді і ПС, як модель змісту тексту, теж буде цілісною. Якщо ж текст частково перекручений або зруйнований, то і відповідні фрагменти ПС теж будуть мати відбиток останнього. Але її подальше опрацювання в багатьох випадках дозволяє відновити зміст перекручених або зруйнованих фрагментів тексту. Наведемо елементарний приклад фрази: "*Ко_у водять по ко_у"*. Вже для такого простого випадку використання електронних словників для гарантовано правильної підстановки пропущених літер не допоможе. Але на основі аналізу семантичної ролі словоформ і контексту, відбитих у ПС, система в першому випадку підставить на місці пропуску літеру "*з",* а в другому – "*л".* Іншим прикладом може бути слово "*д_м",* у якому в якості пропущеної літери може бути одна з таких: *а, и, і.* Природно, що вибір правильної літери для відновлення пропущеної може бути здійснений на основі достатньо глибокого лінгвістичного аналізу контексту, а також, у разі потреби, шляхом залучення знань про предметну область. На практиці, звичайно, зустрічаються значно більш складні ситуації, наприклад, коли інформація, яка необхідна для відновлення змісту якогось фрагмента, міститься в попередніх або наступних фрагментах. Слід зазначити, що при запропонованому підході поняття, яке зустрілося на початку тексту і виявилося полісемічним або частково зруйнованим, може уточнюватися в інших фрагментах.

При відновленні змісту текстової інформації (як і при її руйнації) корисно також враховувати ту обставину, що різні словоформи вносять різний внесок в зміст тексту. Так, можна виділити змістово-значущі словоформи і їхні сполучення (суб'єкт, об'єкт і відношення між ними), перекручування або руйнація яких можуть призвести до того, що відновити їх зміст буде неможливо. Але навіть у цих випадках може допомогти аналіз інших фрагментів тексту (аналогічно тому, як людина намагається від-

новити зміст тексту на папері, який потрапив під дощ). Крім того, змістово-значущі словоформи нерівномірно розподілені у фразах (реченнях). Закономірності розподілу цих словоформ для різних мов також різні. Більш того, самі фрази також мають різну змістову цінність і існують певні закономірності їх розподілу у фрагментах. Так, змістово більш значущі речення, як правило, розміщені на початку абзаців.

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.

1. Воробьев И.Н., Круглов В.В. Основы военной футурологии. – М.: ВАФ, 1998, 175с. 2.Плет В. Стратегическая разведка. Основные принципы. – М.: Издательский Дом "Форум", 1997, – 376 с. 3. Рось А.О., Замаруєва І.В., Петров В.Л. Концептуальні засади моделювання інформаційної боротьби // Наука і оборона. 2000. -№2. -С. 47-53. 4. FM 100-34. Military Department of U.S.A // Field Manual.- June, 1999

Надійшла до редколегії 21.08.09

УДК 681.3

Г.Б. Жиров, канд. техн. наук

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ ПІДПРИЄМСТВ ВІЙСЬКОВО-ПРОМИСЛОВОГО КОМПЛЕКСУ

В статті розглядається питання захисту інформації в корпоративній мережі підприємства й необхідні організаційні міри для захисту технології обробки інформації. Запропонований підхід та алгоритм дій дозволяє зменшити імовірність несанкціонованого витоку інформації в мережі.

Ключові слова: захист інформації, промислове шпигунство, виток інформації.

In the article the question of protection of the information in a corporate network of the enterprise and necessary organizational measures for protection of technology of processing of the information is considered. The approach and algorithm of actions which allows to reduce probability of not authorised source of the information in a network is offered.

Keywords: information protection, industrial espionage, information leakage.

Постановка проблеми. На сьогоднішній день підприємства, корпорації, науково-дослідні установи, конструкторські бюро та інші організації дуже гостро стикаються з загальною проблемою захисту інформації. Це насамперед тому, що відбувається бурхливий розвиток нових технологій, особливо ІТ-технологій з одного боку, а з іншого боку наявності у суспільстві промислового шпигунства. Промислове шпигунство – одна з форм недобросовісної конкуренції, яка використовується на всіх рівнях економіки, починаючи з невеликих підприємств і закінчуючи державами. Основне призначення промислового шпигунства – економія засобів і часу, які потрібно витратити, щоб наздогнати конкурента, що займає лідируюче положення, або не допустити в майбутньому відставання від конкурента, якщо той розробив або розробляє нову перспективну технологію, а також щоб вийти на нові для підприємства ринки. Це справедливо і відносно міждержавної конкуренції, де до питань економічної конкурентоспроможності додаються і питання національної безпеки.

Незважаючи на те, що більшість інформації потрапляють до рук фахівців з офіційних джерел (публікацій, патентів, баз даних), інколи інформація просто викрадається. Промислове шпигунство може торкнутися будь-якого бізнесу, чиєю важливою складовою є інформація. Це і списки клієнтів, підписані угоди, особисті записи, дослідницька документація або плани-макети майбутнього продукту і т.п.