УДК 659.3

Замаруєва І.В., д.т.н.; **Барабаш О.В.,** д.т.н.; **Пампуха І.В.,** к.т.н.

АВТОМАТИЗАЦІЯ АНАЛІЗУ ЗМІСТУ ПРИРОДНО-МОВНИХ ТЕКСТІВ ЯК ШЛЯХ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ

Zamarueva I.V., Barabash O.V., Pampukha I.V. Automation of the analysis of the content of natural language texts as a way to ensure the safety of managerial decisions.

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-analytic providing; information warfare; information resource; information influence; information technologies.

Замаруєва І.В., Барабаш О.В., Пампуха І.В. Автоматизація аналізу змісту природно-мовних текстів як шлях забезпечення безпеки прийняття управлінських рішень.

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.

Замаруева И.В., Барабаш О.В., Пампуха И.В. Автоматизация анализа содержания естественно-языковых текстов как путь обеспечения безопасности принятия управленческих решений.

На основании анализа факторов информационного воздействия были выдвинуты требования к системе защиты информационно-аналитического обеспечения. А именно: опережающее владение ситуацией на основе анализа всей доступной информации в сравнении с существующими технологиями; ориентация на обработку знаний (т.е. содержания информации), а не текстов (формы информации); ориентация на комплексную автоматизацию всех этапов аналитической обработки информации; система защиты информационного ресурса должна обеспечивать оценку информации на достоверность, полноту и объективность. Раскрыты пути обеспечения выдвинутых требований.

Ключевые слова: информационно-аналитическое обеспечение; информационная борьба; информационный ресурс; информационное воздействие; информационные технологии.

Вступ

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 однієї із складових військового протиборства, було отримано 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: земля, море, повітря та космос, включає також інформаційний простір. При цьому останній набуває вирішального значення. Стратегічні завдання провідних країн світу визначені 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 побудови системи інформаційно-аналітичного забезпечення в інтересах безпеки прийняття управлінських рішень у воєнній сфері є актуальним науковим завданням.

Аналіз останніх досліджень та публікацій. Основна відмінність між відомими підходами до обробки природно-мовної інформації (ПМІ) полягає у способах представлення та аналізу змісту таких текстів. Перший підхід базується на припущенні, що основний зміст тексту визначається множиною ключових слів – термінів і понять, які до нього входять (Bag of Words) [2]. Такий підхід ігнорує лінгвістичну взаємозв’язність і семантику природної мови, однак дозволяє швидко виконувати операції обробки текстів за формальними ознаками. Обробка ПМІ за такого представлення змісту базується переважно на статистичних та ймовірнісних моделях.

Інший підхід полягає у логіко-семантичній обробці природно-мовної інформації, що передбачає визначення змісту текстів за рахунок аналізу їх граматики, використання баз знань і тезаурусів, які відображають семантичні зв’язки між окремими словами та групами слів [3]. У результаті такої обробки отримується формалізоване представлення змісту ПМІ, що дозволяє аналізувати його методами штучного інтелекту. Через суттєві витрати на підтримку баз знань і тезаурусів для кожної мови, тематики і виду документу, зазначений підхід застосовується, як правило, для вирішення вузькоспеціалізованих задач [4], до яких можна віднести і задачу виявлення кібернетичних загроз в окремій системі.

Аналіз відомих методів виявлення кібернетичних загроз дозволяє віднести їх до двох основних груп [5-8]:

- сигнатурні методи дозволяють виявляти загрози за умови відомих параметрів, які її характеризують, та граничних значень цих параметрів;

- методи виявлення аномалій передбачають розробку профілю «безпечної» роботи інформаційної системи та постійний моніторинг відхилення поточних даних від заданого профілю.

Перевагою сигнатурних методів є висока достовірність (низьке число хибних виявлень загроз) і невисокі затрати ресурсів. Але при цьому не забезпечується виявлення загроз, у яких відсутні характеристичні параметри.

Методи виявлення аномалій дозволяють виявляти як відомі, так і невідомі раніше загрози, однак не забезпечують високої достовірності такого виявлення. Це обумовлено тим,

що параметри загрози можуть співпадати з еталонними значеннями профілю «безпечної» роботи системи.

Для об'єднання переваг зазначених методів та компенсації притаманних їм недоліків застосовується принцип комплексування, що дозволяє забезпечити можливість виявлення як відомих, так і нових видів кібернетичних загроз; досягти високої достовірності виявлення та низької ресурсозатратності [7].

Метою статті є розробка концептуальних положень побудови системи інформаційно-аналітичного забезпечення в інтересах безпеки прийняття управлінських рішень у воєнній сфері.

Виклад основного матеріалу дослідження

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 однієї сторони та неповною – з іншої.

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 офіцеру-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, лаконічність.

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

Що нового в цій інформації? Які нові моменти з'явилися в 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 буде сприйматися 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 працівника; 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 (на основі 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, 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 [9]. 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 меж 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 [10], 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);

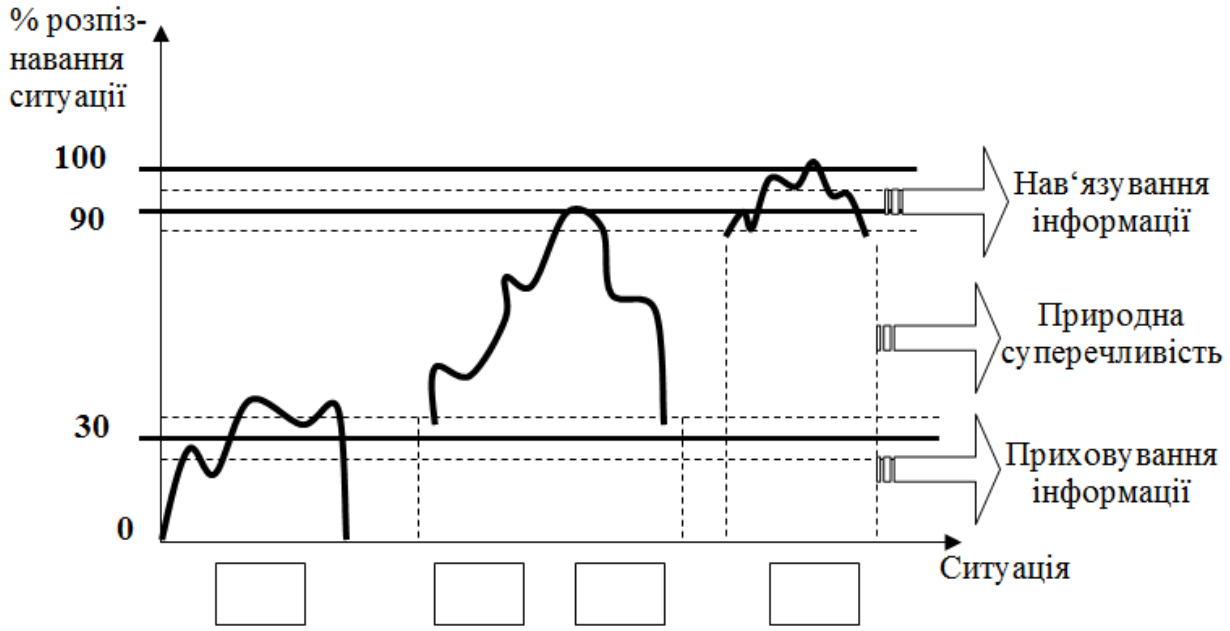

Рис. 1. Оцінки умовних меж дезінформації та природної суперечливості для системи захисту при розпізнаванні певних

– 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 [10]. 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 й сигнали, і яка може бути перетворена до подання в текстовій формі в ЕОМ. Вибір об'єкта захисту обумовлено 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.

Видокремлення 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 рішень має забезпечувати наступні функції інформаційно-аналітичної діяльності:

- попередній пошук, відбір і класифікація інформації під цільову настанову 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 розуміти загальні 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 (табл. 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 інформаційно-аналітичної діяльності

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 [11] 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 інформаційно-аналітичної діяльності 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.

Список використаної літератури

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

2. Большакова Е.И. Автоматическая обработка текстов на естественном языке и компьютерная лингвистика : учеб. пособие / Е.И. Большакова, Э.С. Клышинский, Д.В. Ландэ и др. – М.: МИЭМ, 2011. – 272 с.

3. Басипов А.А. Семантический поиск: проблемы и технологии / А.А. Басипов, О.В. Демич // Вестн. Астрахан. гос. техн. ун-та. Сер. управление, вычисл. техн. информ. – 2012. – № 1. – С. 104 – 111.

3. Манокін Є. В. Ідентифікація загроз / Є.В. Манокін // Оборонний вісник. – К.: 2012. – № 11-12, С. 19 – 22.

4. Ландэ Д.В. Основы интеграции информационных потоков: Монография. – К.: Инжиниринг, 2006. – 240 с.

5. Комар М.П. Ителлектуальная система обнаружения сетевых атак на информационные ресурсы на основе метода главных компонент / М.П. Комар // Системи обробки інформації. – Харків, ХУПС, 2011. – №8 (98). – С. 203 – 207.

7. Лукацкий А.В. Обнаружение атак. – 2-е изд. – СПб.: БХВ-Петербург, 2003. – 608 с.

8. Лаптев В.Н. Методика обнаружения и идентификации компьютерных атак в информационно-телекоммуникационных системах на основе метода индуктивного прогнозирования состояний / В.Н. Лаптев, О.В. Сидельников // Научный журнал КубГАУ. [Електронний ресурс] – 2012. – № 77(03). – Режим доступу: http://ej.kubagro.ru/2012/03/pdf/32.pdf.

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

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

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

Автори статті

Замаруєва Ірина Вікторівна - доктор технічних наук, професор, Державний університет телекомунікацій, Київ, Україна.

Барабаш Олег Володимирович - доктор технічних наук, професор, завідувач кафедри вищої математики, Державний університет телекомунікацій, Київ, Україна.

Пампуха Ігор Володимирович – кандидат технічних наук, доцент, Державний університет телекомунікацій, Київ, Україна.

Authors of the article

Zamaruyeva Iryna Viktorivna - sciences doctor (technic), professor, State University of Telecommunications, Kyiv, Ukraine.

Barabash Oleh Volodymyrovych - sciences doctor (technic), professor, head of Department of Mathematics, State University of Telecommunications, Kyiv, Ukraine.

Pampukha Ihor Volodymyrovych - candidate of Science (technic), State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 21.08.2017 р. Рецензент: д.т.н., доцент В.Є. Мухін