УДК 681.5:519.246:519.233.5:517.956.221(043.2)

Додонов О.Г., д.т.н.,
Ланде Д.В., д.т.н.,
Коваленко Т.В.

АРХІТЕКТУРА СИСТЕМИ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Інститут проблем реєстрації інформації НАН України
ipri@ipri.kiev.ua

Представлено технологічні та методологічні основи створення і застосування засобів підтримки прийняття рішень на основі сценарного підходу, архітектуру системи інформаційної підтримки, створення та використання онтологій для побудови сюжетів інформаційної протидії. Детально розглянуто методику аналітичного дослідження, що базується на використанні інструментальних засобів аналізу і візуалізації інформаційних потоків і часових рядів. Наведені архітектурні рішення можуть бути використані у системах, що базуються на застосуванні контент-моніторингу інформаційного простору та сценарному аналізі, а також при проведенні аналітичної та прогнозної діяльності

Ключові слова: сценарний підхід; система контент-моніторингу інформаційного простору; архітектура системи; онтологія понять; моніторинг інформаційного простору; аналітична обробка; інформаційний потік; часові ряди

Вступ

Створення автоматизованої системи інформаційної підтримки процесів протидії ворожим інформаційним компаніям, виконання заходів щодо відбиття деструктивних зовнішніх і внутрішніх інформаційних впливів – актуальна проблема сучасності, особливо в умовах ведення інформаційних війн [1-2].

В якості основних завдань такої системи розглянемо:

- побудову сценаріїв протидії інформаційним деструктивним впливам на основі деякої онтології понять;
- контент-моніторинг (безперервний змістовний аналіз) інформаційного простору з урахуванням знань експертів;
- виявлення закономірностей (трендів) і аномалій шляхом аналізу динаміки зміни значень окремих факторів;
- виявлення інформаційних впливів та інформаційних операцій;
- прогнозування розвитку інформаційних сюжетів та ситуацій;
- оцінка ефективності процедур інформаційної підтримки прийняття рішень.

Відповідно, для реалізації такої системи інформаційної підтримки процесів, пов'язаних, зокрема, з національною безпекою необхідно:

- створити онтологію понять предметної області (вузлів – факторів безпеки і відповідних причинно-наслідкових (казуальних) зв'язків – залежності факторів), визначити вид цільової функції безпеки об'єктів-вузлів цієї онтології залежно від значень факторів безпеки;
- постійно актуалізувати значення факторів безпеки і зв'язків залежно від результатів моніторингу інформаційного простору та знань експертів;
- визначати можливі сценарії на основі аналізу онтології і виявлення відповідних часткових онтологій;
- аналізувати динаміку зміни значень окремих факторів та зв'язків з метою виявлення закономірностей, прогнозування;
- постійно проводити оцінку ефективності проведеної інформаційної підтримки.

Для рішення цих завдань, передбачається, що система інформаційної підтримки повинна складатися з трьох основних підсистем (рис. 1): підсистеми введення онтології понять, підсистеми моніторингу інформаційного простору, підси-

стеми аналітичної обробки, та відповідних інтерфейсів з адміністраторами і користувачами.

Онтології понять предметної області

Онтологія в даному випадку являє собою функціональний аналог бази знань, що відбиває знання експертів про предметної області, тобто в якості вузлів графа онтології вибираються найважливіші фактори предметної області забезпечення безпеки, а в якості зв'язків – причинно-наслідкові зв'язки між факторами (з математичної точки зору – граф з направленими ребрами) [3]. Вузлам і зв'язкам приписуються числові значення, які в подальшому можуть коригуватися. Зв'язки також можуть мати різну вагу (силу впливу) і бути як позитивними (збільшення значення першого фактора приводить до збільшення значення другого чинника), так і негативними (збільшення значення першого фактора приводить до зменшення значення другого чинника).

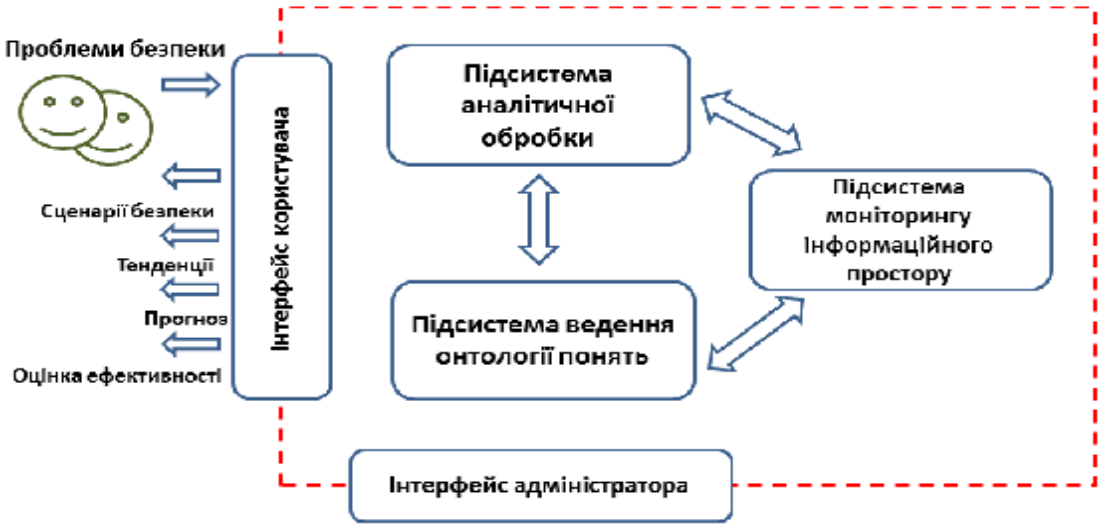

Рис. 1. Архітектура системи інформаційної підтримки

Онтології, як правило, складаються експертами, але на сьогодні можливо автоматизоване створення онтологій на базі аналізу текстових масивів (корпусів) відповідного змісту (масивів документації, повідомлень ЗМІ, науково-технічної інформації тощо).

На рис. 2 наведено набір базових модулів, що складають підсистему ведення онтологій.

Інструменти ведення онтологій – сучасні онтологічні редактори, а також спеціальні СУБД, орієнтовані на зберігання мережевих структур.

Рис. 2. Склад підсистеми ведення онтологій

Визначення можливих сценаріїв на основі аналізу онтології

Сценарії інформаційної підтримки, як правило, зв'язуються з певними факторами безпеки (найчастіше об'єктами і вразливостями). Після вибору цільових факторів сценарію в графі онтології виявляються підграфи (часткові онтології), найтісніше пов'язані з вибраними чинниками.

Вибір цільової функції, пов'язаної з цільовим об'єктом, здійснюється експертами. Найчастіше цільова функція, що залежить від значень факторів, лінійна, відрізняються лише коефіцієнти, які підбираються експертно, а потім ітеративно уточнюються під час експлуатації автоматизованої системи. Лінійна функція дозволяє спрощувати обчислення в разі великої розмірності простору факторів, однак, в деяких випадках через залежності факторів, цільова функція повинна приймати нелінійний вигляд.

Далі вирішується завдання часткової оптимізації цільової функції на обраних підграфах, тобто обчислюється цільова функція в залежності від змін факторів безпеки, що відповідають можливим сценаріями.

Динаміка зміни значень окремих факторів і зв'язків

Передбачається постійна актуалізація значень факторів безпеки і зв'язків між ними залежно від обсягів і змісту повідомлень, що з'являються в цільовому фрагменті інформаційного простору, і знань експертів. Для моніторингу інформаційного простору необхідно використовувати спеціалізовані системи контент-моніторингу *Web*-простору, соціальних медіа, ЗМІ тощо.

Коригування цільової функції може виконуватися експертами в залежності від зміни пріоритетів безпеки, зміни структури графа онтології. Крім того, в результаті використання даної автоматизованої системи можливе усунення деяких можливих вразливостей в інформаційному просторі, виявлення «прихованих» зв'язків, зміна існуючих зв'язків між факторами, створення додаткових зв'язків (у тому

числі, шляхом інформаційної протидії, впливу на реальні об'єкти інформаційної інфраструктури як власної , так і ймовірного противника).

Аналіз динаміки зміни значень окремих факторів безпеки і зв'язків в часі (як по їхньому відображенню в інформаційному просторі, так і внесених експертами) дозволяє виявляти деякі закономірності зміни цих факторів (періодичності, тренди, аномалії) шляхом застосування сучасних засобів цифрової обробки сигналів (регресійний, дисперсійний, вейвлет-аналіз тощо), виявляти можливі інформаційні операції шляхом порівняння з відповідними шаблонами їх динаміки, а також здійснювати прогнозування [4].

Оцінка ефективності інформаційної підтримки безпеки регіону з точки зору поставлених цілей дозволяє реалізовувати зворотний зв'язок, тобто коригувати цільову функцію, модифікувати онтологію, розширювати інформаційну та експертну підтримку, планувати подальший розвиток системи.

Контент-моніторинг інформаційного простору

Сьогодні мережа Інтернет утворює значимий динамічний сегмент інформаційного простору, інформаційні потоки, зміст та обсяги яких необхідно враховувати при проведенні аналітичних досліджень. Основним об'єктом аналізу при цьому є подієві або тематичні зрізи цих потоків – масиви інформаційних повідомлень, документів, що відповідають певним подіям або тематикам.

Завдання підсистеми моніторингу інформаційного простору наступні:

- моніторинг цільових об'єктів;
- знаходження релевантних тематичних повідомлень в інформаційному просторі;
- контроль медіаприсутності і медіаактивністю цільових об'єктів;
- виявлення нових об'єктів моніторингу;
- формування ретроспективних фондів для подальшого аналізу.

Для ефективного проведення інформаційно-аналітичних досліджень на основі аналізу контенту мережі Інтернет в рамках даної системи пропонується послідовність кроків, етапів обробки інформації. Сукупність таких етапів, що базуються на використанні необхідних і доступних інструментальних засобів, спеціальних прийомів, можна розглядати як методику, процедуру проведення дій, націлених на отримання аналітичних матеріалів, які можуть використовуватися для підтримки прийняття рішень (рис. 3).

Застосування системи контент-моніторингу інформаційного простору дозволяє проводити змістовний ретроспективний аналіз, виходити на відповідні публікації, події, сюжети, виявляти нові, раніше невідомі фактори безпеки та інформаційні взаємозв'язку.

Інформаційна база системи, що базується на використанні, серед іншого, мережевого контенту формується засобами контент-моніторингу. Ці кошти охоплюють величезні обсяги інформації (*Big Data*) з динамічно зростаючих інформаційних потоків при наявності шумовий інформації, слабо доступних ресурсів (*Hidden Web, Deep Web*), так званого «прихованого Інтернету» [6].

Рис. 3. Склад підсистеми моніторингу інформаційних ресурсів

Підсистема аналітичної обробки

Підсистема аналітичної обробки (на рис. 4 наведено її склад) являє собою аналітичний блок системи інформаційної підтримки, що забезпечує вирішення наступних завдань:

- визначення динаміки тематичних сюжетів;
- визначення критичних точок в динаміці тематичних сюжетів;
- відстеження сюжетних ланцюжків, відповідних подій, процесів;
- виявлення основних подій і об'єктів з тематичного сюжету;
- виявлення і візуалізація взаємозв'язків подій і об'єктів моніторингу, а також об'єктів моніторингу між собою.

Рис. 4. Склад підсистеми аналітичної обробки

У відповідності зі своїм призначенням дана підсистема, разом з підсистемою моніторингу інформаційного простору, дозволяє реалізувати наступні етапи інформаційно-аналітичного дослідження [5-6]:

- формування запиту в середовищі обраної системи. Знаходження тематичних публікацій за запитом за допомогою систем контент-моніторингу;
- визначення динаміки тематичних публікацій за запитом;
- визначення критичних точок в динаміці тематичних публікацій;
- визначення основних подій у критичних точках;
- виявлення об'єктів моніторингу;
- виявлення та візуалізація взаємозв'язків;
- прогноз розвитку подій.

Висновки

Представлено архітектуру системи інформаційної підтримки прийняття рішень, ідеологія створення та використання онтологій для побудови сюжетів інформаційної протидії, детально розглянуто методику аналітичного дослідження, яка базується на використанні інструментальних засобах аналізу і візуалізації інформаційних потоків і часових рядів.

Запропоновані архітектурні рішення можна використовувати при реалізації систем інформаційної підтримки прийняття рішень, що базуються на контент-моніторингу інформаційного простору та сценарному аналізі, а так само в якості бази для проведення аналітичної та прогнозної діяльності.

Список літератури

1. Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операции та безпека суспільства: Загрози, протидія, моделювання: монографія. – К .: Інтертехнологія, 2009. – 164 с.

2. Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В. Сценарный анализ эффективности управления информационной поддержкой государственной политики России в Арктике. // Национальная безопасность / nota bene. – 2011. – № 6. – С. 104-137.

3. Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В. Структурно-динамический подход к сценарному анализу процессов информационного противоборства в Арктике // Труды XII Всероссийского совещания по проблемам управления (ВСПУ 2014). – М.: ИПУ РАН, 2014. – С. 8889-8901.

4. Додонов А.Г., Ландэ Д.В. Моделирование и анализ тематических информационных потоков // Информационное противодействие угрозам терроризма, 2013. – № 20. – С. 52-59.

5. Додонов А.Г., Ландэ Д.В. Методика аналитического исследования динамики событий на основе мониторинга веб-ресурсов сети Интернет // Информационные технологии и безопасность: основы обеспечения информационной безопасности: Материалы международной научной конференции ИТБ-2014. – К.: ИПРИ НАН Украины, 2014. – С. 3-17.

6. Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г.Конкурентная разведка в компьютерных сетях. – К.: ИПРИ НАН Украины, 2013. – 248 с.

Статтю подано до редакції 09.09.2015