DOI https://doi.org/10.36059/978-966-397-502-3-59

Міхєєв Ю. І.,
кандидат технічних наук, старший дослідник,
доцент кафедри інформаційної боротьби
Національного університету оборони України
м. Київ, Україна

Лобода В. В.,
старший науковий співробітник
науково-дослідного відділу інформаційної та кібернетичної безпеки
Житомирського військового інституту імені С. П. Корольова
м. Житомир, Україна

ВИМОГИ ДО СИСТЕМИ ЗАХИСТУ ВІД ЗОВНІШНІХ ІНФОРМАЦІЙНИХ ЗАГРОЗ

Наявність сучасних інформаційно-телекомунікаційних технологій зумовив появу інформаційного простору із новими комунікаційними можливостями. Це спричинило виникнення нових загроз національній безпеці держави. Так, подання та розповсюдження спеціально підготовленої інформації в засобах масової комунікації під виглядом новинних повідомлень переводять її у розряд маніпулятивного та інформаційного впливу [1, с. 1]. Одним з наслідків дії такого впливу може стати прийняття хибних рішень та втрата довіри до керівництва держави як окремою особою, так і всім населенням країни. Запобігти можливим наслідкам, спричиненим інформаційним впливом, можливо лише завдяки створенню надійної системи захисту від зовнішніх інформаційних загроз, яка повинна передбачати появу таких загроз, визначати їх ступінь, здійснювати нейтралізацію та надавати пропозиції щодо подальшого розвитку ситуації представникам відповідних державних органів та відомств.

У доповіді наведено варіант структури системи захисту від зовнішніх інформаційних загроз, розглянуто етапи її створення. Зазначено, що така система повинна складатися із підсистем моніторингу інформаційного простору та визначення рівня негативного інформаційно-психологічного впливу (ІПсВ), спрямованого на свідомість особи, яка приймає рішення.

У зв'язку з тим, що сьогодні наявний інформаційний простір у своїй більшості представлений ресурсами Інтернет, підсистема його моніторингу повинна охоплювати всі можливості щодо пошуку інформації, а саме [2, с. 483, 3, 75 с.]: пошукові системи, тематичні каталоги ресурсів, сайти новин, RSS-повідомлення, інформаційні агентства, які

здійснюють он-лайн відеотрансляцію новин з урахуванням їх особливостей щодо висвітлення інформації, новинні каналі в соціальних мережах Інтернет. Тому необхідним етапом при створенні даної підсистеми є формування бази даних пошукових ресурсів, наявних в Інтернеті. Список інформаційних ресурсів повинен формуватися таким чином, щоб вони, доповнюючи один одного, максимально охоплювали інформацію за визначеною темою.

Подальша робота системи повинна бути пов'язана з обробленням знайденого матеріалу. При вирішенні даного завдання необхідним є організація автоматичного реферування знайденої інформації. Для візуалізації знайденої інформації з метою її подальшого аналізу доцільно скористатися технологією побудови семантичних мереж. Порівняння семантичних мереж різних текстів дозволяє встановити ступінь їх змістової близькості, що може використовуватися для автоматичної класифікації документів за заданими рубриками, їх пошуку за подібністю заданого тексту, а також розбиття інформаційного масиву на класи документів близького змісту [4, с. 45].

Основні етапи створення підсистеми визначення рівня негативного ІПсВ повинні передбачати наявність компетентних експертів у цій галузі знань. На основі статистичної обробки даних, отриманих за результатами моніторингу інформаційного простору, у подальшому можливо встановити значення періодів спостереження та визначити для них відповідні критерії рівня ескалації загального негативного ІПсВ відносно визначеної групи осіб. Результати оцінювання повинні стати підґрунтям для розробки рекомендацій щодо дій в умовах негативного ІПсВ.

Таким чином, поєднавши функції та завдання двох підсистем в умовах сучасного інформаційного простору, перспективна система захисту від зовнішніх інформаційних загроз повинна забезпечити:

періодичний автоматизований збір та тематичний пошук документів у відкритих джерелах інформації;

– автоматичну та автоматизовану обробку текстових документів, виділення з них об'єктів інтересу та пов'язаних з ними фактів;

– класифікацію різномовних текстів за єдиними критеріями;

– автоматичну лінгвістичну обробку;

– відбір відомостей з банку текстової інформації або з бази знань за вимогами оператора;

– інтегрування та узагальнення знань, які містяться в різномовних текстах з певної предметної галузі;

– перевірку даних, які містяться в різномовних текстах та в їх сукупності, на наявність дезінформації;

– виявлення закономірностей у певній предметній галузі та їх формування на змістовому рівні;

– збереження в базі даних отриманої інформації, а також надання авторизованого доступу користувачів до перегляду та аналітичної обробки документів;

– створення єдиного структурованого архіву об’єктів інтересу, досьє на них, а також подій та взаємовідношень між ними з метою моніторингу змін їх стану в процесі діяльності, виконання часових, географічних та тематичних зрізів при формуванні різноманітних звітів;

– надання аналітикам засобів швидкого виявлення неявних зв’язків між об’єктами моніторингу та пов’язаними з ними фактами й подіями;

– візуалізацію результатів аналітичних досліджень шляхом генерації дайджестів статей та фактів, формалізованих досьє, семантичних мереж та інших аналітичних звітів;

– визначення рівня інформаційної загрози від негативного ІПсВ;

– розроблення варіантів нейтралізації негативного ІПсВ;

– можливість вибору оптимально варіанта нейтралізації негативного ІПсВ за обраним критерієм;

– прийняття рішення про нейтралізацію негативного ІПсВ;

– підготовку та всебічне забезпечення реалізації рішення;

– нейтралізацію негативного ІПсВ;

– оцінювання рівня інформаційної загрози після впливу на неї запропонованої системи.

Список використаних джерел:

1. Указ Президента України № 685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року “Про Стратегію інформаційної безпеки”. URL: https://www.president.gov.ua/documents/6852021-41069

2. Кацалап В. О., Міхєєв Ю. І., Грищук О. М. Спосіб визначення важливості інформаційних джерел в системі моніторингу телевізійного простору. *Scientific Collection «InterConf+»*. 2024. 47(209). С. 482–491.

3. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія / О. В. Левченко. Житомир. 2021. 172 с.

4. Michael W. Berry. Survey of Text Mining. Clustering, Classification and Retrieval Michael W. Berry. – Springer-Verlag, 2004. 244 p.