та знешкодження вибухових пристроїв та мін

Для виявлення та знешкодження вибухових пристроїв та мін безпілотний літаючий апарат 1 піднімається над поверхнею мінного поля 6 і здійснює його сканування. При цьому у блоці подачі модульованого сигналу надвисоких частот пошуку мін та їх детонації 2 генерується подача модульованого сигналу надвисоких частот, яка передається на опромінювач 3, яким і здійснюється подача модульованого сигналу надвисоких частот пошуку мін 5 на поверхню мінного поля 6. При виявленні міни 5 зворотній сигнал з опромінювача 3 поступає до блоку подачі модульованого сигналу надвисоких частот пошуку мін та їх детонації 2, з якого сигнал поступає до детонаційного модуля 4, що забезпечує знешкодження міни 5. До переваг дрона відноситься можливість безконтактного виявлення та знешкодження мін.

УДК 004.4

О. Прокопенко, д-р філос. (комп'ютерні науки); В. Федорієнко, канд. тех. наук
Національний університет оборони України імені Івана Черняховського, Україна

ТЕХНОЛОГІЧНІ АСПЕКТИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ

O. Prokopenko, Ph.D of Computer Science; V. Fedoriienko, Ph.D of Technical Sciences

TECHNOLOGICAL ASPECTS OF IMPROVING INFORMATION AND ANALYTICAL SUPPORT FOR INFORMATION SPACE MONITORING

На долю українців випала нелегка участь у боротьбі за відстоювання незалежності та територіальної цілісності України, внаслідок широкомасштабної збройної агресії російської федерації. Зазвичай, активна фаза збройного протистояння практично завжди супроводжується широко розгорнутою інформаційною кампанією, яка, як правило, розпочинається задовго до початку кінетичної фази конфлікту. Основу проведення будь-якої інформаційної кампанії становлять процеси здійснення негативного інформаційного впливу у інформаційному просторі, мета яких полягає в ускладненні реалізації комунікативних заходів для досягнення стратегічних цілей держави. Негативний інформаційний вплив, заснований на використанні змісту ворожих пропагандистських наративів, активно розповсюджуються у глобальному інформаційному просторі, що негативно впливає на соціальну свідомість, нав'язуючи створений противником світогляд, твердження, факти, аргументи, чутки, тощо [1, 2].

Задовго до початку Революції гідності, одним з доктринальних елементів реалізації зовнішньополітичної стратегії рф стало застосування "м'якої сили" [3], як основного інструменту відновлення свого впливу серед країн пострадянського простору. Зазначене несе у собі загрози для національної безпеки України, а також здійснює свій негативний вплив в усіх її сферах. Головними передумовами застосування "м'якої сили" стали трансформаційні перетворення міжнародних відносин у 21 столітті. Стрімке зростання науково-технічного прогресу, виражене у широкому застосуванні інформаційних технологій в усіх сферах діяльності, наклало свій відбиток на "діджиталізацію" сучасного суспільного устрою, трансформації комунікативних процесів, удосконаленню процесів прийняття управлінських рішень, розширенні нових можливостей для ведення бізнесу, диверсифікацію виробництва під нові вимоги сучасного ринку, тощо.

Розвиток сучасного інформаційного суспільства, поряд з усіма перевагами і величезними можливостями, породжує ряд проблем, пов'язаних із веденням державної

внутрішньої і зовнішньої політики щодо захисту власного інформаційного простору. Сила держави, з цього питання, визначається її здатністю розвивати і розповсюджувати власні цінності, культуру і ідеологію, створювати привабливість власного суспільства. Критеріями визначення м'якої сили держави стають, наприклад, кількість створених інформаційних продуктів (фільми, книги, музика, тощо), та її експорт до інших країн для створення більшої привабливості країни. Агресивність дій у застосуванні державою "м'якої сили" виражається у застосуванні відкритої пропаганди у своїх інформаційних продуктах, так званого інформаційного тероризму, глобалізації фейків, що започатковує основу проведення "гібридних воєн", а згодом – здійснення загарбницької війни, активної фази бойових дій у всіх її проявах. Так, однією з відомих нам стратегій "м'якої сили" є ідеологія "російської весни", мета якої полягала у дезорганізації системи державного управління, захоплення територій зі створенням маріонеткових державних квазіутворень буферних та "сірих зон", втручання у внутрішню політику України, що негативно вплинуло на всі сфери національної безпеки України. Внаслідок завчасно спланованих інформаційно-психологічних спеціальних операцій російськими спеціальними службами були проведені заходи, які сприяли швидкому захопленню АР Крим. Наступними кроками стала спроба дестабілізації ситуації у східних та південних регіонах України, з метою утворення на цій території квазі-держави "Новоросія".

Російська агресія має на меті знищення України як незалежної держави, де збройна агресія виступає лише одним з її елементів. Проте, аналізуючи події, які відбуваються на фронті ведення російсько-української війни, чітко простежується головний її інструментарій у вигляді інформаційної зброї, яку щоденно "прокачують" у ефірах пропагандистських ЗМІ. Деструктивний інформаційний вплив рф виражений у:

- відкритій пропаганді, підміні понять, перекручуванні історичних фактів;
- торгівельно-економічному тиску;
- енергетичній блокаді;
- терорі і залякуванні громадян України;
- дискредитації України у Світі;
- втручанні у політичні процеси;
- звинувачуванні у штучно-створених власних злочинах.

На сьогодні, для ефективної протидії негативному інформаційному впливу, гостро постає питання використання сучасних інформаційних технологій моніторингу, збору і обробки інформації з відкритих джерел у інформаційних системах військового призначення. Це пояснюється необхідністю вироблення необхідних заходів інформаційного протиборства проти розгорнутих інформаційних спеціальних операцій противника, які можуть відбуватися комплексно з активізацією, підвищеною динамічністю і напруженістю ведення бойових дій на окремих напрямах фронту. За кількістю, інтенсивністю і масштабністю вкидань інформаційної пропаганди ворога, на основі використання відомих математичних методів аналізу і прогнозування, можливо визначати етапи інформаційно-психологічної спеціальної операції, що надає додаткові можливості для своєчасних адекватних дій з інформаційної протидії.

Питання моніторингу інформаційного простору найбільшої ефективності набуло у програмних продуктах зарубіжних і вітчизняних розробників. До них відносяться як повнофункціональні продукти, де забезпечуються процеси обробки даних: збір даних, аналіз даних, візуалізація і інтерпретація даних, так і окремі сервіси і бібліотеки, за допомогою яких спрощуються процеси розробки програмного забезпечення на високорівневих мовах програмування: Python, C#, C++, PhP, Java та інші.

До першої категорії програмних продуктів належать: IdexAttack, Semantrum, InfoStream, Wisdom Well, Web-Observer, Semantic Force, Multigo, Google Trends, Brandwatch, UAport, GreyLog. Усі зазначені продукти працюють в мережі Інтернет та

реалізовані на веб платформах. Здебільшого, зазначені програмні продукти, розроблені у вигляді агрегаторів новин, у яких за допомогою притаманних для кожного програмного продукту технологій, відслідковується, обробляється і візуалізується необхідна інформація у вигляді графіків, діаграм та інших графічних представлень, що дозволяє легше сприймати великі об'єми даних, швидко отримати візуальне уявлення про те, як дані пов'язані між собою і як вони можуть бути використані для вирішення конкретних проблем.

За допомогою другої категорії розробляється вузькоспеціалізоване спеціальне програмне забезпечення для конкретних потреб. Для прикладу, технологічні аспекти інформаційно-аналітичного забезпечення моніторингу інформаційного простору збройних сил, крім вирішення наведених вище задач, повинно включати наступний функціонал:

– можливості з приймання-передавання, обробки текстових повідомлень про розташування і дії ворога, від населення тимчасово окупованих територій;
– технологію пошуку ворожих наративів в інформаційних повідомленнях відкритих джерел інформації, їх взаємозв'язок і прогнозовані ступені ризику на певні складові сектору безпеки і оборони України;
– систему підтримки прийняття рішень для оперативного вироблення, прийняття і реалізації необхідних заходів протидії деструктивного інформаційно-психологічного впливу противника.

Зазначене досягається за рахунок обробки спеціалізованими сервісами, на основі штучного інтелекту, значних за об'ємом текстових масивів даних. Обробка інформаційного контенту веб-сторінок і соціальних мереж здійснюється на основі Web-скрапінгу і парсингу даних. Технології Machine Learning в продуктах автоматизованого моніторингу вирішують задачі класифікації і кластеризації при розпізнаванні характеристик досліджуваного контенту інформації. Це дозволяє виявляти і аналізувати інформаційні загрози, визначати тональність повідомлень, семантику та структуру тексту, відслідковувати обговорення певної теми в соціальних мережах, тощо.

Сукупність наведених вище положень, дозволяє стверджувати про доволі обширні можливості сучасного інформаційного забезпечення, що дозволяє створювати нові інформаційні технології моніторингу інформаційного простору для певної специфіки діяльності. Можливості з обробки тексту, побудованих на основі технологій штучного інтелекту, дозволяють виявляти у джерелах інформації не лише маніпулятивний зміст і ворожі наративи, а також здійснювати:

– аналіз ключових слів у повідомленнях, які пов'язані з конкретною темою, та визначити, які саме аспекти повідомлень є ворожими;
– оцінку рівня страху у повідомленнях, на основі аналізу лексики, тону та стилю повідомлень;
– оцінку рівня конфліктності, на основі аналізу кількості та ступеню емоційної напруги в повідомленнях, а також за кількістю звернень до агресивних слів та висловлювань;
– дослідження джерел (соціальних мережі, тематичні блоги), які поширюють інформацію до інших джерел.

Таким чином, своєчасне виявлення негативного інформаційного впливу на основі використання передових інформаційних технологій, підвищує ефективність вироблення комплексу необхідних заходів для його нейтралізації.

Література

1. Почепцов Г. Сучасні інформаційні війни. Видання третє, доповнене та перероблене. Київ : Видавничий дім "Києво-Могилянська академія", 2016. 504 с.

2. Курбан О. В. Сучасні інформаційні війни у мережевому он-лайн просторі. Навчальний посібник. Київ : ВІКНУ, 2016. 286 с.
3. Joseph S. Nye. Soft Power: The Means To Success In World Politics. USA, NY : Public Affairs, 2005. 191 p.

УДК 621.039.586

В. Стручок
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ВПЛИВ ЛЮДСЬКОГО ФАКТОРА НА ВИНИКНЕННЯ ТЕХНОГЕННИХ АВАРІЙ

V. Struchok

THE INFLUENCE OF THE HUMAN FACTOR ON OCCURRENCE OF TECHNOGENIC ACCIDENTS

При дослідженні причин виникнення аварії на Чорнобильській атомній електростанції (АЕС), що сталася 26 квітня 1986 року, було встановлено, що мав місце цілий комплекс як об'єктивних, так і суб'єктивних факторів, що призвів до цієї вибухової аварії.

До об'єктивних головних факторів, зокрема, належать значні недоліки у конструкції стержнів системи регулювання та захисту реактора типу РБМК та структурі і значень нейтронно-фізичних характеристик його активної зони [2].

Однак, звертає на себе увагу вплив суб'єктивного, людського фактора на виникнення вибухової аварії, оскільки в офіційних повідомленнях про аварію першопричиною її виникнення було визначено помилки експлуатаційного персоналу станції. Тоді, коли відповідальність за аварію несуть сотні спеціалістів різних галузей економіки, що є дотичними до ядерної енергетики. Тут необхідним є врахування існуючих на той час більше 30 років підходів до ядерної енергетики, ізольованості від вчених інших країн і досягнень зарубіжної науки, процедури погодження проектів, над секретності робіт у цій галузі, що рано чи пізно мало призвести до аварії.

Але, очевидним є, що на той час значний вплив на роботу експлуатаційного персоналу мав встановлений тоді адміністративно-командний метод управління в економіці СРСР, у тому числі й у енергетиці. Зокрема, випробування на реакторі IV енергоблоку вважалися важливими і 25 квітня 1986 року була третя спроба їх провести. Експеримент мали провести вдень 25 квітня. І персонал почав його проведення та знизив потужність блока, щоб провести наступні операції. Однак, експеримент був зупинений на вимогу диспетчерської служби енергомереж, яка заборонила відключення блоку на період проходження вечірнього періоду навантажень. Дана перерва після зниження потужності блока до 50% значно зменшила запас реактивності, скоротила кількість занурених в активну зону стержнів системи управління і захисту реактора, що призвело до «отруєння» реактора, попадання його в «йодну яму». Персоналу не можна було погоджуватись з диспетчерами, а необхідно було увімкнути систему захисту реактора в роботу. Крім цього, для проведення цієї роботи необхідний був час, співрозмірний з призупиненням експерименту, що в умовах адміністративно-командної системи управління було неможливим. Важливим є й те, що персонал вважав, що дані випробування носять чисто електротехнічний характер. Програма випробувань не була достатньо проаналізована спеціалістами, що відповідають за безпеку роботи АЕС, тому у ній були відсутні відповідні спеціальні розділи з безпеки, також програма не була погоджена з головним конструктором і науковим керівником. Ці дії і призвели до тяжких аварійних наслідків на АЕС.