Між ключовими словами можуть існувати відношення синонімії або еквівалентності значення, тобто синонімії з точки зору певної інформаційно-пошукової системи. Накопичення ключових слів шляхом змістовного аналізу текстів або алгоритмічно, наприклад, порівнянням слів тексту з фіксованим переліком неключових слів, є важливим етапом при виборі вихідної лексики будь-якого тексту.

Ключовим словам властиві ієрархічні відносини. Ті з них, які у цих відносинах посідають верхній рівень, становлять ядро семантичного поля; підпорядковані їм ключові слова складають словесні ряди, які перебувають на периферії семантичних полів тексту.

Залежно від того, як часто користувачі з усього світу використовують певний запит для пошуку необхідної їм інформації, ключові слова бувають трьох типів. Найконкурентніші ключовики, просування сайту за якими – складний, довгий і дорогий процес, – високочастотні. Наступні типи – середньочастотні і низькочастотні. Цікавий факт: в Google щодня виконуються більше 3,5 мільярдів пошукових запитів. Знання того, як підібрати ключові слова – перший крок для забезпечення успіху в роботі з інформацією.

Якщо ключові слова у традиційному розумінні в контексті аналітико-синтетичної обробки документів слугують для згортання інформації, то в Інтернет-мові вони міняють свій вектор на абсолютно протилежний і вживаються для розгортання інформації. Вони іменуються ключовиками, існує цілий масив різних порад для їх підбору. Наприклад, експерти радять для їх набору використовувати методику кластеризації. Процедура включає в себе угруповання слів і фраз, які найкраще просувати на єдиній сторінці ресурсу. На цьому етапі усі зібрані запити поєднують у групи за змістом, за цінністю (транзакційні, мультимедійні, інформаційні), за географічною залежністю тощо

Отже, робота з ключовими слова у процесі аналітико-синтетичної обробки документів зберігає свою важливість у нових умовах передачі і сприйняття текстової інформації. Розробляються додаткові методики такої роботи, оскільки розгортаються функційні особливості інтернет-тексту.

Література

1. Бібліотечно-інформаційна діяльність. Терміни та визначення понять: ДСТУ 7448:2013. [Чинний від 2014.07.01]. К. : Мінекономрозвитку України, 2014. ІІІ, 44 с.

2. Українська архівна енциклопедія [Держ. ком. архівів України, Укр НДІ арх. справи та документознавства; редкол. : Матяш І. Б. (гол. ред.) та ін.]. К., 2008. 880 с.

УДК 007:[070:323.266]:32.019.5

ІНФОРМАЦІЙНІ ВІЙНИ І БЕЗПЕКА ІНФОРМАЦІЇ

О. С. Щербіна

У XXI столітті війна перетворилася не тільки в протистояння військової сили, а й під час війни у протистояння інформаційних технологій. Навіщо завойовувати країну силою зброї, стикаючись з опором і несучи втрати? Адже можна підпорядкувати її зсередини, силами її ж громадян, що і є кінцевою метою, глобальною стратегією інформаційної війни.

Інформаційна війна в класичному розумінні являє собою ідеологічну, психологічну обробку збройних сил, населення, військово-політичного керівництва противника в

інтересах створення тої громадської думки, яка потрібна, або її дезінформації і, таким чином, нав'язування супротивній стороні своєї політичної волі.

В широкому значенні слова під терміном «інформаційна війна» розуміємо війну з використанням інформаційних технологій.

На сьогоднішній день не існує загальноприйнятої концепції інформаційної війни, про що свідчить аналіз наукових праць з проблем інформаційної війни. Дослідники, які вивчають інформаційну війну, виділяють різні аспекти даного багатогранного явища.

Прибічники першого підходу до концепції інформаційної війни сходяться на тому, що перемога в ній буде залежати в основному від рівня розвитку та використання новітніх інформаційних технологій у військовій сфері.

Другий підхід пов'язаний з виникненням нового середовища для протиборства, так званого «кібернетичного простору» та нового виду зброї, що має назву інформаційної.

Дослідники третього підходу найбільшого значення надають соціальним аспектам інформаційної війни та вважають, що інформаційне протиборство являє собою цілеспрямовані інформаційні впливи соціальних інформаційних систем (окремих людей, певних соціальних груп, народів, країн) одна на одну з метою отримання певного виграшу в матеріальній сфері. В цих умовах інформація, як зброя, передусім, діє на систему управління, не знищуючи її, а підкоряючи.

Сьогодні багато-хто з дослідників оперує терміном «інформаційно-психологічна війна», тобто відкриті та приховані цілеспрямовані інформаційні впливи соціальних, політичних, етнічних та інших систем одна на одну з метою одержання визначеного виграшу в матеріальній сфері, спрямованих на забезпечення інформаційної переваги над супротивником і завдання йому матеріального, ідеологічного чи іншого збитку або шкоди. Згідно з офіційними документами збройних сил США, деструктивний вплив на системи управління досягається шляхом проведення психологічних операцій, які спрямовані проти персоналу і осіб, які приймають рішення, здійсненням впливу на їх моральну стійкість, емоції і мотиви прийняття рішень; виконанням заходів з оперативної безпеки, дезінформації і фізичної руйнації об'єктів військової інфраструктури противника. Тобто, інформаційна війна складається з дій, які розпочинаються з метою досягнення інформаційної переваги у забезпеченні національної воєнної стратегії шляхом впливу на інформацію і інформаційні системи противника з одночасним укріпленням і захистом власної інформації, а також інформаційних систем і інфраструктури.

Існують різні погляди, у тому числі й протилежні, щодо правомірності існування терміну «інформаційна війна». Однак, з кожним роком теорія і практика інформаційної війни збагачується новітніми розробками. Це свідчить про те, що кількість прихильників існування терміну «інформаційна війна» все ж таки переважає число противників цього поняття.

Таким чином, інформаційна війна ведеться в комплексі з кібер- та психологічною війнами з метою ширшого охоплення цілей, із залученням радіоелектронної боротьби та мережевих технологій. Інформаційна війна може включати:

– збір тактичної інформації;

– гарантування безпеки власних інформаційних ресурсів;

– поширення пропаганди або дезінформації задля деморалізації військ та населення ворога,

– підрив якості інформації супротивника і попередження можливості збору інформації супротивником.

В той же час, з виникненням інформаційного суспільства, зумовленим розвитком інформаційних технологій, виникла суттєва загроза несанкціонованого зняття інформації. З'являються все більш досконалі способи використання каналів витоку різних видів інформації. Оскільки на теперішній час інформація має все більшу

комерційну вартість, то підприємства почали приділяти значну увагу своїй інформаційній безпеці. Інформаційна безпека підприємств є однією із суттєвих складових частин національної безпеки країни, забезпечення якої сприяє досягненню успіху при вирішенні задач у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності.

Відповідно до ст. 13 Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [1] інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Шляхи досягнення інформаційної безпеки пов'язані з відверненням та запобіганням ряду інформаційних ситуацій негативного характеру, наприклад як-от:

– неправильне розуміння наявної інформації;
– несвоєчасне її отримання (із запізненням);
– неповнота інформації, її дефіцит для розв'язання конкретного питання;
– навпаки, надлишок інформації, її надмірність, наявність інформаційного шуму – зайвої, непотрібної в даному випадку, а тому шкідливої інформації;
– проникнення до інформаційної системи (або мережі) дезінформації;
– зловживання конфіденційністю (довірчим характером) певної інформації.

Таким чином, інформаційна безпека – це стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди.

Слід відмітити, що інформаційна безпека особи та суспільства тісно пов'язані між собою. Інформаційна безпека особи – це стан захищеності психіки та здоров'я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану. Інформаційна безпека суспільства – можливість безперешкодної реалізації суспільством й окремими його членами своїх конституційних прав, пов'язаних із вільним одержанням, обробленням, створенням і поширенням інформації, а також ступінь їх захисту від деструктивного інформаційного впливу.

Інформаційна безпека держави – це стан її захищеності та інформаційного розвитку, при якому акції інформаційного впливу, спеціальні інформаційні операції, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів та комп'ютерна злочинність не завдають суттєвої шкоди національним інтересам.

Саме навчальна дисципліна «Інформаційні війни і безпека інформації» дає можливість отримати цілісне уявлення про інформаційні війни, їх історію, особливості прояву на початку XXI століття, загрози в інформаційній сфері та завдання щодо забезпечення інформаційної безпеки України.

Література

1. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». URL: https://zakon.rada.gov.ua/laws/show/537-16#Text

2. Почепцов Г. Г. Сучасні інформаційні війни. Київ: НАУКМА, 2016. 498 с.

3. Курбан О. В. Сучасні інформаційні війни в мережевому онлайн просторі. Київ: ВІКНУ, 2016. 286 с.

4. Лужецький В. А. Інформаційна безпека: навчальний посібник. Вінниця: УНІВЕРСУМ Вінниця, 2009. 240 с.