УДК 004.8:004.912

С. В. Чернишук

МЕТОДИКА ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ ЗАГРОЗ У ПРИРОДНОМОВНИХ ТЕКСТАХ

На підставі аналізу проявів кібернетичних загроз (КЗ) у природномовних текстах (ПМТ) визначено правила їх ідентифікації та розкрито методику їх виявлення.

Постановка проблеми. Поява нового класу загроз безпеці, які отримали назву «кібернетичні», зумовлює необхідність розробки адекватних організаційних, технічних та правових заходів для протидії таким загрозам та їх стримування. Першочерговим кроком у цьому напрямку є створення систем виявлення КЗ, які здатні ідентифікувати небезпеку на етапі її зародження та раннього розвитку і сформувати пропозиції щодо протидії [1–3].

Існуючі системи виявлення КЗ, як правило, реалізуються у вигляді міжмережних екранів, систем захисту від несанкціонованого доступу, сканерів уразливостей, систем контролю цілісності, відстеження змін контрольованих процесів та аналізу журналів реєстрації [4]. Тобто функціональні можливості переважної більшості таких систем обмежуються аналізом мережного трафіка або параметрів роботи окремого вузла інформаційно-телекомунікаційної мережі [2–5] з подальшим визначенням рівня невідповідності отриманих результатів встановленому еталону.

Разом з тим, у [6] встановлено, що КЗ слід розглядати як фактори (події, явища) інформаційного, комунікаційного, комп'ютерно-мережного та соціотехнічного просторів (або їх комбінацію), які за умови їх умисного цілеспрямованого використання створюють небезпеку порушення процесів управління, обробки та передачі інформації, що відбуваються у кібернетичних системах (КС) різних сфер (соціальної, технічної, соціотехнічної), або можуть зашкодити елементам таких систем. При цьому під КС розуміється впорядкована сукупність об'єктів (елементів), що взаємодіють з метою виконання певної функції та здатні обмінюватися інформацією [7].

Наведене визначення та результати досліджень, викладені у [8], свідчать про наявність ознак КЗ не лише в комунікаційному та комп'ютерно-мережному просторі, а й в інформаційному та соціотехнічному середовищах. Тому окрім аналізу сигналів технічних систем виникає необхідність обробки відомостей, що розміщуються на відкритих інформаційних ресурсах. Враховуючи випереджаючі (порівняно з іншими джерелами) темпи зростання обсягів інформації, яка міститься в ПМТ відкритих ресурсів інформаційно-телекомунікаційних систем (ІТС) [9], актуальною є розробка методичного апарату виявлення КЗ шляхом обробки таких текстів.

Огляд останніх досліджень і публікацій. Основна відмінність між відомими підходами до обробки ПМТ полягає у способах подання та аналізу змісту таких текстів. Один з них базується на припущенні, що основний зміст ПМТ визначається множиною ключових слів – термінів і понять, які до нього входять (Bag of Words) [9]. Такий підхід ігнорує лінгвістичну взаємозв'язність і семантику природної мови, однак дозволяє швидко

© С. В. Чернишук, 2013

виконувати операції обробки текстів за формальними ознаками. Обробка ПМТ за такого подання змісту базується переважно на статистичних та ймовірнісних моделях.

Інший підхід полягає в логіко-семантичній обробці ПМТ, що передбачає визначення їх змісту за рахунок аналізу граматики, використання баз знань і тезаурусів, які відображають семантичні зв'язки між окремими словами та групами слів [10]. У результаті такої обробки отримується формалізований опис змісту ПМТ, що дозволяє аналізувати його методами штучного інтелекту. Через суттєві витрати на підтримку баз знань і тезаурусів для кожної мови, тематики і виду документа, зазначений підхід застосовується, як правило, для розв'язання вузькоспеціалізованих задач [11], до яких можна віднести і задачу виявлення КЗ окремій системі.

Аналіз відомих методів виявлення КЗ дозволяє розподілити їх на дві основні групи [2–5]:

сигнатурні методи (дозволяють виявляти загрозу за умови відомих параметрів, які її характеризують, та порогових значень цих параметрів);

методи виявлення аномалій (передбачають розробку профілю «безпечної» роботи КС, яка підлягає захисту, і постійний моніторинг відхилення поточних даних від нього).

Перевагою сигнатурних методів є висока достовірність (незначна кількість хибних виявлень загроз) і невисокі ресурсозатрати, але при цьому не забезпечується ідентифікація загроз, характеристичні параметри яких відсутні.

Методи виявлення аномалій дозволяють ідентифікувати як відомі, так і не відомі раніше загрози, однак не забезпечують високої достовірності результатів. Це зумовлено тим, що параметри загрози можуть збігатися 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 КЗ; високу достовірність результатів; низьку ресурсозатратність [4].

Формулювання завдання дослідження. Метою дослідження є розробка методики виявлення КЗ шляхом логіко-семантичної обробки ПМТ, яка комплексуватиме сигнатурні методи та методи виявлення аномалій і дозволить підвищити оперативність ідентифікації КЗ за рахунок автоматизації.

Виклад основного матеріалу. Усі відомі технології виявлення загроз базуються на: їх ознаках, які проявляються у просторі, що контролюється; джерелах інформації, у яких виявляються ці ознаки; методах аналізу інформації, отриманої з відповідних джерел [4]. Зазначені складові є об'єктивно необхідними для виявлення КЗ, тому вони підлягають обов'язковому визначенню для досягнення сформульованої мети дослідження.

Визначення ознак КЗ

Визначенню ознак КЗ передував аналіз реальних випадків їх прояву в повідомленнях, розміщених на відкритих ресурсах ІТС. За КС, відносно якої виявлялися КЗ, обрано Збройні Сили (ЗС) України як складну соціотехнічну систему. Результати дослідження дозволили виділити такі класи ознак:

1. Констатація в явній або неявній формі в тексті факту прямої загрози (небезпеки) КС, що захищається, або її складовим. Наприклад: *«Реформа Збройних сил України – це стратегія знищення української армії та флоту»* [12], *«атака СБУ спрямована на*

генералів та старших офіцерів [ГШ ЗСУ]», «головна мішень – сам начальник Генштабу» [13], *«…нищать життєво важливі структури нашої армії та флоту»* [14], *«иноземцы ликвидируют … нашу армию»* [15].

Іншими словами, факти, що виражають пряму або опосередковану небезпеку КС або її складовим, свідчать про наявність загрози такій системі.

2. Наявність у ПМТ фактів, що не відповідають (або суперечать) образу усталеного (безпечного) функціонування КС, яка підлягає захисту. Наприклад: *«Збройні Сили України вже давно не можуть займатися властивими для себе обов'язками»* [13], *«наступит момент, когда армия будет окончательно небоеспособна»* [15], *«резкое сокращение численности армии [Украины]»* [16], *«…намагаються зупинити розробку і впровадження системи [управління військами] української розробки "Калина"»* [17].

Тобто факти, що свідчать про відхилення від профілю безпечного функціонування КС у штатному режимі, вважаються такими, які містять ознаки КЗ.

Решта можливих проявів КЗ у ПМТ або може бути зведена до визначених класів, або не піддається формальному опису, а тому не враховується в подальших дослідженнях з огляду на їх нечисленність.

Характеристика джерел інформації, у яких виявляються ознаки загроз

Принциповою особливістю аналізу ПМТ є те, що його предметом виступають знання про предметну область, які розкриваються у змісті текстів. Завдання розпізнавання, добування та формалізації знань дозволяє вирішувати знання-орієнтований підхід [18], який передбачає формалізацію змісту ПМТ та автоматизацію обробки отриманого формалізованого опису в інтересах вирішення конкретних завдань аналізу текстів [19]. Основними компонентами знань (з точки зору їх формалізованого опису) є поняття, відношення між ними, а також характеристики (атрибути) понять та відношень. Обробка вхідного тексту направлена на розпізнавання в ньому основних компонентів знань і встановлення логіко-семантичних відношень між ними з метою формування семантичної структури змісту ПМТ – семантичної мережі [20], вузлами якої є поняття, а ребрами – відношення між цими поняттями.

Отже, на першому етапі знання-орієнтованої обробки ПМТ інформація подається в єдиному вигляді шляхом вилучення знань із текстів і формалізації їх у вигляді семантичних мереж. Формалізований опис змісту ПМТ аналізується із врахуванням знань про предметну область (у контексті даного дослідження про КС, що підлягає захисту). Для цього створюється база знань, у якій інтегрується вся необхідна для комплексного аналізу апріорна (наявна) і поточна інформація.

На другому етапі методами логіко-семантичної обробки знань отримана зі змісту ПМТ інформація аналізується на функціональну повноту, а також сумісність та суперечливість апріорній інформації з бази знань. У результаті такої обробки виявляються протиріччя у фактах, що дозволяє вирішити прикладну задачу виявлення КЗ у ПМТ.

Спосіб опису наявної та поточної інформації в базі знань про КС та її безпечне функціонування потребує уточнення. Одним із підходів до подання знань про деяку предметну область, який на практиці показав свою ефективність, є застосування онтологій. Оскільки в літературі зустрічається велика кількість тлумачень поняття «онтологія» [21], слід прийняти таке з них, яке б відповідало меті дослідження. Тому в подальшому під онтологією розумітимемо деякий формальний опис предметної області, що визначається як впорядкована множина такого вигляду:

$$O = < T, R >, \quad (1)$$

де T – скінченна множина понять (концептів, класів) предметної області, яку відображає онтологія O;

R – скінченна множина відношень між поняттями заданої предметної області [22].

Графічно (1) може бути зображено рис. 1:

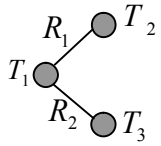

Рис. 1. Фрагмент онтології

Слід зазначити, що для розв'язання задачі виявлення КЗ в онтології мають бути якомога повніше відображені знання про процеси управління, які відбуваються в КС: об'єкт і суб'єкт управління, їх склад, характеристики та особливості функціонування; алгоритми (протоколи) взаємодії між елементами КС та обміну інформацією; допустимі стани, у яких система здатна виконувати своє призначення тощо.

Як приклад на рис. 2 наведено варіант онтології безпечного функціонування умовної КС. Прямокутниками позначено поняття, а овалами зі стрілками – відношення між ними.

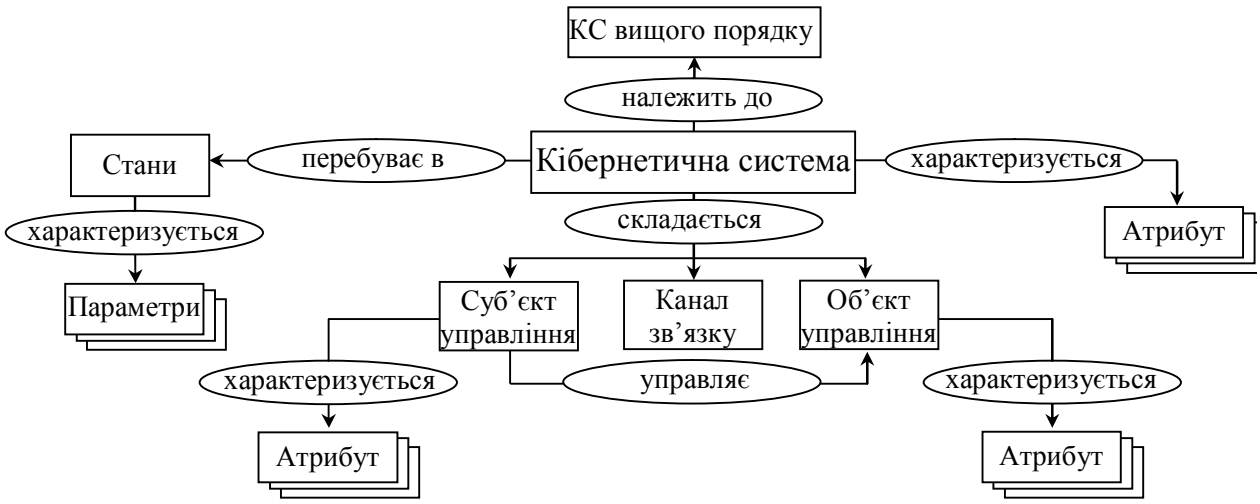

Рис. 2. Онтологія умовної кібернетичної системи

Розглянуті підходи до опису знань із заданої предметної області у вигляді онтології та змісту ПМТ у вигляді семантичних мереж можуть бути успішно використані для виявлення в текстах ознак КЗ за визначеними класами прояву таких загроз.

Методи аналізу знань, отриманих із ПМТ

Розробку підходів до аналізу отриманих із ПМТ знань здійснюватимемо окремо для кожного із визначених класів ознак КЗ.

Ідентифікацію КЗ за ознаками першого класу по суті реалізує сигнатурний метод їх виявлення. Особливістю цього процесу в ПМТ є те, що в ролі параметрів деякої загрози мають виступати її семантичні ознаки, які дозволяють однозначно ідентифікувати саме її. У [8] визначено такі ознаки та сформульовано критерій виявлення КЗ: для встановлення

факту реалізації КЗ g необхідно і достатньо ідентифікувати зв'язок між ознакою об'єкта o та ознакою n, що характеризує негативні наслідки для цього об'єкта:

$$(\exists o) \wedge (\exists n) \Rightarrow \exists g \in G, \qquad (2)$$

де o – ознака, що визначає об'єкт захисту;

n – ознака, що визначає негативні наслідки або небезпечні результати реалізації загрози g для об'єкта o.

Критерій (2) описує прояви КЗ першого класу і може бути зображений деяким семантичним шаблоном (рис. 3).

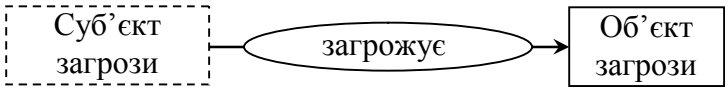

Рис. 3. Семантичний шаблон КЗ

Суб'єкт загрози є необов'язковим фігурантом відношення «загрожує», тому його обведено штриховою лінією.

З огляду на зазначене, виявлення КЗ за ознаками першого класу зводиться до пошуку в семантичному описі тексту такої семантичної конструкції, яка збігається із заданим семантичним шаблоном, та подальшого визначення його конкретних значень: об'єкта загрози, негативних наслідків та, по можливості, суб'єкта загрози. При цьому в онтології КС виділяється фрагмент, що відповідає визначеному значенню шаблону.

Приклад: *«…нищать життєво важливі структури нашої армії та флоту»* (рис. 4).

Рис. 4. Семантична конструкція КЗ

Якщо за КС, що підлягає захисту, обрано ЗС України, то в її онтології буде виділено відповідний фрагмент (рис. 5).

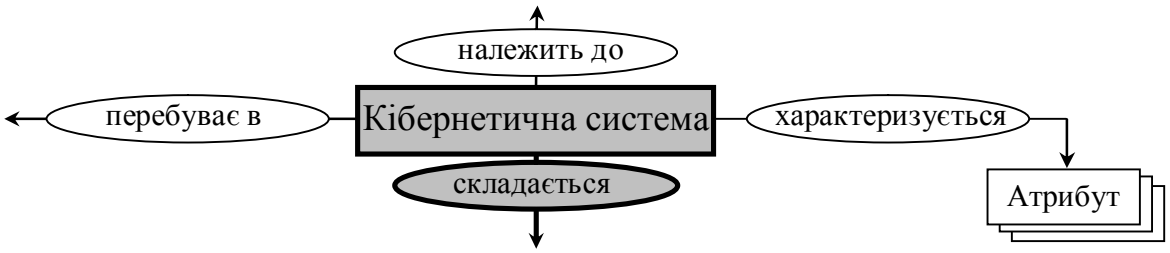

Рис. 5. Приклад виявлення КЗ за ознаками першого класу

Ідентифікацію КЗ за ознаками другого класу реалізує метод виявлення аномалій. Особливістю його є те, що профілю «безпечного» функціонування КС відповідає її онтологія, а за поточні дані, які порівнюються з профілем, виступають семантичні конструкції змісту вхідного тексту.

З урахуванням зазначеного, *виявлення КЗ за ознаками другого класу зводиться до зіставлення семантичного опису тексту та онтології КС і встановлення суперечностей між ними. При цьому в тексті та онтології КС виділяються суперечливі фрагменти.*

Приклад: *«резкое сокращение численности армии [Украины]».*

Відповідно до своєї онтології чисельність ЗС України є одним із атрибутів цієї КС. Тому в результаті порівняння наведеного фрагмента ПМТ й онтології КС буде виділено такий фрагмент (рис. 6):

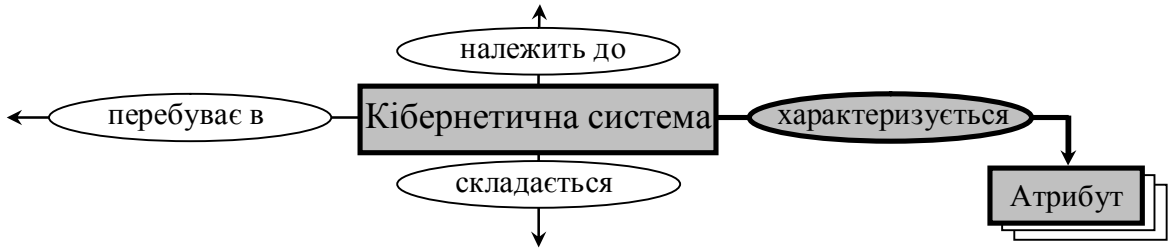

Рис. 6. Приклад виявлення КЗ за ознаками другого класу

Нееквівалентність фактів, а отже, і суперечність семантичного опису ПМТ й онтології може виражатися у формі:

1. Протиріччя в поняттях: відношення містить не передбачені онтологією поняття.

2. Протиріччя у відношеннях: між поняттями встановлено не передбачене онтологією відношення.

Формальні правила виявлення КЗ у ПМТ

Розв'язок сформульованих задач виявлення КЗ першого та другого класу потребує розробки формальних правил, які б дозволяли однозначно ідентифікувати прояви таких загроз у ПМТ. Для цього введемо такі позначення. Розрізнятимемо онтологію та семантичну мережу вхідного тексту за індексами $O_o =< T_o, R_o >$ і $O_t =< T_t, R_t >$ відповідно. Тоді приймемо, що: $t_o \in T_o$ – деяке поняття t_o належить онтології, тобто множині T_o; $r_o \in R_o$ – відношення між поняттями онтології, яке належить множині R_o; $T_i(t_o) \in T_o$ – підмножина множини T_o понять, суміжних з поняттям t_o онтології; $T_i(r_o) \in T_o$ – підмножина множини T_o понять, інцидентних відношенню r_o онтології; $R_i(t_o) \in R_o$ – підмножина множини R_o відношень між поняттями онтології, інцидентних поняттю t_o онтології; $R_z(t_o) \in R_o$ – підмножина множини R_o відношень онтології, які відображають небезпеку для поняття t_o онтології; $t_t \in T_t$ – деяке поняття t_t належить семантичному опису ПМТ, тобто множині T_t; $r_t \in R_t$ – відношення між поняттями семантичного опису тексту, яке належить множині R_t.

У термінах введених позначень формальне правило виявлення КЗ за ознаками першого класу набуває такого вигляду:

$$\exists r_t(t_t) : t_t \in T_o \wedge r_t \in R_z(t_o). \qquad (3)$$

Правило (3) трактується таким чином: у ПМТ виявлено відношення $r_t(t_t)$, учасником якого є поняття $t_t \in T_o$ онтології КС, а семантичне значення виявленого відношення

збігається з відношенням $r_z(t_o) \in R_z(t_o)$, що відображає небезпеку для елементів КС, яким відповідають поняття онтології.

Формальні правила виявлення КЗ за ознаками другого класу задамо окремо для протиріч у поняттях і протиріч у відношеннях.

1. Протиріччя у поняттях:

$$\exists r_t(t_t): t_t \in T_o \wedge r_t \in R_o \wedge t_t \notin T_i(r_o). \quad (4)$$

Відповідно до правила (4) виявлене в тексті поняття t_t не може брати участь у вжитому відношенні $r_t(t_t)$.

2. Протиріччя у відношеннях:

$$\forall t_o \in T_o \ \neg\exists r_o \in R_o : r_t = r_o. \quad (5)$$

Правило (5) трактується в такий спосіб: множина R_o усіх відношень, у які можуть вступати поняття t_o онтології, пов'язані відношенням r_t, не містить самого відношення r_t.

Отже, методика виявлення КЗ у ПМТ включає такі етапи (див. рис. 7):

1. Проектування та побудова онтології $O_o = < T_o, R_o >$ безпечного функціонування КС, що підлягає захисту, за інформацією із різнотипних джерел: набору текстів за заданою предметною областю, експертів та аналітиків.

2. Виконання логіко-семантичної обробки вхідних ПМТ та побудова семантичних описів їх змісту у вигляді семантичних мереж $O_t = < T_t, R_t >$.

3. Зіставлення отриманої семантичної мережі ПМТ з онтологією КС на основі формальних правил (3)–(5). Виділення суперечливих фрагментів вхідного тексту та онтології.

4. Детальний аналіз виділеного фрагмента та (у разі необхідності) усього тексту аналітиком на предмет наявності КЗ та прийняття ним остаточного рішення.

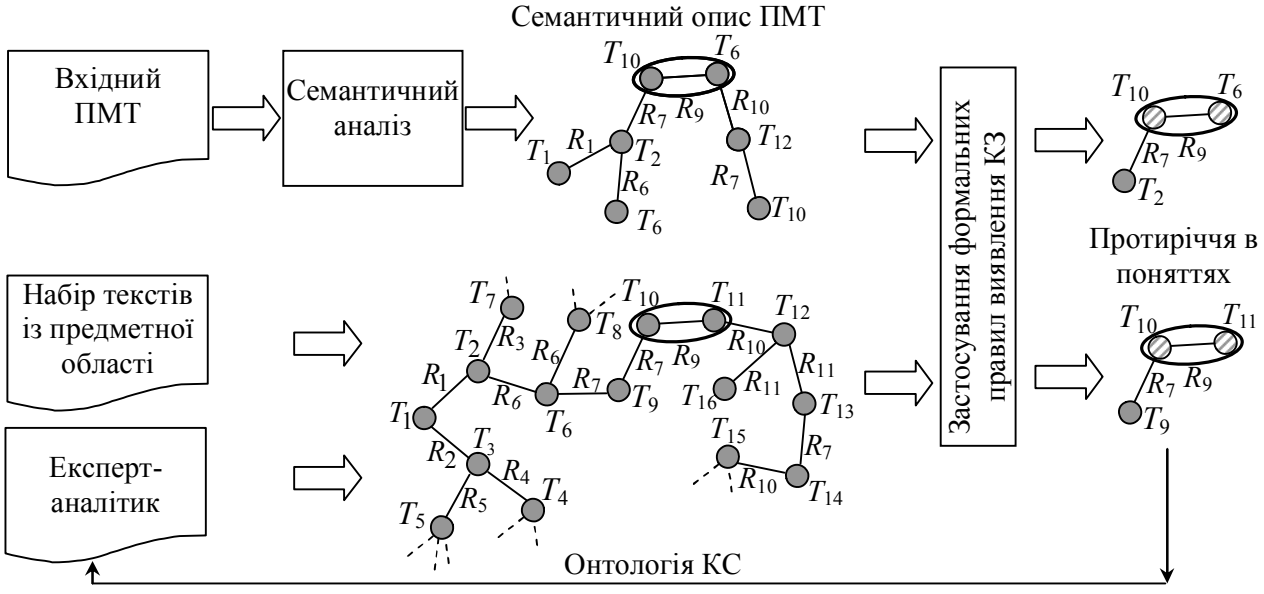

Рис. 7. Структурно-логічна схема методики виявлення КЗ у ПМТ

Для перевірки дієвості запропонованої методики на підставі відомостей [23] у середовищі проектування Protege розроблено фрагмент онтології функціонування ЗС України в мирний час, яка включає:

а) більше 150 відкритих назв структурних підрозділів ЗС України з відповідними синонімами та урахуванням варіантів написання;

б) більше 1000 термінів у 16 групах, серед яких:

227 найменувань керівних посад відповідних структурних підрозділів;

383 найменування зразків озброєння та військової техніки;

585 якісних (кількісних) параметрів і оцінок діяльності особового складу та функціонування штатного озброєння підрозділів ЗС України й органів управління тощо;

в) близько 50 семантичних шаблонів з використанням термінів обох попередніх груп.

Автоматизована розробка онтології проводилася на базі аналізу текстів відкритих інформаційних ресурсів [24–27] за допомогою спеціалізованих засобів комп'ютерного аналізу текстів. Затрачений час для розробки онтології (виділення понять та їх класифікація за розділами) – 5 людино-днів роботи експерта, а для лінгвістичного наповнення створеної онтології (відбір і систематизація типових проявів загроз, створення відповідних семантичних шаблонів, загальне налаштування і тестування створеного лінгвістичного процесора) – близько 50 людино-днів роботи лінгвіста.

У підсумку із 1000 оброблених ПМТ було виявлено майже 60 текстів (22 – за ознаками першого класу, 37 – за ознаками другого класу), які містили ознаки загроз ЗС України. При цьому заздалегідь визначена аналітиком кількість текстів з ознаками КЗ становила 74. У результаті досягнута точність автоматичного виявлення КЗ – 80% за помилками першого роду (пропуск текстів, що містять ознаки КЗ) та 99,5% за помилками другого роду (хибне виявлення ознак КЗ, якщо їх насправді немає), а подальший аналіз виявлених текстів аналітиком дозволив забезпечити стовідсоткову точність за помилками другого роду. При цьому оперативність виявлення КЗ порівняно із ручною обробкою ПМТ підвищилася майже в 10 разів. Аналіз помилок першого роду виявлення КЗ свідчить, що точність автоматичного виявлення може бути дещо підвищена за рахунок подальшого доопрацювання онтології.

Висновки. Таким чином, за рахунок обробки значних обсягів даних, що містяться в ПМТ відкритих ресурсів ІТС, можливо збільшити кількість виявлених КЗ, при цьому для підвищення оперативності цього процесу необхідно автоматизувати аналіз змісту текстів. З цією метою в статті запропоновано методику виявлення КЗ у ПМТ, яка ґрунтується на логіко-семантичному аналізі їх змісту із застосуванням формальних правил виявлення.

Відмінністю даної методики від існуючих є застосування семантичних мереж та онтології для опису змісту текстів і профілю безпечного функціонування КС відповідно. При цьому виявлення КЗ здійснюється шляхом зіставлення семантичної мережі тексту, який аналізується, з онтологією КС та застосування формальних правил ідентифікації. Розроблені правила відображають сигнатурний метод виявлення загроз та метод виявлення аномалій, що дає змогу ідентифікувати як уже відомі КЗ, так і абсолютно нові.

Результати експериментального дослідження точності та оперативності розробленої методики свідчать про значне (на порядок) скорочення часу обробки при сталому рівні точності виявлення (більше 80%).

Подальших досліджень потребує проблема оцінюванні рівня небезпеки для КС в цілому на підставі часткових фактів, що свідчать про наявність загроз її елементам.

СПИСОК ЛІТЕРАТУРИ

1. Даник Ю. Національна безпека: запобігання критичним ситуаціям : монографія / Ю. Даник, Ю. Катков, М. Пічугін. – Житомир : Рута, 2006. – 388 с. : іл.
2. Комар М. П. Интеллектуальная система обнаружения сетевых атак на информационные ресурсы на основе метода главных компонент / М. П. Комар // Системи обробки інформації. – Х. : ХУПС, 2011. – № 8 (98). – С. 203–207.
3. Манокін Є. В. Ідентифікація загроз / Є. В. Манокін // Оборонний вісник. – К., 2012. – № 11–12. – С. 19–22.
4. Лукацкий А. В. Обнаружение атак / А. В. Лукацкий. – [2-е изд.]. – СПб. : БХВ-Петербург, 2003. – 608 с.
5. Лаптев В. Н. Методика обнаружения и идентификации компьютерных атак в информационно-телекоммуникационных системах на основе метода индуктивного прогнозирования состояний [Электронный ресурс] / В. Н. Лаптев, О. В. Сидельников // Научный журнал КубГАУ. – 2012. – № 77(03). – Режим доступа : http://ej.kubagro.ru / 2012/03/pdf/32.pdf.
6. Даник Ю. Г. Визначення сутності та змісту кібернетичної загрози / Ю. Г. Даник, В. І. Шестаков, С. В. Чернишук // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць ЖВІ НАУ. – Житомир : ЖВІ НАУ, 2012. – Спецвип. 2. – С. 5–14.
7. Бакаев В. Н. Теория автоматического управления : учеб. пособ. / В. Н. Бакаев. – Вологда : ВоГТУ, 2002. – 211 с.
8. Шестаков В. І. Модель виявлення кібернетичних загроз за результатами моніторингу відкритих джерел інформації / В. І. Шестаков, С. В. Чернишук // Збірник наукових праць ВІ КНУ ім. Тараса Шевченка. – К. : ВІ КНУ, 2012. – № 39. – С. 224–228.
9. Автоматическая обработка текстов на естественном языке и компьютерная лингвистика : учеб. пособ. / [Е. И. Большакова, Э. С. Клышинский, Д. В. Ландэ и др.]. – М. : МИЭМ, 2011. – 272 с.
10. Басипов А. А. Семантический поиск: проблемы и технологии / А. А. Басипов, О. В. Демич // Вестник Астрахан. гос. техн. ун-та. – Астрахань, 2012. – № 1. – С. 104–111.
11. Ландэ Д. В. Основы интеграции информационных потоков : монография / Д. В. Ландэ. – К. : Инжиниринг, 2006. – 240 с.
12. Джоджик Я. Реформа Збройних сил – стратегія знищення української армії [Електронний ресурс] / Я. Джоджик // Народне слово : загальнополіт. тижневик Укр. Народ. Партії. – Режим доступу : http://slovo-unp.com/admin/print.php?subaction= showfull&id= 1333633657&archive=1334237759&start_ from =&ucat=1&i=archive.
13. Хвещук Ю. Війна всередині Збройних Сил України [Електронний ресурс] / Ю. Хвещук. – Режим доступу : http://politiko.ua/blogpost100122.
14. Болтян О. Знищення армії та флоту – зрада Батьківщини [Електронний ресурс] / О. Болтян. – Режим доступу : http://www.krym.svoboda.org.ua/dopysy/dopysy/041350.
15. Кому выгоден развал Украинских Вооруженных Сил [Электронный ресурс]. – Режим доступа : http://zarodinu.org.ua/page/74.
16. Такаев Б. Что стоит за реформой Вооруженных сил Украины? [Электронный ресурс] / Б. Такаев. – Режим доступа : http://odnarodyna.com.ua/content/chto-stoit-za-reformoy-vooruzhennyh-sil-ukrainy-i.

17. Із життя «кротів» в Україні… [Електронний ресурс]. – Режим доступу : poslezavtra.com.ua/iz-zhittya-krotiv-v-ukraïni.
18. Знання-орієнтований підхід до автоматизації інформаційно-аналітичної діяльності / І. В. Замаруєва, А. О. Рось, О. Ю. Губайдулін та ін. // Проблемы программирования : научн. журнал. – К. : ИПС НАНУ, 2000. – № 1–2. – С. 601–614.
19. Знание-ориентированный подход к анализу естественно-языковой текстовой информации в интересах мониторинга и оценки ситуаций [Электронный ресурс] / В. Н. Шемаев, И. В. Замаруева, М. В. Приймак, Е. Н. Дубровский. – Режим доступа : http://iai.kpi.ua/_archive/2003/shemaev.pdf.
20. Автоматическая классификация текстовых документов с использованием нейросетевых алгоритмов и семантического анализа [Электронный ресурс] / А. М. Андреев, Д. В. Березкин, В. В. Морозов, К. В. Симаков. – Режим доступа : http://www.inteltec.ru/publish/articles/textan/RCDL2003.shtml.
21. Артемьева И. Л. Математические модели онтологий предметных областей. Ч. 1. Существующие подходы к определению понятия «Онтология» / И. Л. Артемьева, А. С. Клещев // Науч.-техн. информ. Серия 2 «Информационные процессы и системы». – М. : ВИНИТИ, 2001. – № 2. – С. 20–27.
22. Гаврилова Т. А. Базы знаний интеллектуальных систем : учеб. для вузов / Т. А. Гаврилова, В. Ф. Хорошевский. – СПб. : Питер, 2000. – 384 с.
23. Структура Збройних Сил України [Електронний ресурс]. – Режим доступу : http://www.mil.gov.ua/index.php?part=structure&lang=ru.
24. Командування Збройних Сил України [Електронний ресурс]. – Режим доступу : http://www.mil.gov.ua/index.php?part=command&lang=ru.
25. Положення про Міністерство оборони України [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/406/2011.
26. Озброєння Збройних Сил України [Електронний ресурс]. – Режим доступу : http://www.mil.gov.ua/index.php?part=armament&lang=ru.
27. Біла книга – 2012. Збройні Сили України [Електронний ресурс]. – Режим доступу : http://www.mil.gov.ua/files/white_book/WB_2012_ua.pdf.

Подано 20.08.13

С. В. Чернышук

МЕТОДИКА ОБНАРУЖЕНИЯ КИБЕРНЕТИЧЕСКИХ УГРОЗ В ЕСТЕСТВЕННО-ЯЗЫКОВЫХ ТЕКСТАХ

На основании анализа проявлений кибернетических угроз в естественно-языковых текстах определены правила их идентификации и раскрыта методика их обнаружения.

S. V. Chernyshuk

METHODOLOGY OF CYBERTRAETS DETECTION IN NATURE LANGUAGE TEXTS

On basis of cyberthreats manifestations in nature language texts analysis rules of their identification are developed and methodology of their detection is suggested.