information operation. The goal is, usually, to change the opinion of the target audience about the information operation object. Based on data obtained from experts and open sources, the knowledge base of the subject domain is built in the form of a weighted graph. It represents a hierarchy of factors that influence the main goal. Beside numeric value, the impact of each sub-goal in the graph is also characterized by certain delay and duration. With these parameters taken into consideration, the degree of main goal achievement is calculated, and changes of target parameters of information operation object are monitored. Usage of the proposed methodology is demonstrated on the example of detection and analysis actions intended to discredit the National academy of sciences of Ukraine. For this purpose, automated decision support and content monitoring tools are used.

**Keywords:** open source; decision support system; information operation; content monitoring system; expert estimate.

**Циганок Віталій Володимирович**, доктор технічних наук, старший науковий співробітник, завідувач лабораторії систем підтримки прийняття рішень, Інститут проблем реєстрації інформації Національної академії наук України, Київ, Україна.

ORCID: 0000-0002-0821-4877.

E-mail: vitaliy.tsyganok@gmail.com.

**Каденко Сергій Володимирович**, кандидат технічних наук, старший науковий співробітник, старший науковий співробітник лабораторії систем підтримки прийняття рішень, Інститут проблем реєстрації інформації Національної академії наук України, Київ, Україна.

ORCID: 0000-0001-7191-5636.

E-mail: seriga2009@gmail.com.

**Андрійчук Олег Валентинович**, кандидат технічних наук, старший науковий співробітник лабораторії систем підтримки прийняття рішень, Інститут проблем реєстрації інформації Національної академії наук України, Київ, Україна.

ORCID: 0000-0003-2569-2026.

E-mail: oleh.andriichuk@i.ua.

**Tsyganok Vitaliy**, doctor of engineering, senior researcher, head of decision support systems laboratory, Institute for information recording of the National academy of sciences of Ukraine, Kyiv, Ukraine.

**Kadenko Sergii**, candidate of technical sciences, senior researcher, senior researcher of decision support systems laboratory, Institute for information recording of the National academy of sciences of Ukraine, Kyiv, Ukraine.

**Andriichuk Oleh**, candidate of technical sciences, senior researcher of decision support systems laboratory, Institute for information recording of the National academy of sciences of Ukraine, Kyiv, Ukraine.

DOI 10.20535/2411-1031.2019.7.1.184225
УДК 004(056.53::622)

ВАЛЕНТИН ПЕТРИК,
АНДРІЙ ДАВИДЮК

## СИСТЕМА АВТОМАТИЗОВАНОГО АНАЛІЗУВАННЯ ДАНИХ ПРО ТЕРОРИСТИЧНУ ДІЯЛЬНІСТЬ З РЕСУРСІВ МЕРЕЖІ ІНТЕРНЕТ

Створено систему автоматизованого аналізування даних про терористичну діяльність з ресурсів мережі Інтернет. Її використання орієнтовано на попередження терористичних актів

та протидії їм шляхом аналізу текстового контенту на предмет наявності в ньому даних, що пов'язані з терористичною діяльністю. Ця діяльність належить до найбільш важко прогнозованих та небезпечних для суспільства і держави явищ. Вона вирізняється особливим динамізмом і багатоплановістю, розвинутою технічною оснащеністю, високим рівнем структурної організації, наявністю значних фінансових активів, а також здатністю до адаптації і модернізації в умовах основних соціальних тенденцій сучасності – глобалізації та інформатизації. Це підтверджує існування реальної загрози національній та кібербезпеці держави. Здебільшого для попередження та протидії терористичній діяльності надається перевага організаційним заходам. Тому для протидії терористичній діяльності запропоновано якісно нові підходи. Одним з таких підходів є аналізування даних про терористичну діяльність з ресурсів мережі Інтернет. Для вирішення цієї задачі поширене застосування інформаційних технологій, зокрема, програмних засобів. З огляду на це проаналізовано засоби автоматизованого аналізування даних. Серед них виокремлено спеціалізовані системи моніторингу інформаційного простору. Вони характеризуються, по-перше, оперативністю, яку не можуть забезпечити традиційні пошукові системи; по-друге, повнотою, яку не завжди забезпечують звичайні агрегатори новин і, по-третє, необхідні аналітичні засоби, які дозволяють користувачеві створювати звіти за публікаціями заданої тематики протягом певного періоду часу. Як наслідок, встановлено, що застосування автоматизованого аналізування даних досить ефективне для попередження і протидії терористичним актам. Тому для реалізації такої протидії запропоновано систему автоматизованого аналізування даних про терористичну діяльність з ресурсів мережі Інтернет. Перевагами її використання є зручність, зокрема, наявність простого інтерфейсу та можливість виявлення ознак терористичної діяльності.

**Ключові слова:** автоматизована система; аналізування даних; терористична діяльність; програмне забезпечення.

**Вступ.** У сучасних умовах інформація і управління нею стає підставою і головним інструментом досягнення цілей в новітній світобудові. Офіційно про це заявлено 22 липня 2000 року в Японії в ході підписання керівниками восьми провідних країн світу «Окінавської хартії глобального інформаційного суспільства» [1]. У цьому документі задекларовано, що інформаційно-телекомунікаційні технології стали одним з найбільш важливих факторів, що впливають на формування суспільства XXI ст.

Зі збільшенням обсягів інформації інформаційний простір став переповненим неактуальною, неповною інформацією, яка хаотично розповсюджується. Унаслідок цього пошук глибинних семантичних зв'язків, достовірної інформації та знань ускладнюються. Тому, для вирішення цієї проблеми застосовується аналізування даних (Data Mining). Саме поняття "Data Mining", що з'явилося в 1978 році, набуло великої популярності в сучасному трактуванні приблизно з першої половини 1990 років. До цього часу аналізування даних здійснювався в рамках прикладної статистики, при цьому в основному вирішувалися завдання оброблення невеликих баз даних [2].

Важливе завдання "Data Mining" пов'язане з виокремленням із тексту його характерних елементів або властивостей, наприклад: метадані документа, ключові слова з анотації [3]. Ці елементи можна використати для віднесення документа до деяких категорій з наперед заданими схемами класифікації. Цим також забезпечується новий рівень семантичного пошуку документів [4].

**Аналіз останніх досліджень і публікацій.** Актуальність даного дослідження зумовлена існуючими терористичними загрозами життю суспільства, а особливо в умовах збройного конфлікту з Російською Федерацією. Дослідженню застосування інформаційних технологій для боротьби з тероризмом присвячено праці [5] - [8]. При цьому зосереджується увага на методах класифікації даних, описано роль Організації об'єднаних націй у боротьбі з тероризмом, здійснено аналіз продуктивності класифікаторів (Lazy Tree, Multilayer

Perceptron, Multiclass, Naïve Bayes) для моніторингу тенденцій появи терористичних актів у світі. Запропоновано методологію на основі аналізування веб трафіку. Застосування ангоритму інтелектуального аналізу даних веб сайтів дозволило в режимі реального часу виявляти користувачів мережі Інтернет, що можуть бути підозрюваними в терористичній діяльності [6]. Проаналізовано можливості використання правоохоронними органами інтелектуального аналізу даних при відстеженні діяльності терористів та їх злочинної діяльності [7]. Серед досягнень вітчизняних вчених варто виокремити дослідження, що направлені на аналізування великих обсягів даних [8]. З огляду на це можна вважати, що проблема боротьби з тероризмом є загальносуспільною проблемою всього світу. Застосування інформаційних технологій для протидії тероризму є прогресивним напрямком забезпечення безпеки кожної держави та її громадян. Тому аналізування даних про терористичну діяльність з ресурсів мережі Інтернет є актуальним.

**Метою статі є** виявлення ознак терористичної діяльності завдяки розробленню системи автоматизованого аналізування даних про таку діяльність з ресурсів мережі Інтернет.

**Виклад основного матеріалу дослідження.** Для оперативного аналізу інформаційної обстановки з метою виявлення ознак терористичної діяльності застосовуються спеціалізовані системи моніторингу інформаційного простору. Такі системи забезпечують, по-перше, оперативність, яку не можуть забезпечити традиційні пошукові системи (час індексації мережевого контенту навіть кращими з них становить від декількох діб до декількох тижнів), по-друге, повноту (як у переліку джерел, так і поданні матеріалів джерел), яку не завжди забезпечують звичайні агрегатори новин і, по-третє, необхідні аналітичні засоби, які дозволяють користувачеві створювати звіти, що базуються на публікаціях за заданою тематикою протягом певного періоду часу.

У плані протидії терористичній діяльності, частиною якої є інформаційні операції слід уважно стежити за динамікою публікацій про цільову організацію, якщо є можливість, з урахуванням тональності цих публікацій, користуватися доступними аналітичними засобами, наприклад, вейвлет-аналізу. При цьому доцільно орієнтуватися на можливі моделі інформаційних атак, наприклад, якщо ця модель охоплює фази: “фонові публікації” – “затишшя” – “артпідготовка” – “затишшя” – “атака”, то вже за першими трьома елементами можна з великою імовірністю передбачити прийдешні події. Багато сучасних інформаційно-аналітичних систем містять засоби відображення статистики входження в бази даних понять. Зокрема, для розроблення системи використовувалася підсистема формування статистики входження до веб-ресурсу InfoStream [8].

При вивченні трендів інформаційних операцій як тимчасові ряди розглядаються ряди за кількістю тематичних публікацій протягом певного проміжку часу (наприклад, за добу). Тому для виявлення трендів досліджуються інформаційні потоки за терористичною тематикою.

У результаті аналізу численних діаграм поведінки тематичних інформаційних потоків, виявлено найбільш типові, базові профілі їх поведінки. Тематичні потоки щодо терористичної діяльності, характеризуються симетричною кривою динаміки, можуть бути вузькі, короткочасні, так і розтягнуті в часі.

У разі інформаційних потоків, які асоціюються з конкретними тематичними потоками, необхідно описувати динаміку кожного з них окремо. При цьому доцільно враховувати те, що зростання одного з них може автоматично призводити до зменшення інших і навпаки. Тому обмеження на обсяги інформації за всіма тематиками поширюється і на сукупність усіх інформаційних сюжетів. У разі вивчення загального інформаційного потоку спостерігається явище “перетікання” обсягів публікацій з одних, які втрачають актуальність інформаційних сюжетів, до інших. Наведені у тренді повідомлень тематики, які за змістом відповідають етапам інформаційної підготовки терористичних актів показані на рис. 1.

При цьому аналітикам доцільно орієнтуватися на такі моделі, наприклад, якщо моніторинг дозволяє визначити фази: “фон” – “затишшя” – “артпідготовка” – “затишшя” – “атака”. Тоді вже за першими трьома компонентами можна з великою імовірністю передбачити майбутні події [9].

Варто зазначити, що подібна динаміка кількості тематичних повідомлень під час проведення інформаційних операцій описується рівнянням поширення електромагнітних хвиль [10]:

$$y = A + Bt\sin(t),$$

де $t$ – час;

$A$ – константа кількості повідомлень,

$B$ – константа фази інформаційної операції, які визначаються емпірично.

На рис. 2 діаграма кількості публікацій відповідає тренду терористичної діяльності. Об'єднуючи графіки початку інформаційної підготовки терористичного акту (див. рис. 1) і тренду терористичної діяльності (див. рис. 2) можна отримати повне графік відображення терористичних операцій в інформаційному просторі.

Представлені моделі повністю відповідають реальним даним, які екстрагуються системами контент–моніторингу [11]. Тому наведені залежності можуть використовуватися як шаблони для виявлення терористичних операцій як шляхом аналізування ретроспективного фонду мережевих публікацій, так і шляхом оперативного моніторингу появи їх ознак в реальному часі.

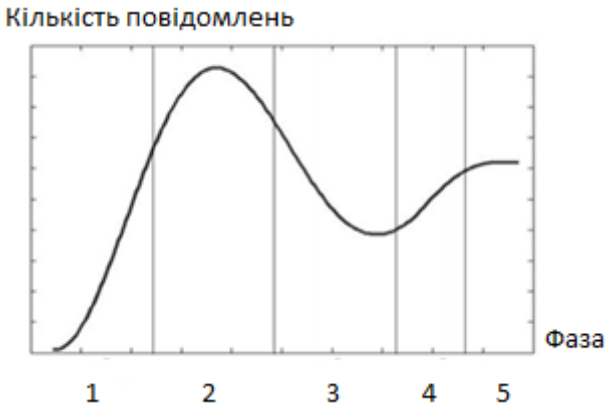



Рисунок 1 – Динаміка кількості тематичних повідомлень під час проведення інформаційної підготовки терористичного акту: 1 – "фон";
2 – "затишшя";
3 – "артпідготовка";
4 – "затишшя";
5 – "атака / тригер зростання"

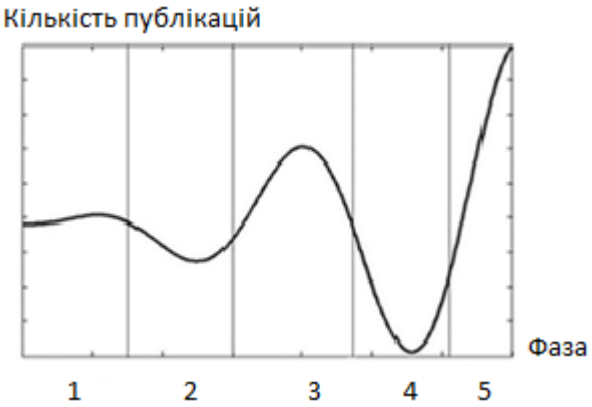



Рисунок 2 – Діаграма кількості публікацій, відповідних тренду терористичної діяльності:
1 – атака / тригер зростання;
2 – пік завищених очікувань;
3 – втрата ілюзій;
4 – суспільне усвідомлення;
5 – продуктивність / фон

Як відомо, для виявлення терористичних операцій доцільно стежити за динамікою публікацій і, якщо є можливість, користуватися доступними аналітичними засобами, засобами цифрової обробки даних і розпізнавання образів, наприклад, вейвлет –аналізу, Data Mining. Розроблена система реалізуватиме алгоритм, який представлено на рис. 3.

Практичне застосування розробленої системи є досить простим. Перед інсталяцією програмного забезпечення для коректної його роботи потрібно виконати початкові налаштування. Зокрема зазначити шлях до директорії завантажень, оскільки безпосередньо будемо працювати з її вмістом, а також шляху до директорії, у якій будуть зберігатися конвертовані дані, для подальшої роботи з ними (див. ліст. 1). Виконавши дані конфігураційні зміни, можна здійснити інсталяцію програмного забезпечення "Teror_analiz" на жорсткий диск комп'ютера користувача. Наступним кроком є запуск програмного забезпечення. Після появи діалогового вікна програми, вона готова до налаштування параметрів роботи (задання ключових слів) та безпосереднього використання.

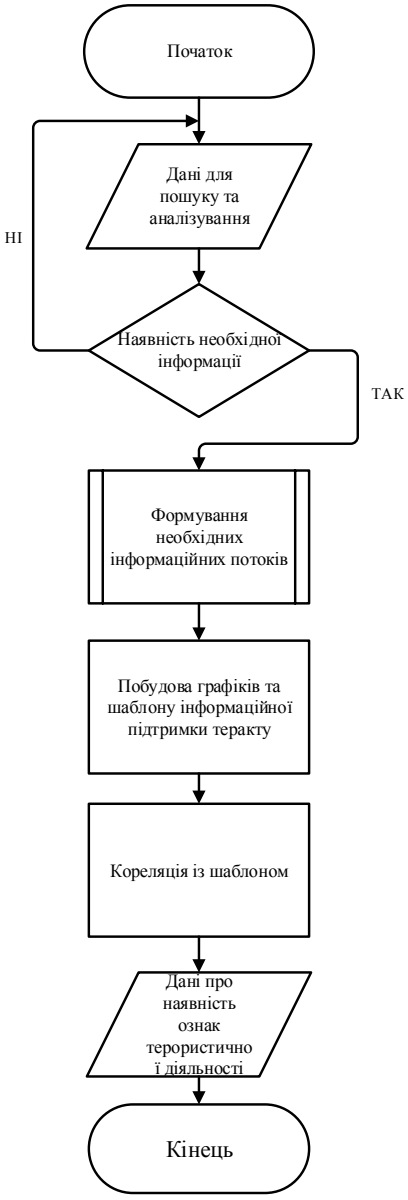



Рисунок 3 – Алгоритм роботи системи

*Лістинг 1*

```
def graf():
(pd.read_csv(r'C:\Users\Chechire Cat\Downloads\multiTimeline.csv', header=None, names=['dt',
'val'], parse_dates=['dt'], dtype={'val': 'float'}, skiprows=3)
[['val', 'dt']]
   .to_csv(r'C:\Users\Chechire Cat\PycharmProjects\mosia\primer.csv', index=False, header=None,
date_format='%d.%m.%Y'))
(pd.read_csv(r'C:\Users\Chechire Cat\Downloads\multiTimeline(1).csv', header=None, names=['dt',
'val'], parse_dates=['dt'], dtype={'val': 'float'}, skiprows=3)
[['val', 'dt']]
.to_csv(r'C:\Users\Chechire Cat\PycharmProjects\mosia\primer(1).csv', index=False, header=None,
date_format='%d.%m.%Y'))
(pd.read_csv(r'C:\Users\Chechire Cat\Downloads\multiTimeline(2).csv', header=None, names=['dt',
'val'], parse_dates=['dt'], dtype={'val': 'float'}, skiprows=3)
[['val', 'dt']]
.to_csv(r'C:\Users\Chechire Cat\PycharmProjects\mosia\primer(2).csv', index=False, header=None,
date_format='%d.%m.%Y'))
```

Після запуску виконавчого файлу починаємо роботу з системою через графічний інтерфейс. Для цього у вікні клієнтського інтерфейсу потрібно ввести потрібний запит та натиснути кнопку “Почати” (див. рис. 4).

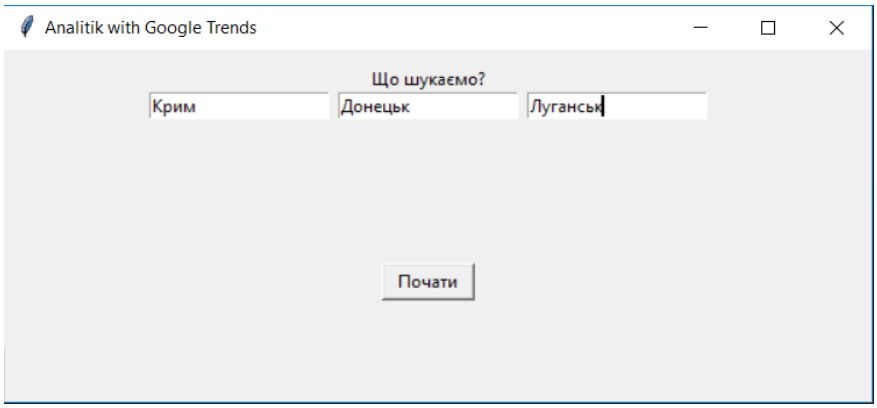



Рисунок 4 – Клієнтський інтерфейс програми

Після того як з’єднання встановлено вікно закриється, і програма з’єднується з браузером і переходить на сайт Google Trends. На ньому безпосередньо будуть завантажуватися дані для побудови графіків (див. рис. 5) [9].

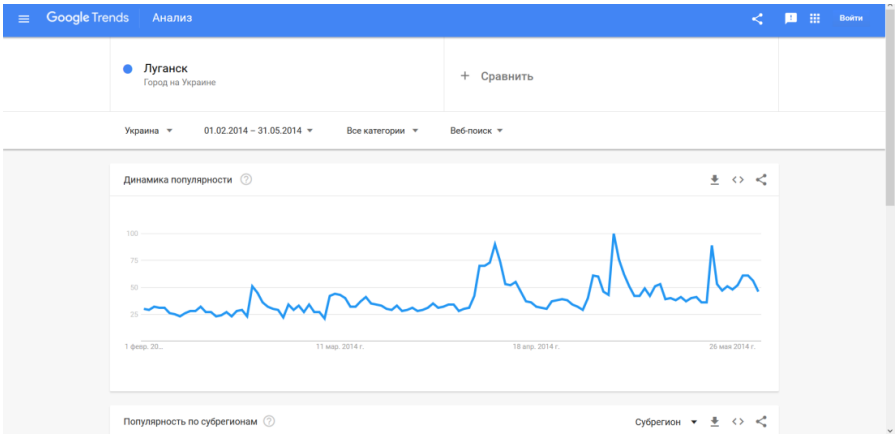



Рисунок 5 – Сайт Google Trends

Після цього браузер зробить запит до користувача для уточнення подальших дій, а саме завантаження даних чи їх перевірки, обираємо “Зберегти файл”. Далі буде побудований графік інформаційного потоку за ознаками терористичної діяльності (див. рис. 6).

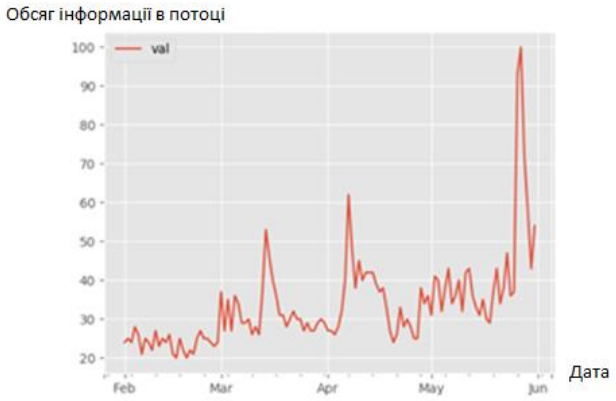
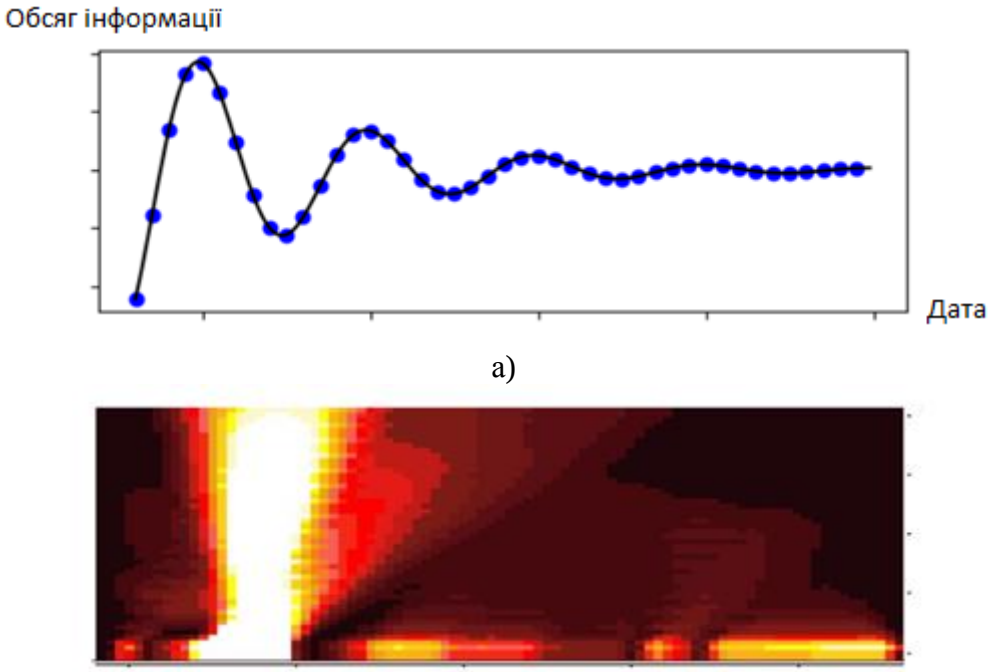



Рисунок 6 –Графік інформаційного потоку за ознаками терористичної діяльності

В кінці отримуємо графік, на якому зображена кореляція інформаційного потоку з шаблоном інформаційної підтримки теракту (див. рис. 7). На даному графіку (дворівнева гістограма або, інакше, теплова карта) можемо бачити результати кореляції в зручній для сприйняття формі. Світлі відтінки означають збіг з шаблоном, тоді як темні вказують на ділянку, що максимально відрізняється від шаблону тому можемо указати, що в другій частині графіка нам показано високу вірогідність появи терористичного акту, або ж діяльності пов'язаної з ним.




а)

б)

Рисунок 7 –Графік залежності обсягів інформації від часу її поширення
а)неперервна функція; б) неперервне вейвлет перетворення

Застосування системи автоматизованого аналізування даних про терористичну діяльність з ресурсів мережі Інтернет дозволить ефективно попереджати та протидіяти терористичній діяльності, стануть вагомим доповненням до існуючих організаційних заходів.

**Висновки.** Сучасний етап світового розвитку характеризується все більш зростаючим впливом інформації, засобів інформатизації та зв'язку, а також суспільних відносин, що складаються в процесі збору, обробки, зберігання, передачі та поширення інформації на економічний, соціальний і духовний розвиток як окремих держав, так і світової спільноти у цілому. Незважаючи на переваги інформатизації та автоматизації, до основних загроз сучасному суспільству віднесено терористичну діяльність, що стрімко розвивається з розвитком інформаційних технологій.

Сучасний тероризм вирізняється особливим динамізмом і багатоплановістю, розвинутою технічною оснащеністю, високим рівнем структурної організації, наявністю значних фінансових активів, а також здатністю до адаптації й модернізації в умовах основних соціальних тенденцій сучасності – глобалізації та інформатизації. Це підтверджує існування реальної загрози національній та кібербезпеці держави.

З огляду на це, розроблено систему автоматизованого аналізування даних про терористичну діяльність з ресурсів мережі Інтернет. Програмна реалізація даної системи може використовуватися для аналітичної діяльності щодо попередження та протидії терористичній діяльності. Вона дозволяє оперативного аналізувати інформаційну обстановку

для виявлення ознак терористичних операцій, здійснювати моніторинг інформаційного простору. Таке програмне забезпечення характеризується, по-перше, оперативністю, яку не можуть забезпечити традиційні пошукові системи (час індексації мережевого контенту навіть кращими з них становить від декількох діб до декількох тижнів), по-друге, повнотою (як в плані джерел, так і подання матеріалів джерел), яку не завжди забезпечують звичайні агрегатори новин і, по-третє, які дозволяють користувачеві створювати звіти, що базуються на публікаціях за заданою тематикою протягом певного періоду часу.

**У перспективах подальших досліджень** планується модернізація розробленого програмного забезпечення щляхом розширення його функціоналу. Також планується розробка автоматизованих засобів привентивної протидії інформаційним операціям.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


[1] И. Бочарников, "Информационное противодействие терроризму в современных условиях". [Електронний ресурс]. Доступно: https://elibrary.ru/item.asp?id=21292041. Дата обращения: Март 21, 2019.

[2] B. Kemper, "Principles of Exploratory Data Analysis in Problem Solving: What Can We Learn from a Well-Known Case?". [Online]. Available: https://www.researchgate.net/publication/228410393_Principles_of_Exploratory_Data_Analysis_in_Problem_Solving_What_Can_We_Learn_from_a_Well-Known_Case. Accessed on: Mar 21, 2019.
doi: 10.1080/08982110903188276 2009.

[3] M. Ghada Tolan, and S. O. Soliman, "An Experimental Study of Classification Algorithms for Terrorism Prediction", *International Journal of Knowledge Engineering*, vol. 1, no. 2, pp. 107-112, 2015.
doi: 10.7763/IJKE.2015.V1.18.

[4] "Алгоритмы интеллектуального анализа данных (службы Analysis Services — Интеллектуальный анализ данных) – SQL Server 2014 Analysis Services". [Електронний ресурс]. Доступно: https://docs.microsoft.com/ru-ru/sql/analysis-services/data-mining/data-mining-algorithms-analysis-services-data-mining?view=sql-server-2014. Дата обращения: Март 21, 2019.

[5] V. Kumar, M. Mazzara, M. Gen., A. Messina, and J. Lee, "A Conjoint Application of Data Mining Techniques for Analysis of Global Terrorist Attacks – Prevention and Prediction for Combating Terrorism", [Online]. Available: https://arxiv.org/abs/1901.06483. Accessed on: Mar 21, 2019.
doi: 10.1007/978-3-030-14687-0_13.

[6] Y. Elovici, A. Kandel, M. Last, B. Shapira, and O. Zaafrany, "Using Data Mining Techniques for Detecting Terror-Related Activities on the Web". [Online]. Available: https://www.semanticscholar.org/paper/Using-Data-Mining-Techniques-for-Detecting-on-the-Elovici-Kandel/11d8bc502b639a1c31167502f2afacb3973695bc. Accessed on: March 21, 2019.

[7] R. Okonkwo, and F. Enem, "Combating crime and terrorism using data mining techniques". [Online]. Available: https://www.semanticscholar.org/paper/Combating-crime-and-terrorism-using-data-mining-Okonkwo-Enem/3dc2c4e99f0feae4f93fb2440a4eb5c1e40cf9cf. Accessed on: Mar 21, 2019.

[8] Д. Ланде, та Н. Гулякіна, "Деякі нелінійні методи, що застосовуються при розпізнаванні інформаційних операцій", Анотований збірник проектів спільного конкурсу ДФФД-БРФФД. [Електронний ресурс]. Доступно: http://dwl.kiev.ua/art/dffd/index.html. Дата звернення: Берез. 21, 2019.

[9] А. Дудатьєв, "Моделі для організації протидії інформаційним атакам", Захист інформації, т. 17, №. 2, с. 157-162, 2015.
doi: 10.18372/2410-7840.17.8790.

[10] “Уравнения электромагнитной волны в физике. SolverBook”. [Електронний ресурс]. Доступно: http://ru.solverbook.com/spravochnik/uravneniya-po-fizike. Дата звернення: Берез. 21, 2019.
[11] The Sherman Kent Center for Intelligence Analysis. Au.af.mil., 2012. [Online]. Available: http://www.au.af.mil/au/awc/awcgate/cia/strategic_warning_kent.htm. Accessed on: Mar 21, 2019.

Стаття надійшла до редакції 28.03.2019.

## REFERENCE

[1] I. Bocharnikov, “Information Counteraction to Terrorism in Modern Conditions”. [Online]. Available: https://elibrary.ru/item.asp?id=21292041. Accessed: March 21, 2019.
[2] B. Kemper, “Principles of Exploratory Data Analysis in Problem Solving: What Can We Learn from a Well-Known Case?”. [Online]. Available: https://www.researchgate.net/publication/228410393_Principles_of_Exploratory_Data_Analysis_in_Problem_Solving_What_Can_We_Learn_from_a_Well-Known_Case. Accessed on: Mar 21, 2019.
doi: 10.1080/08982110903188276 2009.
[3] M. Ghada Tolan, and S. O. Soliman, “An Experimental Study of Classification Algorithms for Terrorism Prediction”, *International Journal of Knowledge Engineering*, vol. 1, no. 2, pp. 107-112, 2015.
doi: 10.7763/IJKE.2015.V1.18.
[4] “Data Mining Algorithms (Analysis Services – SQL Server 2014 Analysis Services”. [Online]. Available: https://docs.microsoft.com/en/sql/analysis-services/data-mining/data-mining-algorithms-analysis-services-data-mining?view=sql-server-2014. Accessed on: March 21, 2019.
[5] V. Kumar, M. Mazzara, M. Gen., A. Messina, and J. Lee, “A Conjoint Application of Data Mining Techniques for Analysis of Global Terrorist Attacks – Prevention and Prediction for Combating Terrorism”, [Online]. Available: https://arxiv.org/abs/1901.06483. Accessed on: Mar 21, 2019.
doi: 10.1007/978-3-030-14687-0_13.
[6] Y. Elovici, A. Kandel, M. Last, B. Shapira, and O. Zaafrany, “Using Data Mining Techniques for Detecting Terror-Related Activities on the Web”. [Online]. Available: https://www.semanticscholar.org/paper/Using-Data-Mining-Techniques-for-Detecting-on-the-Elovici-Kandel/11d8bc502b639a1c31167502f2afacb3973695bc. Accessed on: March 21, 2019.
[7] R. Okonkwo, and F. Enem, “Combating crime and terrorism using data mining techniques”. [Online]. Available: https://www.semanticscholar.org/paper/Combating-crime-and-terrorism-using-data-mining-Okonkwo-Enem/3dc2c4e99f0feae4f93fb2440a4eb5c1e40cf9cf. Accessed on: Mar 21, 2019.
[8] Д. Ланде, та Н. Гулякіна, “Деякі нелінійні методи, що застосовуються при розпізнаванні інформаційних операцій”. [Електронний ресурс]. Доступно: http://dwl.kiev.ua/art/dffd/index.html. Дата звернення: Берез. 21, 2019.
[9] A. Dudatyev, “Models to counter information attacks”, Ukrainian Information Security Research Journal, vol. 17, no. 2, pp. 1567-162, 2015.
doi: 10.18372/2410-7840.17.8790.
[10] “Electromagnetic wave equations in physics. SolverBook”. [Online]. Available: http://solverbook.com/spravochnik/uravneniya-po-fizike. Accessed on: March 21, 2019.
[11] “The Sherman Kent Center for Intelligence Analysis”. [Online]. Available: http://www.au.af.mil/au/awc/awcgate/cia/strategic_warning_kent.htm. Accessed on: March 21, 2019.

VALENTYN PETRYK,
ANDRII DAVYDIUK

**SYSTEM OF AUTOMATED DATA ANALYSING ABOUT TERRORISTIC ACTIVITY FROM INTERNET RESOURCES**

A system for automated analysis of terrorist activity data from Internet resources was created. Its use is aimed at preventing and countering terrorist acts by analyzing textual content to contain data related to terrorist activity. This activity is one of the most severely predicted and dangerous for society and the state phenomena. It is characterized by a special dynamism and multifaceted nature, advanced technical equipment, a high level of structural organization, the presence of significant financial assets, as well as the ability to adapt and modernize in the context of the main social trends of today - globalization and informatization. This confirms the existence of a real threat to the national and cybersecurity of the state. Mostly to prevent and counter-terrorist activity, organizational measures are preferred. Therefore, counteraction to terrorist activity requires qualitatively new approaches. One such approach is to analyze terrorist activity data from Internet resources. To address this challenge, the widespread use of information technology, in particular software. In this context, automated data analysis tools are analyzed. Among them are specialized systems for monitoring information space. They are characterized, first of all, by the speed that traditional search engines cannot provide; secondly, the completeness not always provided by conventional news aggregators and, thirdly, the necessary analytical tools that allow the user to generate reports on publications of a given topic over some time. As a result, the use of automated data analysis is quite effective in preventing and counteracting terrorist attacks. Therefore, a system for automated analysis of terrorist activity data from Internet resources has been proposed for the implementation of such counteraction. The advantages of using it are the convenience, in particular, the presence of a simple interface and the ability to detect signs of terrorist activity.

**Keywords:** automated system; analysis of information; terrorist activity; software.

**Петрик Валентин Михайлович,** кандидат наук з державного управління, доцент, доцент кафедри управління та тактико-спеціальної підготовки, Інститут спеціального зв'язку та захисту інформації національного технічного університету "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0002-7714-0111.

E-mail: iszzi_open@ukr.net.

**Давидюк Андрій Вікторович,** аспірант, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

ORCID: 0000-0003-1238-2598.

E-mail: andrey19941904@gmail.com.

**Petryk Valentyn,** candidate of state-owned management, associate professor, associate professor of the management and tactical training academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

**Davydiuk Andrii,** postgraduate student, Pukhov Institute for Modeling in Energy Engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.