https://doi.org/10.31891/2219-9365-2022-71-3-8
УДК 004.056:621.397.3:004.942

ВОЛОДИМИР ДЖУЛІЙ
Хмельницький національний університет
https://orcid.org/0000-0003-1878-4301
e-mail: dg2303@ukr.net
ІГОР МУЛЯР
Хмельницький національний університет
https://orcid.org/0000-0002-6659-605X
muliariv@khmnu.edu.ua
ОРИСЛАВА ЗАЦЕПІНА
Хмельницький національний університет
e-mail: orysiia@gmail.com
ВАДИМ ПІЧУРА
Хмельницький національний університет
e-mail: vadimpichura007@gmail.com

ІНФОРМАЦІЙНО-ОЗНАКОВА МОДЕЛЬ ДЖЕРЕЛА ШКІДЛИВОЇ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

Розглянута актуальна задача побудови інформаційно-ознакової моделі джерела шкідливої інформації в соціальних мережах. Інформаційно-ознакова модель шкідливої інформації в соціальних мережах, дозволяє сформувати дані для виявлення та протидії поширенню шкідливої інформації в мережі. Комплекс моделей складається з моделі шкідливої інформації, інформаційно-ознакової моделі шкідливої інформації, моделі джерела інформації, моделі соціальної мережі. Кожна з моделей містить унікальні атрибути та відношення між інформаційними об'єктами, також комплекс моделей дозволяє сформувати відповідні вимоги до алгоритмів оцінки та аналізу джерел повідомлень та забезпечує вибір контрзаходів.

Ключові слова: моделі, алгоритми*, модель шкідливої інформації, соціальні мережі, контрзаходи, джерела повідомлень.*

VOLODYMYR DZHULIY, IGOR MULYAR,
ORYSLAVA ZACEPINA, VADYM PICHURA
Khmelnytskyi National University

AN INFORMATION-SIGN MODEL OF THE SOURCE OF HARMFUL INFORMATION IN SOCIAL NETWORKS

The problem of detecting and countering the spread of harmful information has an insufficient number of scientific and technical solutions. The available means of combating and detecting harmful information in social networks do not meet the requirements for adequacy, speed, accuracy and completeness of the decisions made. This is due to the following reasons: the systems are divided into two unrelated modules - monitoring, countermeasures, between which the operator is located. It is necessary to process extremely large flows of messages in real time, implement countermeasures in a short period of time, in manual mode the operator is unable to stop the spread of malicious information in the social network.

The task of the research is to develop: models of harmful information, source and social network; algorithms for analyzing the sources of messages spreading harmful information in social networks and ranking countermeasures.

Solving the set tasks will allow: to improve the quality of decisions made in the process of detecting and countering harmful information; sort information objects of influence for the operator by priority; set the input data for the configuration of the system for detecting and countering the spread of malicious information in networks.

The information-sign model of malicious information in social networks allows you to generate data for detecting and countering the spread of malicious information in the network. The complex of models consists of a model of malicious information, an information-sign model of malicious information, a model of the source of information, a model of a social network. Each of the models contains unique attributes and relationships between information objects, as well as a set of models allows for the formation of appropriate requirements for algorithms for the evaluation and analysis of message sources and provides a choice of countermeasures.

Keywords: models, algorithms, malicious information model, social networks, countermeasures, message sources.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

На сучасному етапі, глибина проникнення у повсякденне життя соціальних мереж є значною. Перевагою соціальних мереж є можливість учасникам комунікації висловлювати оперативно свою думку значній кількості групі людей, публікувати відео-, медіа файли. Соціальні мережі є не лише засобом спілкування групи людей, а й також інструментом поширення інформації, в тому числі шкідливої інформації. Необхідно зазначити, що злочинні та терористичні угруповання беруть на озброєння, дедалі частіше, засоби інформаційного впливу, розробляють та пишуть стратегії, спрямовані на залучення нових

адептів та розширення сфери впливу через соціальні мережі. Таким чином, однією зі складових надійного забезпечення інформаційної безпеки держави є виявлення, моніторинг, аналіз та активна протидія розповсюдженню шкідливої інформації в соціальних мережах [1-3].

Проблема виявлення та протидії поширенню шкідливої інформації має не достатню кількість науково-технічних рішень. Доступні засоби протидії та виявлення шкідливої інформації в соціальних мережах не відповідають вимогам до адекватності, швидкості, точності та повноти прийнятих рішень. Це обумовлено наступними причинами: системи розділені на два незв'язаних модулі – моніторинг, протидія, між якими знаходиться оператор. Соціальні мережі мають складну структуру, до складу яких входять різнорідні повідомлення, що недостатньо враховується під час реалізації мети протидії – джерело, тип повідомлення, та інші характеристики. Необхідно обробляти у реальному масштабі часу надвеликі потоки повідомлень, в стислий термін реалізувати контрзаходи, в ручному режимі оператор не в змозі зупинити поширення шкідливої інформації в соцмережі [2-6].

Постановка задачі

Протидія поширенню шкідливої інформації у соцмережах є важливим елементом інформаційної безпеки особистості, суспільства, держави, проте більшість систем, на теперішній час не враховують простір функціональності системи виявлення та протидії шкідливій інформації, необхідна автоматизація процесу протидії. Соціальні мережі мають складну структуру, параметри повідомлень та джерел не в повній мірі враховуються під час виборів мети виявлення та протидії шкідливій інформації. При розробці методу протидії поширенню шкідливої інформації необхідно: в повній мірі враховувати кількість повідомлень на сторінці, характеристики джерела, зворотній зв'язок від джерела та аудиторії; підтримувати дві стадії: експлуатація, налаштування; ранжувати контрзаходи з урахуванням коефіцієнтів складності [4,7,8].

Задача дослідження полягає у розробці: моделей шкідливої інформації, джерела та соціальної мережі; алгоритмів проведення аналізу джерел повідомлень поширення шкідливої інформації у соціальних мережах та проведення ранжування контрзаходів; методу виявлення та протидії поширенню шкідливої інформації у соціальних мережах з урахуванням вимог до обґрунтованості; архітектури компонентів системи протидії поширеню шкідливої інформації в соцмережах [8,9].

Вирішення поставлених задач дозволить: підвищити якість прийнятих рішень у процесі виявлення та протидії шкідливій інформації; сортувати інформаційні об'єкти впливу для оператора по пріоритету; задати вхідні дані налаштування системи виявлення та протидії поширенню шкідливої інформації в мережах.

Основна частина

Моделі даних соціальних мереж характеризуються, незалежно від їх структури, загальними атрибутами - джерела, повідомлення, ознаки зворотного зв'язку на повідомлення суб'єкта. Наявність ознак зворотного зв'язку в моделі соцмережі дозволяє характеризувати джерело повідомлення. Нехай $ACTIVITY\ \{countLike, countREpost, countComment, countView\}$ множина у повідомленнях від реципієнтів всіх ознак зворотного зв'язку інформації у соцмережі, де $countLike$ – кількість позначок, $countREpost$ – кількість копій з посиланням на джерело («репостів»), $countComment$ - кількість коментарів, $countView$ – кількість переглядів.

Виходячи з поставлених задач, необхідно визначити атрибути множини $ACTIVITY$, а також відношення $R(SOURCE, MESSAGE)$, які в подальшому дозволять проводити аналіз повідомлення та джерела, що містять шкідливу інформацію та вибирати відповідний об'єкт для протидії. Наприклад, якщо сума елементів активності до повідомлення дає можливість обчислити індекс активності повідомлення, таким чином може бути отриманий, в даній ситуації, інтегральний показник індексу активності, який в свою чергу залежить від кількості повідомлень джерела, очевидно одним із атрибутів моделі даних джерела буде *index active*. Якщо кількість переглядів повідомлення дозволяє обчислити індекс перегляду, таким чином можемо отримати інтегральний показник індексу перегляду для джерела інформації, отримаємо наступний атрибут моделі даних джерела - *index_viewability*. Функція $f : MESSAGE \to SOURCE$ задає область визначення, вхідні та вихідні значення (аргументи). Функція сюр'єктивна - є відображенням множини $MESSAGE$ на множину $SOURCE$, при відображенні кожен елемент множини $SOURCE$ є образом множини $MESSAGE$ (хача б одного елемента). Таким чином, отримаємо:

$$\forall source \in SOURCE \exists message \in MESSAGE : source = f(message) \quad (1)$$

Повідомлення (аргументи) на стіні джерела можуть бути різного типу (відповідь, пост, коментар). Таким чином, для окремих аргументів (повідомлень) може бути заданий числовий коефіцієнт (рейтинг) у дереві повідомлень соціальної мережі (рис. 1).

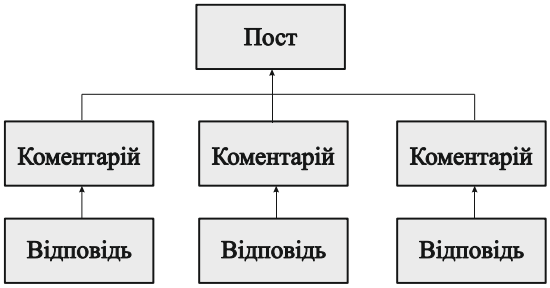

Рис. 1. Дерево повідомлень соцмережі

В залежності від кількості аргументів, джерело повідомлення можливо оцінити за потенціалом (potential): джерело із низьким потенціалом; джерело із середнім потенціалом; джерело із високим потенціалом. Якщо джерело повідомлень має атрибути: index_active, index_viewability, то можна задати індекс впливу - index_impact, який відображає рівень впливу джерела повідомлення на аудиторію.

Виділимо атрибути в кортежі, що характеризують *SOURCE* через елементи множини *ACTIVITY* і відношення $R(SOURCE, MESSAGE)$ - $\langle index_{active}, index_{viewabiliy}, potential, index_{impact} \rangle$. Також, атрибутами моделі джерел повідомлень є: *social_network_type* – тип даних структури соцмереж; *followers* – кількість пов'язаних користувачів; *registration time* - час реєстрації в мережі джерела інформації. Модель даних джерела повідомлень відрізняється наявністю нових атрибутів, класів, відношень.

Розглянемо модель шкідливої інформації в мережі Інтернет. Основою для формування поняття - шкідлива інформація виступають два терміни [10]: *I* – information (Інформація); *IO* – information object (Інформаційний об'єкт) –логічно цільний блок відповідної інформації, представлений у фіксованої формі, використовується та створений в ході інформаційної діяльності. Формально терміни пов'язані між собою, так, що $IO \subseteq I$ (рис. 2. а) - інформаційний об'єкт є елементом множини всієї інформації, над якою проводиться аналіз. Із терміном «інформація» також пов'язаний термін - *IA* – information area («інформаційний простір»), а множини I, IO є підмножинами інформаційного простору. Соціальні мережі представляють собою сукупність взаємозалежних вузлів: спільноти, акаунти, сторінки, вкладення, пости; зв'язки між об'єктами – однорівневі відношення (перебувають у співтоваристві, у друзях); відношення вкладеності (сторінка запису містить посилання на пост, стіна містить пост) [6-8]. Соціальні мережі можуть бути представленні графами: частина об'єктів - інформаційні, вершина графа, а зв'язки між об'єктами - ребра між вершинами. Таким чином, справедливо, що $IO \subseteq I \subseteq IA$, $SN \subseteq I \subseteq IA$, область перетину між *SN* (соцмережа) та *IO* є предметом дослідження у соціальних мережах розробки моделі шкідливої інформації (рис. 2. б).

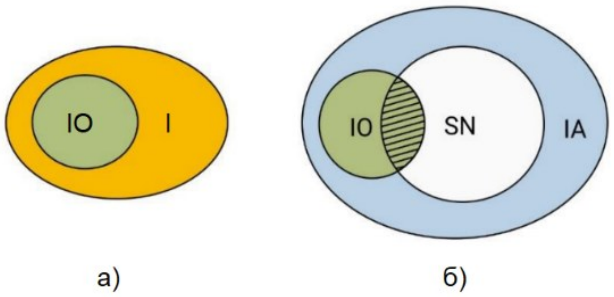

Рис. 2. Графічне представлення відношень множини інформаційного простору

Інформаційний об'єкт - *MIO* (шкідливий інформаційний об'єкт), містить відповідні ознаки, які дозволяють прийняти рішення, що інформація завдає шкоди державі, суспільству, бізнесу особистості. В залежності від умови експерт встановлює ознаки *Token* інформаційної загрози *T*. Наприклад, батько сам вибирає обмеження для дитини, у випадку використання система батьківського контролю. Якщо представник бізнес - компанії зацікавлений у захисті конфіденційного інформації бізнеса, в даній ситуації він їх сам задає. Таким чином, у соціальній мережі, теоретико-множинна модель шкідливої інформації, включає наступні базові елементи: *IO* - інформаційний об'єкт (Information Object); *T* - інформаційна загроза (Threat); *MIO* – шкідливий інформаційний об'єкт; *Token* – ознака інформаційної загрози, що знаходиться у шкідливому інформаційному об'єкті; *Feature* – ознака наявності інформаційного об'єкта [0,1]; зв'язок між інформаційними об'єктами.

Теоретико-множинна модель шкідливої інформації (2) формально представлена наступним чином:

$$\begin{aligned} &IO = \{io\}; MIO = \{io\}; MIO_i = \{io\} \\ &MIO \subset IO; \forall io \in MIO : io \in IO \\ &MIO_i \subseteq MIO; \forall io \in MIO_i : io \in MIO \\ &Token_{mio_i} \subset T; Token_{mio_i} = \{t\} \\ &CheckFeature(io,t) = \{True; False\} \\ &io \in MIO_i \Leftrightarrow \exists Token_{mio_i} : checkFeature(io,t) = True \end{aligned}, \quad (2)$$

де IO – множина інформаційних об'єктів, io – інформаційний об'єкт, T - множина ознак інформаційної загрози, t_i –*i -а* ознака інформаційної загрози, MIO – множина шкідливих інформаційних об'єктів мережі, MIO_i - *i-й* клас шкідливої інформації, $Token_{mio_i}$ - множина ознак загрози, що характеризують MIO.

Таким чином, для виявлення та протидії поширенню шкідливій інформації в мережі необхідно задати набір ознак, характерних для інформаційної загрози в соціальній мережі.

Особливістю моделі шкідливої інформації соціальної мережі є те, що модель допускає наявність дискретних ознак у множині ознак: зв'язок інформаційного об'єкта з іншими інформаційними об'єктами у соцмережі; частота повторення ознаки; дата створення інформаційного об'єкта.

Протидія поширенню шкідливого інформаційного об'єкта в соціальній мережі може здійснюватися лише на рівні джерел чи повідомлень. Таким чином, необхідно виділити такі інформаційні загрози та відповідні інформаційні ознаки повідомлення у соцмережі, що характеризують його як шкідливий об'єкт. Інформаційно-ознакова модель (табл.1) - впорядкована сукупність інформації про зв'язки повідомлень та їх ознак зі змістом повідомлень. Інформаційні ознаки повідомлень - окремі властивості повідомлень, їх зміст. Інформаційна загроза – задається оператором системи. Шкідлива інформація в соціальній мережі – задається оператором шляхом формування набору відповідних ключових слів. Інформаційні ознаки - формують множину усіх можливих інформаційних ознак *t*. На рис.3 наведено співвідношення, взаємозв'язок різних рівнів інформаційно-ознакової моделі шкідливої інформації Показано, що формується повідомлення, розміщується повідомлення в джерелі розповсюдження, на сторінці групи, облікового запису. Повідомлення можуть містити ознаки шкідливої, а також не містити ознаки шкідливої інформації. Інформаційні ознаки (табл. 1) формують рівень інформаційних загроз в соціальній мережі.

Таблиця 1

Інформаційно-ознакова модель шкідливої інформаціїсоціальної мережі

Інформаційні загрози	**Шкідлива інформація у соцмережах**	**Інформаційні ознаки**
Приклад Самогубство	Приклад Повідомлення, що містить прохання, пропозицію, наказ зробити самогубство, описує самогубство як спосіб вирішення проблем	t_1
	Приклад Повідомлення, що містить позитивну оцінку схвалення вчинення самогубства, дій, спрямованих на самогубство	t_2

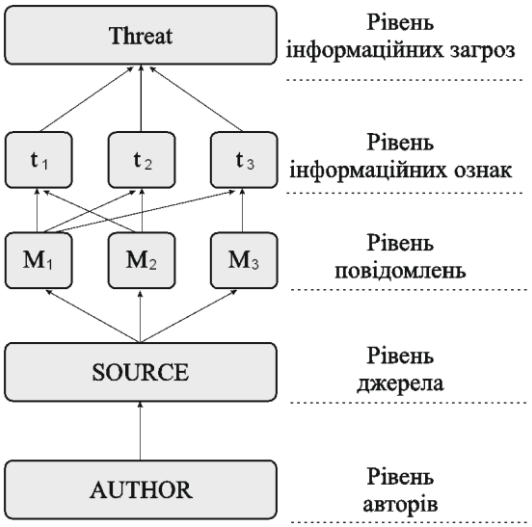

Рис. 3. Інформаційно-ознакова модель шкідливої інформації

Таким чином, зібравши відповідну інформацію на сторінці джерела можливо визначити, які з цих повідомлень інформаційної мережі належать до шкідливих повідомлень. Результатом виявлених загроз та їх кількості буде прийняте відповідне рішення про протидію джерелу, повідомленню.

Запропонована інформаційно-ознакова модель шкідливої інформації в соціальних мережах, дозволяє сформувати дані для виявлення та протидії поширенню шкідливої інформації в мережі. Комплекс моделей складається з моделі шкідливої інформації, інформаційно-ознакової моделі шкідливої інформації, моделі джерела інформації, моделі соціальної мережі. Кожна з моделей містить унікальні атрибути та відношення між інформаційними об’єктами, також комплекс моделей дозволяє сформувати відповідні вимоги до алгоритмів оцінки та аналізу джерел повідомлень та забезпечує вибір контрзаходів.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Запропонована модель соціальної мережі, що включає джерела, повідомлення, зв'язки (відношення) між інформаційними об’єктами, відрізняється наявністю нових рв'язків та структурних елементів. Розроблено модель джерела, в якій враховуються наступні параметри: індекс впливу, індекс активності, індекс перегляду, потенціал. Запропонована теоретико-множинна модель шкідливої інформації в соціальній мережі, складається з ознак шкідливої інформації та взаємопов'язаних об'єктів, що в сукупності формують шкідливо-інформаційні об'єкти в мережі Інтернет. Також розроблена інформаційно-ознакова модель шкідливої інформації в соціальних мережах, дозволяє сформувати дані для виявлення та протидії поширенню шкідливої інформації в соціальних мережах.

Література

1. Ленков, С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, В.М. Джулій, В.С. Орленко, О.В. Сєлюков, А.В. Атаманюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.

2. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/ articles/view/011–02–23/26490.htm.

3. Ленков, С.В. Методы и средства защиты информации. В 2-х томах /С.В. Ленков, Д.А. Перегудов, В.А. Хорошко –К: Арий, 2008.–464с

4. Остапов С. Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король–Харків : Вид-во ХНЕУ, 2016. – 476 с.

5. Лєнков, С.В. Аналіз існуючих методів та алгоритмів виявлення атак в бездротових мережах передачі даних / С.В. Лєнков, В.М. Джулій, Н.М. Берназ, С.О. Божук // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 56. – С.124-132

6. Довгий, С.О. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / С.О. Довгий, О.Я. Савченко, П.П. Воробієнко – К.: Український Видатничій Центр, 2012. – 520 с.

7. Джулій, В.М. Модель оцінки ймовірнісно-часових характеристик інформаційної взаємодії в мережі інтернет речей / В.М. Джулій, І.В. Муляр, О.В. Сєлюков, Б.М. Кізюн // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – Вип. № 63. – С.96-106

8. Джулій, В.М., Кльоц Ю.П., Муляр І.В., Жилевич М.Л., Джулій А.В. Контроль додатків інтернет-трафіка комп’ютерних мереж методами машинного навчання. Вісник Хмельницького національного університету. Технічні науки. 2021. № 5. С. 22-26.

9. Джулій, В.М. Метод класифікації додатків трафіка комп'ютерних мереж на основі машинного навчання в умовах невизначеності / В.М. Джулій, О.В. Мірошніченко, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №74. – С. 73-82.

10. Лавров, Є. А. Математичні методи дослідження операцій : підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик – Суми : Сумський державний університет, 2017. – 212 с.

References

1. Lenkov, S.V. (2020), Model bezpeky poshyrennia zaboronenoi informatsii v informatsiino-telekomunikatsiinykh merezhakh / S.V. Lenkov, V.M. Dzhulii, V.S. ORLENKO, O.V. Sieliukov, A.V. Atamaniuk // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – №68. – pp. 53-64.

2. Cotsialni merezhi – realni zahrozy virtualnoho svitu. [Elektronnyi resurs]. – Rezhym dostupu : http://ogo.ua/ articles/view/011–02–23/26490.htm

3. Lenkov, S.V. (2008), Metodyy sredstva zashchytы ynformatsyy. V 2-kh tomakh / S.V. Lenkov, D.A. Perehudov, V.A. Khoroshko – K: Aryi–464s.

4. Ostapov, S. E. (2016) Tekhnolohii zakhystu informatsii: navchalnyi posibnyk / S.E. Ostapov, S.P. Yevseiev, O.H. Korol–Kharkiv : Vyd-vo KhNEU. – 476 s.

5. Lenkov, S.V. (2017), AnalIz Isnuyuchih metodiv ta algoritmiv viyavlennya atak v bezdrotovih merezhah peredachI danih / S.V. Lenkov, V.M. Dzhuliy, N.M. Bernaz, S.O. Bozhuk // Zbirnik naukovih prats Viyskovogo Institutu Kiyivskogo natsionalnogo universitetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vip. No 56. – p.124-132

6. Dovhyi, S.O. (2012), Suchasni telekomunikatsii: merezhi, tekhnolohii, ekonomika, upravlinnia, rehuliuvannia /S.O. Dovhyi, O.I. Savchenko, P.P. Vorobiienko – K.: Ukrainskyi Vydatnychii Tsentr. – 520p.

7. Dzhulii, V.M. (2019), Model otsinky ymovirnisno-chasovykh kharakterystyk informatsiinoi vzaiemodii v merezhi internet rechei / V.M. Dzhulii, I.V. Muliar, O.V. Sieliukov, B.M. Kiziun // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vyp. № 63. – p.96-106

8. Dzhulii V.M., Klots Yu.P., Muliar I.V., Zhylevych M.L., Dzhulii A.V. (2021), Kontrol dodatkiv internet-trafika kompiuternykh merezh metodamy mashynnoho navchannia. Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – Khmelnytskyi. – №5. – pp. 22–26.

9. Dzhulii, V.M. (2022), Metod klasyfikatsii dodatkiv trafika kompiuternykh merezh na osnovi mashynnoho navchannia v umovakh nevyznachenosti / V.M. Dzhulii, O.V. Miroshnichenko, L.V. Solodieieva // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vyp. №74. – pp. 73-82.

10. Lavrov, Ye. A. (2017.), Matematychni metody doslidzhennia operatsii : pidruchnyk / Ye. A. Lavrov, L. P. Perkhun, V. V. Shendryk – Sumy : Sumskyi derzhavnyi universytet, – 212 p.