

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ХАРЧОВИХ ТЕХНОЛОГІЙ

**ІНСТИТУТ КОМП'ЮТЕРНИХ СИСТЕМ І ТЕХНОЛОГІЙ
«ІНДУСТРІЯ 4.0» ІМ. П.Н. ПЛАТОНОВА**

**ХІІ МІЖНАРОДНА
НАУКОВО-ПРАКТИЧНА
КОНФЕРЕНЦІЯ**

**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І
АВТОМАТИЗАЦІЯ – 2019**

**INFORMATION TECHNOLOGIES AND
AUTOMATION – 2019**

Збірник доповідей

Частина I

Одеса,
17-18 жовтня 2019

Секція 1

Наукові напрямки:

**Комп'ютерні
телекомунікаційні мережі та
технології**

**Математичне моделювання
та інформаційні технології**

**Список
скорочень організацій, представники яких взяли участь у конференції**

Таблиця 1

Скорочення	Повна назва організації	Місто	Країна
BNTU	Belarusian National Technical University	Minsk	Belarus
CAFU	CRIAME of Armed Forces of Ukraine	Kyiv	Ukraine
DMTSAU	Dmutro Motorny Tavria State Agrotechnological University	Melitopol	Україна
DNU	Vasyl' Stus Donetsk National University	Вінниця	Україна
EKSTU	East Kazakhstan State Technical University D. Serikbayev	Ust-Kamenogorsk	Kazakhstan
IAEI SB RAS	Institute of Automation and Electrometry of the Siberian Branch of the Russian Academy of Sciences	Novosibirsk	Russia
IRTC IT&S NAS AND MES	International Research and Training Center for Information Technologies and Systems of the National Academy of Sciences (NAS) of Ukraine and Ministry of Education and Science (MES) of Ukraine	Kyiv	Ukraine
KGES	Kharkiv general education school	Kharkov	Україна
LPNUU	Lviv Polytechnic National University	Lviv	Ukraine
NTU "KhPI"	National Technical University "Kharkiv Polytechnic Institute"	Kharkov	Україна
NTU «KPI»	National Technical University "Igor Sikorsky Kyiv Polytechnic Institute"	Kyiv	Ukraine
NU «OMA»	Національний університет «Одеська морська академія»	Одеса	Україна
NULESU	National University of Life and Environmental Sciences of Ukraine	Kyiv	Ukraine
NUOS	NATIONAL UNIVERSITY OF SHIPBUILDING NAMED BY ADM. MAKAROV	Nikolaev	Ukraine
ONAFIT	Odessa National Academy of Food Technologies	Odessa	Ukraine
ONU	Odessa I.I.Mechnikov National University	Odessa	Ukraine
SSU	Sukhumi State University	Sukhumi	Georgia
VNTU	Vinnitsia National Technical University	Vinnitsia	Ukraine
БНТУ	Белорусский национальный технический университет	Минск	Белоруссия
ВНТУ	Вінницький національний технічний університет	Вінниця	Україна
ДВНЗ «КНУ»	Державний вищий навчальний заклад «Криворізький національний університет»	Кривий Ріг	Україна
ДонНТУ	Донецький національний технічний університет	Покровськ	Україна
ІК НАН України	Інститут кібернетики імені В.М. Глушкова НАН України	Київ	Україна
НТУ «ХПІ»	Национальный технический университет "Харьковский политехнический институт"	Харків	Україна
НТУУ "КПІ"	Національний технічний університет «Київський політехнічний інститут» імені Ігоря Сікорського"	Київ	Україна
НУ «ЛП»	Національний університет «Львівська політехніка»	Львів	Україна
ОДАТРА	Одеська державна академія технічного регулювання та якості	Одеса	Україна

Продовження таблиці 1

Скорочення	Повна назва організації	Місто	Країна
ОНАЗ	Одеська національна Академія зв'язку ім. О.С. Попова	Одеса	Україна
ОНАПТ	Одесская национальная академия пищевых технологий	Одесса	Украина
ОНАХТ	Одеська національна академія піщевих технологій	Одеса	Україна
ОНПУ	Одеський національний політехнічний університет	Одеса	Україна
ОНУ	Одеський національний університет імені І. І. Мечникова	Одеса	Україна
ОТК ОНАХТ	Одеський технічний коледж Одеської національної академії харчових технологій	Одеса	Україна
ПНПУ	Південноукраїнський національний педагогічний університет ім. К.Д. Ушинського	Одеса	Україна
ХНУРЕ	Харківський національний університет радіоелектроніки	Харків	Україна
ХРТК	Харківський радіотехнічний технікум	Харків	Україна
ЦНДІ ОВТ ЗС України	Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України	Київ	Україна
ЮНПУ	Южноукраинский национальный педагогический университет им. К.Д.Ушинского	Одесса	Украина

ЗМІСТ

ROMANYUK S.O., ROMANYUK O.N., PAVLOV S.V., PYVOVAR M.A. USAGE OF 3D IMAGES FOR GENETIC DISEASES DIAGNOSIS (<i>VNTU, Ukraine</i>).	7
KUPRIYANOV A.B., XU SHANSHAN. CONVOLUTIONAL NEURAL NETWORK AND LIDAR IMAGES IN FOREST INVENTORY (<i>BNTU, Belarus</i>)	9
СЕМЕНЮК В.О. МАТЕМАТИЧНІ МОДЕЛІ ПРОГНОЗУВАННЯ РЕЗУЛЬТАТІВ ФУТБОЛЬНИХ МАТЧІВ (<i>ВНТУ, Україна</i>)	10
KERESLIDZE N.G. MATHEMATICAL AND COMPUTER MODELS OF INFORMATION WARFARE (<i>SSU, Georgia</i>)	13
KOMLEVA N.O., НЕКНТ Н.І. WEB SERVICE FOR AUTOMATED BUILDING OF THE SEMANTIC CORE OF A SITE (<i>ONPU, Ukraine</i>)	16
КУЛЬЧИЦЬКИЙ О.С., ЛАДИГІНА О.А. ОСОБЛИВОСТІ НАДІЙНОСТІ ТА ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ (<i>ЦНТУ, Україна</i>)	19
ШВЕЦЬ В.Т. ІНФОРМАЦІЙНА ЕНТРОПІЯ І СВОБОДА ВИБОРУ (<i>ОНАХТ, Україна</i>)	22
VYATKIN S.I., ROMANYUK A.N., NECHYPORUK M.L. A NUMERICAL METHOD FOR ANIMATING THREE-DIMENSIONAL OBJECTS (<i>VNTU, Ukraine, IAEI SB RAS, Russia</i>)	26
ЧАПЛІНСЬКИЙ Ю.П., СУББОТІНА О.В. ВИКОРИСТАННЯ ОНТОЛОГО-КЕРОВАНОЇ ТЕХНОЛОГІЇ СИСТЕМОЇ ОПТИМІЗАЦІЇ В СИСТЕМІ УПРАВЛІННЯ БЕПЕЧНІСТЮ ПРОДУКТІВ ХАРЧУВАННЯ (<i>ІК НАН України</i>)	29
FAINZILBERG L.S. INTELLECTUAL INFORMATION TECHNOLOGIES ON SMARTPHONE (<i>IRTC IT&S NAS AND MES, Ukraine</i>)	31
ВОЛОШИНА В.А., ЖУКОВ С.О. БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ СИСТЕМ (<i>ВНТУ, Україна</i>)	34
НАЗАРОВА І.А. МОДЕЛЮВАННЯ ПАРАЛЕЛЬНИХ ПРОЦЕСІВ ПРИ РОЗВ'ЯЗАННІ БАГАТОВИМІРНИХ ЖОРСТКИХ ЗАДАЧ КОШІ (<i>ДонНТУ, Україна</i>)	36
СИРЕНКО А.І. АНАЛІЗ ПРОИЗВОДИТЕЛЬНОСТИ ВИРТУАЛЬНЫХ МАШИН В СИСТЕМЕ ВИРТУАЛИЗАЦИИ CITRIX XENSERVER (<i>ОНАХТ, Україна</i>)	38
ПУЙДЕНКО В.О. СИНТЕЗ МОДУЛЯ ДОСТОВІРНОСТІ/LRU КЕШ-ПАМ'ЯТІ ТА АСОЦІАТИВНОГО КЕШ – БУФЕРУ СТОРІНКОВОГО ПЕРЕТВОРЕННЯ ПРОЦЕСОРНОГО ЯДРА АРХІТЕКТУРИ IA-32 (<i>ХРТК, Україна</i>)	39
LEVINSKYI M.V., LEVINSKYI V.M. AUTOMATIC CONTROL SYSTEMS STEADY STATE PROCESSES ANALYSIS IMPLEMENTATIONS IN MATLAB (<i>NU «ОМА», ОНАФТ, Україна</i>)	42
МОРОЗОВ Д.О., ЗІНОВАТНА С.Л. АВТОМАТИЗАЦІЯ РОЗРАХУНКУ ЗАЛИШКІВ ТОВАРІВ З УРАХУВАННЯМ ПЕРЕТВОРЕННЯ ОСНОВНОГО ПРОДУКТУ У НОВИЙ ВИД ПРОДУКТУ (<i>ОНПУ, Україна</i>)	43
МАЗУРОК Т.Л. НЕЧІТКА МОДЕЛЬ ІНТЕГРОВАНОГО НАВЧАННЯ (<i>ПНПУ, Україна</i>)	46
КРИВЧЕНКО Ю.В., КРИВЧЕНКО А.А. КОМП'ЮТЕРНА РЕАЛІЗАЦІЯ АТРАКТОРНИХ СИСТЕМ У БАГАТОВИМІРНИХ ФАЗОВИХ ПРОСТОРАХ (<i>ОНАХТ, ОТК ОНАХТ, Україна</i>)	49
КОЗАК І.Р. КОМП'ЮТЕРИЗОВАНА СИСТЕМА ЗБОРУ БІОМЕДИЧНИХ ПОКАЗНИКІВ ЛЮДИНИ (<i>ВНТУ, Україна</i>)	51
НАЙДЬОНОВ О.Ю., ЗІНОВАТНА С.Л. АЛГОРИТМ КОНТРОЛЮ ОПЛАТИ З УРАХУВАННЯМ ФІКСОВАНОГО ПАКЕТУ СЕРВІСІВ (<i>ОНПУ, Україна</i>)	53
ГУСЯТИН В.М., ЛЕБЕДЄВ В.О. АРХІТЕКТУРА НАПІВПАРАЛЕЛЬНОЇ ГЛИБОКОЇ НЕЙРОННОЇ МЕРЕЖІ (<i>ХНУРЕ, Україна</i>)	55
КОТЛИК С.В., СОКОЛОВА О.П., КОРНІЄНКО Ю.К. ОГЛЯД ЗАСТОСОВУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ 3D МОДЕЛЮВАННЯ (<i>ОНАХТ, Україна</i>) . . .	58
OTNOSHENNYI I.O. DESIGNING THE SOFTWARE SYSTEM FOR RECOGNITION OF A HANDWRITTEN TEXT USING A NEURAL NETWORK (<i>ONPU, Ukraine</i>)	61
СЛУШНА Н.В. ПЕРСПЕКТИВИ РОЗВИТКУ І ВИКОРИСТАННЯ СИСТЕМ ООБД (<i>ОНАХТ, Україна</i>)	64
KOMLEVA N.O., SHYDER M.O. OUTSOURCING PLANNING PROGRAM OF	65

MATHEMATICAL AND COMPUTER MODELS OF INFORMATION WARFARE

ABSTRACT - NEW MATHEMATICAL AND COMPUTER MODELS OF INFORMATION WARFARE ARE BUILT AND RESEARCHED IN THE GIVEN WORK. ONE OF THE FORMS OF INFORMATION WARFARE IS CONSIDERED: DISSEMINATION OF FALSE INFORMATION. GROUPS ARE DEFINED - RISKS PRONE TO THE PERCEPTION OF MISINFORMATION; ADEPTS - WHO HAVE RECEIVED FALSE INFORMATION AND WITH IMMUNITY - REJECT FALSE INFORMATION FROM THE BEGINNING OR FUTURE ADEPTORS. MODELS OF NUMERICAL CHANGE IN THE COMPOSITION OF THESE GROUPS ARE CONSIDERED.

Formulation of the problem. Among the various forms of introducing the Information Warfare, of particular interest is the type of information warfare, the purpose of which is to influence the psyche of people, manipulating the consciousness of the masses, disorienting individuals, imposing strange stereotypes of behavior on them, etc. Such an effect is sometimes achieved by specific information flows that intensively fall on members of society. A feature of such information flows is the dissemination of false information, misinformation, etc. More details about the goals and means of introducing the Information Warfare through the "word" can be found in [1], [2]. The relevance and significance of the problem associated with organized campaigns for the dissemination of knowingly false information is adequately evaluated in the modern world and certain steps have been taken in this direction. For example, by the decision of the Heads of State and Government of the Council of Europe, a special group "Strategic Communication with the East" was established - **EastStratCom Task Force**, <https://euvsdisinfo.eu>, for the informational "counteraction to Russian disinformation campaigns" aimed at discrediting the EU's Eastern Neighborhood Policy. As stated in the report of the special group - quote: "in four years of its existence, the EU campaign against disinformation has issued more than 140 "Review of Disinformation" newsletters containing more than 5,000 cases of reports of disinformation in 18 different languages. The product is regularly used and cited by various governments, ministries, government agencies, secret services, researchers, analytic centers and journalists across Europe and beyond" – end of quote [3].

It is logical that a campaign against disinformation can be planned and carried out more effectively if there is a clear idea and quantitative characteristics of the false information dissemination. Naturally, the study of false information dissemination using mathematical and computer modeling, conducting computer experiments along with other methods of researching the task, allows us to effectively describe the process under study and plan actions against the disinformation campaign. When modeling the dissemination of false information, we will assume that false information negatively affects the health of human psyche and nervous system. Then we have the right to identify false information with an infection, a virus causing painful changes in a person and the right to apply the achievements of modeling the spread of epidemics by modifying them for the task.

Task formulation. Suppose that in a society with a number of people N at each time t there is a so-called Risk Group (RG) in the number of people $G(t)$ who are exposed to false information. From the RG people who received false information and believed in it move to the Group of Adepts (GA). Let us say, that at the moment of time t the number of people in GA is $A(t)$. Suppose that a person from the GA is aware for a time μ that false information has been imposed on him, after which he leaves this group and replenishes the Group with Immunity (GI). Let us denote the number of people in the GI at time point t through $I(t)$. Noting that the GI member is already insured against repeated exposure to false information, i.e. gains certain immunity. The transition of an individual from one group to another can be represented by the following scheme: $RG \rightarrow GA \rightarrow GI$. If we assume that false information can be disseminated by directly contacting members from the Risk and Adept groups, then we can mathematically describe the process of transition from RG to GA. It is also not difficult to describe the transition from GA to GI. As a result, we obtain, as a first approximation, the following mathematical model for the dissemination of false information:

$$\begin{cases} \frac{dG(t)}{dt} = -\alpha G(t)A(t), \\ \frac{dA(t)}{dt} = \alpha G(t)A(t) - \gamma A(t), \\ \frac{dI(t)}{dt} = \gamma A(t). \end{cases} \quad (1)$$

Where $\alpha, \gamma > 0$, $\gamma = \frac{1}{\mu}$, α - is the false information dissemination coefficient, γ is the false information release coefficient. To the ODE system (1) we add the initial conditions:

$$G(0) = G_0 > 0, \quad A(0) = A_0 > 0, \quad I(0) = I_0 = 0, \quad (2)$$

We obtain a mathematical model **RAI** of false information dissemination, which is analogous to the well-known classical **Kermak-Mackendrick SIR** model [4]. Note that from (1) it follows

$$G(t) + A(t) + I(t) = N.$$

From the second equation of system (1), the conditions are determined under which the number of adherents will increase or not. Meanwhile, the number of adherents is indicators in general, how much the society is exposed to false information i.e. how misinformed it is. It is advisable to introduce a threshold effect, in which it is determined whether the society is massively affected by false information or not. At

$$G_0 > \gamma/\alpha, \quad (3)$$

the number of adherents is increasing and the risk of complete misinformation of society is high. **SIR** models offer vaccination for susceptible people to prevent epidemic growth. For the model (1), (2) if there is an inverse inequality in (3) then the epidemic is prevented.

The solution of the problem. In order to prevent complete disinformation of society in the **RAI** model, one should introduce control parameters, for which it is necessary to supplement model (1), (2) with new parameters. We will assume that in society a certain source disseminates false information in volume $F(t)$ at any given time t . Similarly, at every moment in time t , the opposite false information in volume $N(t)$ is distributed in society. In fact, with the help of $N(t)$ there is a disavowal of false information $F(t)$.

The flows of information $F(t)$ are $N(t)$ aimed at transferring members of the RG to the GA and GI, respectively, while the flow of information $N(t)$ is also aimed at the transfer of members of the GA to the GI. Thus, in the new **RAI** model, the spread of false information will occur not only through interpersonal contacts of RG and GA group members, but also through the impact of the flow of false information $F(t)$ on RG. On the other hand, the disavowal of false information will occur through the influence of the information flow $N(t)$ on RG and GA, and also through interpersonal contacts between RG and GA with GI. Note, that $N(t) \geq 0$, $F(t) \geq 0$ are distributed using IT. When compiling a new **RAI** model, we used the ideas of constructing the **Samarskiy-Mikhailov** model [5]. Let us say, that the reduction rate of risk group members depends on $\lambda N(t)G(t)$, which means the impact of the flow $N(t)$ on the Risk Group with λ coefficient. Similarly, the reduction rate of risk group members also depends on $\kappa F(t)G(t)$, which means the impact of the flow $F(t)$ on the Risk Group with κ coefficient. The reduction rate of risk group members also depends on interpersonal contacts with groups of adherents and immunity and are accordingly equal to - $\alpha G(t)A(t)$, $\beta_1 G(t)I(t)$. Where α , β_1 are the effectiveness coefficients of interpersonal

contacts of the marked groups. Similarly, the rate of change in the number of other groups can be described. Thus, the new mathematical model has the following form:

$$\begin{cases} \frac{dG(t)}{dt} = -\lambda N(t)G(t) - \kappa F(t)G(t) - \alpha G(t)A(t) - \beta_1 G(t)I(t), \\ \frac{dA(t)}{dt} = \alpha G(t)A(t) + \kappa F(t)G(t) + \lambda_1 N(t)G(t) - \gamma A(t) - \beta_2 A(t)I(t), \\ \frac{dI(t)}{dt} = \gamma A(t) + \beta_1 G(t)I(t) + \beta_2 A(t)I(t) + \lambda_2 N(t)G(t), \\ \frac{dN(t)}{dt} = \omega_1 A(t) \left(1 - \frac{N(t)}{M_1}\right), \\ \frac{dF(t)}{dt} = \omega_2 S(t) \left(1 - \frac{F(t)}{M_2}\right). \end{cases} \quad (4)$$

In system (4) all coefficients are positive, $\lambda = \lambda_1 + \lambda_2$, M_1 and M_2 mean the levels of those Internet Technologies with the help of which information flows, respectively, are distributed. Thus, a combined mathematical model is constructed (4), (2) for the dissemination of false information with restrictions on flows and the number of group members. Such combined mathematical models of the Information Warfare were first proposed in [6].

Conclusion. A computational experiment conducted in the MATLAB environment on a computer model, based on the mathematical model (4), (2), makes it possible to conclude that by selecting the value of the control parameters ω_1 and M_1 it is possible to select such $N(t)$ value in which the disavowing of false information is sufficient to prevent complete or significant misinformation of the society.

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) [YS17_78].

REFERENCES

- [1] T. Chilachava and N. Kereselidze, "Continuous Linear Mathematical Model of Preventive Information Warfare," *Sokhumi State University Proceedings, Mathematics and Computer Sciences* vol. 7, 2009, p. 91-112.
http://sou.edu.ge/files/samecniero%20mushaobis%20koordinacia/ssu_shromebi-VII-2009-saboloo.pdf#page=113.
- [2] T. Chilachava and N. Kereselidze, "Non-Preventive Continuous Linear Mathematical Model of Information Warfare," *Sokhumi State University Proceedings, Mathematics and Computer Sciences* vol. 7, 2009, p. 113-141.
http://sou.edu.ge/files/samecniero%20mushaobis%20koordinacia/ssu_shromebi-VII-2009-saboloo.pdf#page=113.
- [3] EU vs Disinfo, "Disinformation Review," <https://euvsdisinfo.eu/disinfo-review/>. [Accessed Oct. 01, 2019].
- [4] W. O. Kermack and A. G. McKendrick, "Contributions to the mathematical theory of epidemics," *Proc. R. Soc. Lond. A*, 15:700-721, 1927.
- [5] A.A. Samarskiy and A.P. Mikhailov, "Mathematical modeling: Ideas. Models. Examples," *M. Fizmatlit*, In Russian, First edition -1997, second revised edition - 2005 -. p. 320.
- [6] N. Kereselidze, "Combined continuous nonlinear mathematical and computer models of the Information Warfare," *International journal of circuits, systems and signal processing*, Volume 12, 2018, pp. 220-228. <http://www.naun.org/main/NAUN/circuitssystemssignal/2018/a682005-aep.pdf>.

XII МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І АВТОМАТИЗАЦІЯ – 2019

INFORMATION TECHNOLOGIES AND AUTOMATION – 2019

ОДЕСА
17– 18 ЖОВТНЯ, 2019

Збірник включає доповіді учасників XII Міжнародної науково-практичної конференції «Інформаційні технології і автоматизація – 2019»

Редакційна колегія: Котлик С.В., Хобін В.А., Плотніков В.М.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.