Issue №11

Part 1

International periodic scientific journal

ONLINE

www.sworldjournal.com

D.A.Tsenov Academy of Economics - Svishtov (Bulgaria)

Indexed in
INDEXCOPERNICUS
(ICV: 82.07)

SWorld Journal

Issue №11
Part 1
January 2022

Published by:
SWorld & D.A. Tsenov Academy of Economics, Svishtov,Bulgaria

ISSN 2663-5712
DOI: 10.30888/2663-5712

UDC 08
LBC 94

The International Scientific Periodical Journal "SWorldJournal" has gained considerable recognition among domestic and foreign researchers and scholars.

Journal Established in 2018. **P**eriodicity of publication: twice a year

The journal activity is driven by the following objectives:

- Broadcasting young researchers and scholars outcomes to wide scientific audience
- Fostering knowledge exchange in scientific community
- Promotion of the unification in scientific approach
- Creation of basis for innovation and new scientific approaches as well as discoveries in unknown domains

The journal purposefully acquaints the reader with the original research of authors in various fields of science, the best examples of scientific journalism.

Publications of the journal are intended for a wide readership - all those who love science. The materials published in the journal reflect current problems and affect the interests of the entire public.

Each article in the journal includes general information in English.

The journal is registered in the INDEXCOPERNICUS, GoogleScholar.

UDC 08
LBC 94
DOI: 10.30888/2663-5712.2022-11-01

Published by:
SWorld &
D.A. Tsenov Academy of Economics
Svishtov, Bulgaria
e-mail: editor@sworldjournal.com

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-022
DOI: 10.30888/2663-5712.2022-11-01-022

УДК 004.056.53:[004.7:004.032.26]

RESEAECH OF PARAMETERS OF QUALITY OF DEFINITION OF NETWORK ATTACKS OF THE PROBE CATEGORY WITH USE OF THE SELF ORGANIZING MAP

ДОСЛІДЖЕННЯ ПАРАМЕТРІВ ЯКОСТІ ВИЗНАЧЕННЯ МЕРЕЖЕВИХ АТАК КАТЕГОРІЇ PROBE З ВИКОРИСТАННЯМ САМООРГАНІЗУЮЧОЇ КАРТИ

Pakhomova V.M. / Пахомова В.М.
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0002-0022-099X
Pavlenko I.I. / Павленко І.І.
master / магістр
ORCID: 0000-0003-4941-6755
Ukrainian State University of Science and Technology, Dnipro, Lazaryan St., 2, 49010
Український державний університет науки і технологій, Дніпро, вул. Лазаряна, 2, 49010

Анотація. *Для визначення мережевих атак категорії Probe створена в Python програма «SOM_Probe» на основі реалізації самоорганізуючої карти Кохонена 30*30, структура якої 15-5 (де 15 – кількість вхідних параметрів мережевого трафіку, 5 – кількість результуючих нейронів), та з використанням відкритої бази KDDCup. Визначені параметри якості (Precision, Recall, F-мірка) виявлення наступних класів атак: Portsweep, Ipsweep, Satan, Nmap, а також проведені дослідження F-мірки за різною кількістю епох навчання нейронної мережі.*

Ключові слова: категорія, *Probe,* ***клас, атака,*** *SOM,* ***точність, повнота,*** *F-мірка.*

Вступ

Постановка проблеми. Створення ефективної системи виявлення мережевих атак вимагає застосування якісно нових підходів до обробки інформації, які повинні ґрунтуватися на адаптивних алгоритмах здатних до самонавчання. Найбільш перспективним напрямком у створенні подібних систем виявлення мережевих атак є застосування нейромережної технології.

Аналіз останніх досліджень. Відомо, що для виявлення мережевих атак можливе використання наступних нейронних мереж (НМ): багатошарового персептрону (Multi Layer Perceptron, MLP); мережі Кохонена або самоорганізуючої карти (Self Organizing Map, SOM); радіально-базисної мережі (Radial Basis Function Network, RBF), серед яких для кластеризації набільш підходить SOM [3]. Так, наприклад, Palomo A. та Esteban J. провели дослідження, використовуючи зростаючу ієрархічну самоорганізуючу карту при використані бази KDD99. У результаті визначено майже максимальний рівень виявлення атаки, що складає 99,99 %, але при цьому є суттєвий недолік, який полягає в великій ймовірності помилки 5,44 % в зрівняні з іншими НМ. Ortis Andres також проводила дослідження із зростаючою ієрархічною самоорганізуючою картою. У результаті створена НМ з підвищенням швидкості виявлення атак, яка при навчанні використовувала метод маркування ймовірностей. Для даної НМ використовувалася база NSL-KDD, досягнуто найвищу частоту виявлення атак 99,68 % з найменшим помилковим спрацьовуванням 0,02 %. У [1] доведено, що якість класифікації залежить від кількості еталонів окремих класів (Dos, Probe, U2R, R2L) у навчальній вибірці.

Дана робота виконана відповідно до НДР [2]. ***Метою статті*** є дослідження параметрів якості визначення мережевих класів атак категорії Probe з використанням самоорганізуючої карти.

1. Постановка задачі та вибір методу

Атаки Probe полягають в скануванні мережевих портів з метою отримання конфіденційної інформації. Відомі наступні класи мережевих атак відповідно до категорії Probe: Portsweep, Ipsweep, Satan, Nmap. У якості початкових даних використана відкрита база даних KDDCup [5]. У якості математичного засобу взята самоорганізуюча карта Кохонена, що навчається без вчителя. Структура SOM має єдиний шар нейронів (шар Кохонена) без коефіцієнтів зсуву та показана на рис. 1.

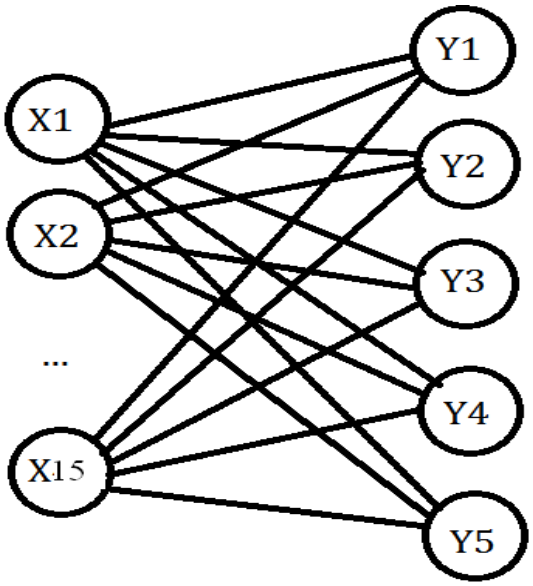

Рисунок 1 – Структура самоорганізуючої карти Кохонена

У якості вхідних змінних НМ параметри мережевого трафіку x1…x15, де x1 – Protocol type; x2 – Service; x3 – Flag; x4 – Source bytes; x5 – Destination bytes; x6 – Hot; x7 – Logged in; x8 – Count compromised; x9 – Serror rate; x10 – Rerror rate; x11 – Same srv rate; x12 – Diff srv rate; x13 – Srv Serror rate; x14 – Srv Rerror rate; x15 – Srv diff host rate. У якості результуючих нейронів y1…y5, де y1 відповідає Portsweep, y2 – Ipsweep, y3 – Satan, y4 – Nmap, y5 – атаки не було.

Ми вважаємо, що використання SOM [6] в якості математичного апарату є доцільним і достатнім. Хоча RBF і навчається швидше ніж MLP, але необхідно визначити кількість радіальних елементів, розташовування їх центрів і значення відхилення, модель RBF потребує декілька більшої кількості елементів, тобто буде працювати повільніше і потребує більше пам’яти, ніж модель MLP. Однак, при створенні MLP необхідно провести додаткові дослідження функцій активації нейронів, алгоритмів навчання та довжини вибірки.

За допомогою мови «Python» створена програмна модель «SOM_Probe», в основу якої покладена реалізація самоорганізуючої карти. У якості основного фреймфорку для створення SOM використано MiniSom (мінімалістичну реалізацію самоорганізуючої карти на основі Numpy). Для відображення інформації обрана бібліотека Matplotlib, до складу якої входить модуль

Matplotlib.pyplot який містить в собі функції для графічного відображення інформації. У якості допоміжної бібліотеки обрано Numpy (бібліотеку з відкритим вихідним кодом, яка поєднує в собі багато математичних функцій). Для аналізу даних використаний модуль Metrics від Sklearn, що включає функції оцінки, метрики продуктивності та обчислення відстані.

2. Навчання та тестування нейронної мережі

Для навчання SOM подана вибірка із 400 прикладів, фрагмент якої наведено на рис. 2. Для тестування SOM використано вибірку із 205 прикладів. У результаті роботи програми «SOM_Probe» отримані карти 30*30, які приведені на рис. 3(а, б) при навчанні та тестуванні НМ відповідно. Розподілення атак на картах наступне: «красне кільце» – Portsweep, «зелений квадрат» – Ipsweep, «синій плюс» – Satan, «жовтий крестик» – Nmap.

3. Дослідження параметрів якості визначення мережевих класів атак

На створеній програмі «SOM_Probe» отримані параметри якості виявлення мережевих класів категорії Probe, деякі із яких зведені в табл. 1 (250000 епох). У таблиці збалансована F-мірка – це гармонічне середнє між Precision та Recall.

```
1,6,2,0,0,0,0,0,2,0.00,0.00,1.00,0.02,0.53,0.00,1
1,6,6,0,0,0,0,0,1,0.00,0.00,1.00,1.00,0.00,0.00,2
1,6,6,0,0,0,0,0,1,0.00,0.00,1.00,1.00,0.00,0.00,2
1,6,6,0,0,0,0,0,1,0.00,0.00,1.00,1.00,0.00,0.00,2
1,6,6,0,0,0,0,0,1,0.00,0.00,1.00,1.00,0.00,0.00,2
1,15,6,0,0,0,0,0,1,0.00,0.00,1.00,1.00,0.00,0.00,2
1,6,6,0,0,0,0,0,1,0.00,0.00,1.00,1.00,0.00,0.00,2
1,6,6,0,0,0,0,0,1,0.00,0.00,1.00,1.00,0.00,0.00,2
1,6,6,0,0,0,0,0,1,0.00,0.00,1.00,1.00,0.00,0.00,2
1,6,6,0,0,0,0,0,1,0.00,0.00,1.00,1.00,0.00,0.00,2
1,13,3,0,77,0,1,0,1,0.00,0.00,1.00,1.00,0.00,0.00,2
1,14,3,693375640,0,1,0,0,3,0.79,0.67,0.21,0.05,0.39,0.00,1
1,6,8,0,0,0,0,0,2,0.69,0.50,0.31,0.01,0.38,0.00,1
2,5,1,8,0,0,0,0,10,0.00,0.00,0.00,1.00,0.00,1.00,2
2,5,1,8,0,0,0,0,6,0.00,0.00,0.00,1.00,0.00,1.00,2
2,5,1,8,0,0,0,0,9,0.00,0.00,0.00,1.00,0.00,1.00,2
2,5,1,8,0,0,0,0,37,0.00,0.00,0.00,1.00,0.00,1.00,2
2,5,1,8,0,0,0,0,43,0.00,0.00,0.00,1.00,0.00,1.00,2
2,5,1,8,0,0,0,0,46,0.00,0.00,0.00,1.00,0.00,1.00,2
2,5,1,8,0,0,0,0,49,0.00,0.00,0.00,1.00,0.00,1.00,2
2,5,1,8,0,0,0,0,33,0.00,0.00,0.00,1.00,0.00,1.00,2
2,5,1,8,0,0,0,0,26,0.00,0.00,0.00,1.00,0.00,1.00,2
2,5,1,8,0,0,0,0,4,0.00,0.00,0.00,1.00,0.00,1.00,2
2,5,1,8,0,0,0,0,43,0.00,0.00,0.00,1.00,0.00,1.00,2
1,6,7,0,0,0,0,0,1,1.00,1.00,0.00,1.00,0.00,0.00,4
1,6,7,0,0,0,0,0,1,1.00,1.00,0.00,1.00,0.00,0.00,4
1,6,7,0,0,0,0,0,1,1.00,1.00,0.00,1.00,0.00,0.00,4
1,6,7,0,0,0,0,0,1,1.00,1.00,0.00,1.00,0.00,0.00,4
1,6,7,0,0,0,0,0,1,1.00,1.00,0.00,1.00,0.00,0.00,4
1,6,7,0,0,0,0,0,1,1.00,1.00,0.00,1.00,0.00,0.00,4
1,6,7,0,0,0,0,0,1,1.00,1.00,0.00,1.00,0.00,0.00,4
1,6,7,0,0,0,0,0,1,1.00,1.00,0.00,1.00,0.00,0.00,4
1,6,7,0,0,0,0,0,1,1.00,1.00,0.00,1.00,0.00,0.00,4
```

Рисунок 2 – Фрагмент навчальної вибірки

Таблиця 1 – Параметри якості, що отримані на програмі «SOM_Probe»

Клас атаки	Навчання НМ			Тестування НМ		
	Precision	Recall	F-мірка	Precision	Recall	F-мірка
Portsweep	1,00	0,97	0,98	1,00	0,98	0,99
Ipsweep	0,93	0,99	0,93	0,97	0,97	0,97
Satan	1,00	1,00	1,00	1,00	1,00	1,00
Nmap	0,94	0,74	0,94	0,83	0,91	0,83

Із таблиці видно, що НМ добре визначає типи мережевих атак. Найменшу точність НМ показала при визначенні атак типу Nmap. Тобто НМ добре визначає мережеві атаки типу Portsweep, Ipsweep та Satan, але при визначенні типу Nmap можуть виникати помилки.

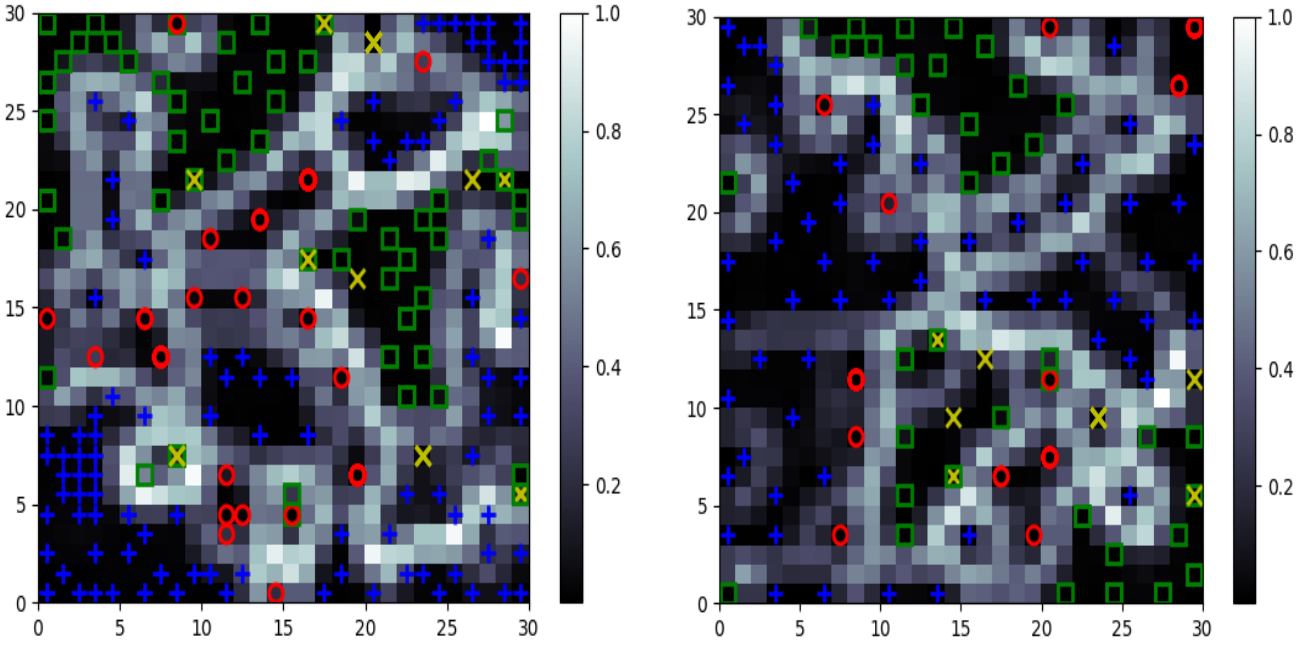

Рисунок 3 – Результат роботи програми «SOM_Probe»: (а) - при навчанні НМ; (б) - при тестуванні НМ

4. Дослідження F-мірки за різною кількістю епох навчання НМ

На створеній програмі «SOM_Probe» проведено дослідження F-мірки за різною кількістю епох навчання НМ (рис. 4), апробація результатів в [4].

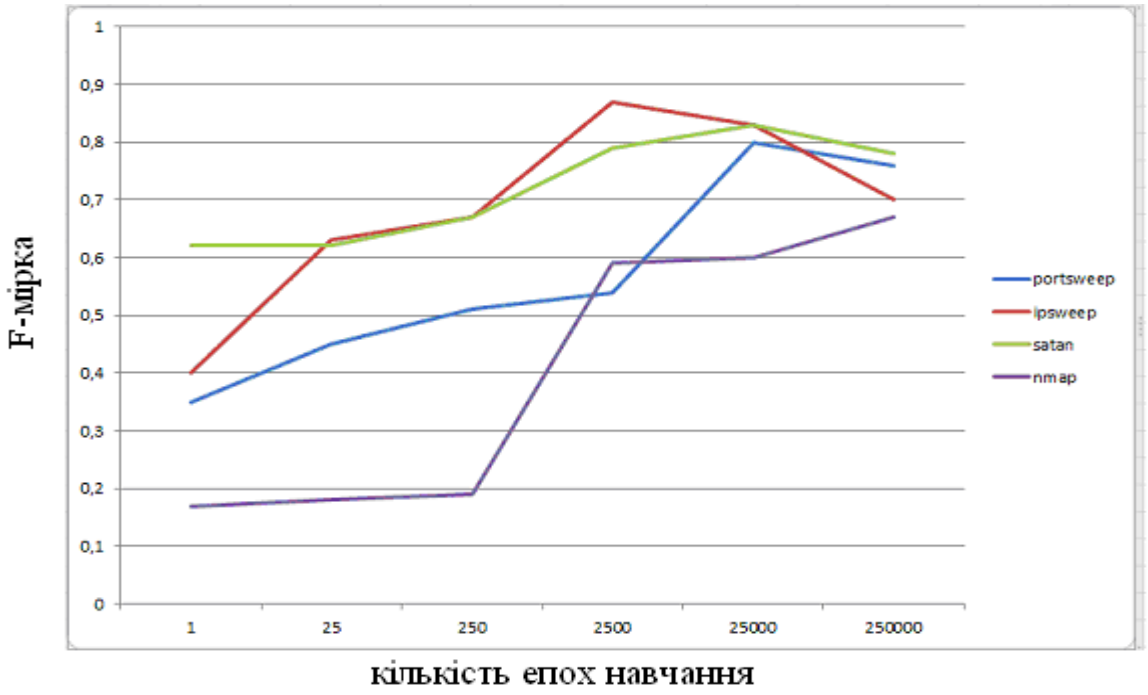

Рисунок 4 – F-мірка за різною кількістю епох навчання

Із рисунку видно, що для всіх типів атак (крім Nmap) F-мірка зростає, досягаючи свого максимуму на відмітці 25000 епох, після чого спостерігається невеликий спад мірки. Але для Nmap спостерігається постійний ріст, максимум якого випадає на 250000 епох. Незначний ріст значення F-мірки для Nmap та встановлення кількості епох навчання на 250000 буде означати втрати на визначені інших типів атак і зниження загальної точності.

Висновки

На основі створеної в Python програми «SOM_Probe» з використанням самоорганізуючої карти Кохонена та бази даних KDDCup проведено дослідження параметрів якості визначення мережевих класів атак категорії Probe. НМ добре визначає мережеві атаки типів: Portsweep; Ipsweep; Satan, але при визначенні типу Nmap можуть виникати помилки. Крім того, проведено дослідження F-мірки за різною кількістю епох навчання з використанням програми «SOM_Probe»: для всіх типів атак (крім Nmap) F-мірка зростає.

Література:

1. Емельянова Ю.Г., Талалаев А.А., Тищенко И.П., Фраленко В.П. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы. Программные системы: теория и приложения. № 3(7). 2011. С. 3-15.

2. НДР «Дослідження механізмів визначення мережевих атак з використанням методів штучного інтелекту»; наук. кер.: доц. Пахомова В.М. Державний реєстраційний номер: 0121U110676. 2021-2022 р.р.

3. Пахомова В.М., Коннов М.С. Дослідження двох підходів до виявлення мережних атак із використанням нейромережної технології // Наука та прогрес транспорту. 2020. № 3(87). С. 81-93. DOI: 10.15802/stp2020/208233.

4. Пахомова В.М., Павленко І.І. Дослідження на створеній мережі Кохонена виявлення PROBE атак. Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості та освіті: Тези XV Міжнародної науково-практичної конференції (Дніпро, 16-17 грудня 2021 р.): УДУНТ, 2021. С. 198.

5. KDDCup1999Data.URL:http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

6. Kohonen T. The self-organizing map. Proceedings of the IEEE. 1990. Vol. 78. No 9. pp.1464-1480.

Abstract. *To determine network attacks of the Probe category, Python created the program "SOM_Probe" based on the implementation of Kohonen Self Organizing Map 30*30, the structure of which is 15-5 (where 15 - the number of network traffic input parameters, 5 - the number of resulting neurons), and using an open database KDDCup. Quality parameters (Precision, Recall, F-measure) of detection of the following classes of attacks are defined: Portsweep, Ipsweep, Satan, Nmap, and also researches of F-measure on various quantity of epochs of training of a neural network are carried out.*

Keywords: *category, Probe, class, attack, SOM, precision, recall, F-measure.*

СОДЕРЖАНИЕ/CONTENTS

Innovative engineering, technology and industry

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-001 3
THERMAL CALCULATION OF CABLE LINES LAID IN POLYMER PIPES
Kyryk V. V., Podoltsev O. D., Rybka O. O.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-007 11
PROGRESSIVE ZINCING ELECTROLYTES
Kryukova E.A., Korobkova M.V.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-016 17
RESEARCH OF DEAERATION AND NUTRITIONAL INSTALLATION OPERATION IN ORDER TO DETERMINE ITS OPTIMAL AND MOST EFFICIENT OPERATING MODE
Hlushchenko O.L., Rudenko K.O.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-027 23
FEATURES OF DESIGN OF BRAND SPECIAL CLOTHES
Nikulina A.V., Shopina T.P.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-032 30
THE RESEARCH OF MICROBIOLOGICAL INDICATORS OF WORT EXTRACTED FROM SWEET SORGHUM AND APPLE CONCENTRATE AS RAW MATERIALS IN THE PRODUCTION OF SAFE FOODSTUFFS
Karputina M.V., Kharheliia D.D., Teterina S.M., Romanova Z.M., Oliinyk S.I., Vitriak O.P.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-054 35
JUSTIFICATION FOR THE CHOICE OF SANITARY PREPARATION OF PREMISES FOR PRODUCTION TRYPHOPHANE AMINO ACIDS
Hrehirchak N. M., SlobodyanO. P., ShulgaM.O.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-067 41
THE EQUATION OF MOVEMENT OF THEWORCING CONTAINER DURING VIBRO-MAGNETIC-ABRASIVE PROCESS OF SUPER HARD CERAMICS
Burlakov V.I., Burlakova H.Ya.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-070 46
OCCUPATIONAL SAFETY AT THE OPERATION OF BIOGAS INSTALLATIONS AT FOOD INDUSTRY ENTERPRISES
Siryk A.O., Evtushenko O.V., Maltseva A.V..

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-077 52
ORGANIC BREAD WITH TEF FLOUR
Falendysh N.O., Blazhenko M.S., Belinska K.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-080 56
INTENSIFICATION OF WATER TREATMENT TECHNOLOGY BY DISCRETE-PULSE ENERGY INPUT
Dolinskyi A.A., Obodovych O.M., Tselen B.Ya., Sydorenko V.V., Ivanytskyi H.K., Lymar A.Yu., Radchenko N.L.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-087 62
MONITORING OF NITRATE CONTENT IN GROUNDWATER
Baitova S.N., Zhuravska N.E.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-095 68
MANUFACTURE AND MANUFACTURING ORGANIZATION OF SPECIAL PURPOSE CAKE FOR RESTAURANT ESTABLISHMENTS
Pavliuchenko O., Shteyman Z.

Computer science, cybernetics and automatics

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-057 74
INVESTIGATION OF THE INFLUENCE OF THE TIME OF CORRELATION OF ACCIDENTAL INTERFERENCE ON THE EFFICIENCY OF CONSEQUENTIAL INFORMATION RESERVATION
Al-Ammori A.N., Poleva N.M., Palchik O.P., Tumanova I.V., Oliinuk V.L.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-059 79
PIECEWISE LINEAR APPROXIMATION OF THE SINUSOIDAL MOTION OF THE VIBROCALIBRATION COMPLEX CARRIAGE
Kryvoruchko I.P.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-072 85
IMPLEMENTATION OF THE QUANTUM GENETIC ALGORITHM IN THE ENVIRONMENT PYTHON
Skakalina E. V.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-083 94
CONCEPTION OF INFORMATION TECHNOLOGY OF REPRESENTATION OF COMPUTATIONAL PROCESS BY PETRY NET
Komlevaya N.O., Paulin O.N.

Security systems in the modern world

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-022 100
RESEAECH OF PARAMETERS OF QUALITY OF DEFINITION OF NETWORK ATTACKS OF THE PROBE CATEGORY WITH USE OF THE SELF ORGANIZING MAP
Pakhomova V.M., Pavlenko I.I.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-088 105
THE STATE OF ECONOMIC SECURITY FOREIGN ECONOMIC ACTIVITIES OF AGRICULTURAL ENTERPRISES
Korniienko T.O., Vinnytska O. A.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-093 110
THE STATE OF THE REGULATORY BASE FOR THE PREPARATION OF REINTEGRATION PROGRAMS IN THE ASPECT OF ENVIRONMENTAL SAFETY
Marova S.F., Pavlenko O.P.

https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-096 115
WAYS TO IMPRROVE ENVIRONMENTAL BRANDING
Pavlenko O.P., Rozmaryna A.L., Vitenchuk K.O., Chaban S.P.

Scientific publication

International periodic scientific journal

ScientificWorldJournal

Issue №11
Part 1
January 2022

In Bulgarian, Ukrainian, Russian and English

Indexed in
INDEXCOPERNICUS
high impact factor (ICV: 82.07)

Academy of Economics named after D.A. Tsenov
Bulgaria jointly with SWorld

Signed: January 30, 2022

e-mail: editor@sworldjournal.com
site: www.sworldjournal.com

www.sworldjournal.com

Articles published in the author's edition

ISSN 2663-5712

www.sworldjournal.com