



International Science Group

ISG-KONF.COM

X
**INTERNATIONAL SCIENTIFIC
AND PRACTICAL CONFERENCE
"MODERN METHODS OF APPLYING SCIENTIFIC
THEORIES"**

**Lisbon, Portugal
March 14 - 17, 2023**

ISBN 979-8-88896-520-7

DOI 10.46299/ISG.2023.1.10

MODERN METHODS OF APPLYING SCIENTIFIC THEORIES

Proceedings of the X International Scientific and Practical Conference

Lisbon, Portugal
March 14 – 17, 2023

UDC 01.1

The 10th International scientific and practical conference “Modern methods of applying scientific theories” (March 14 – 17, 2023) Lisbon, Portugal. International Science Group. 2023. 481 p.

ISBN – 979-8-88896-520-7

DOI – 10.46299/ISG.2023.1.10

EDITORIAL BOARD

<u>Pluzhnik Elena</u>	Professor of the Department of Criminal Law and Criminology Odessa State University of Internal Affairs Candidate of Law, Associate Professor
<u>Liudmyla Polyvana</u>	Department of Accounting and Auditing Kharkiv National Technical University of Agriculture named after Petr Vasilenko, Ukraine
<u>Mushenyk Iryna</u>	Candidate of Economic Sciences, Associate Professor of Mathematical Disciplines, Informatics and Modeling. Podolsk State Agrarian Technical University
<u>Prudka Liudmyla</u>	Odessa State University of Internal Affairs, Associate Professor of Criminology and Psychology Department
<u>Marchenko Dmytro</u>	PhD, Associate Professor, Lecturer, Deputy Dean on Academic Affairs Faculty of Engineering and Energy
<u>Harchenko Roman</u>	Candidate of Technical Sciences, specialty 05.22.20 - operation and repair of vehicles.
<u>Belei Svitlana</u>	Ph.D., Associate Professor, Department of Economics and Security of Enterprise
<u>Lidiya Parashchuk</u>	PhD in specialty 05.17.11 "Technology of refractory non-metallic materials"
<u>Levon Mariia</u>	Candidate of Medical Sciences, Associate Professor, Scientific direction - morphology of the human digestive system
<u>Hubal Halyna</u> <u>Mykolaivna</u>	Ph.D. in Physical and Mathematical Sciences, Associate Professor

TABLE OF CONTENTS

AGRICULTURAL SCIENCES		
1.	Бутенко А.О., Мащенко О.А., Кузьменко Р.О., Коваленко Є.В. ПЕРЕВАГИ ТЕХНОЛОГІЇ БІОЛОГІЗАЦІЇ ВИРОЩУВАННЯ ГРЕЧКИ В УМОВАХ ПІВНІЧНО-СХІДНОГО ЛІСОСТЕПУ УКРАЇНИ	16
2.	Писаренко С.А. УРОЖАЙНІСТЬ СОНЯШНИКУ ЗАЛЕЖНО ВІД ЗАСТОСУВАННЯ ПОЗАКОРЕНЕВИХ ПІДЖИВЛЕНЬ В УМОВАХ СЕЛА ГЛОДОСИ НОВОУКРАЇНСЬКОГО РАЙОНУ КІРОВОГРАДСЬКОЇ ОБЛАСТІ	20
3.	Трикiна Н.М. ВПЛИВ МІКРОДОБРІВ НА РОБОТУ СИМБІОТИЧНОГО АПАРАТУ РОСЛИН СОЇ В УМОВАХ ЦЕНТРАЛЬНОЇ УКРАЇНИ	28
ARCHITECTURE, CONSTRUCTION		
4.	Арiнушкіна Н.С. СУЧАСНІ МАТЕРІАЛИ ДЛЯ ДОРОЖНЬОЇ РОЗМІТКИ	31
5.	Срібняк Н.М., Галушка С.А., Шевчук Т.Д. ДО ПИТАННЯ ВРАХУВАННЯ ТІЩИНОУТВОРЕННЯ ПРИ РОЗРАХУНКУ ЗАЛІЗОБЕТОННИХ ПЕРЕКРИТТІВ	38
ART HISTORY		
6.	Sharykov D., Orel D., Gorbachevskiy V., Romanova L. FEATURES OF THE SPECIFICS OF THE PROGRAM CIRCUS GENRES IN THE SPECIALTY PERFORMING ARTS AT A HIGHER EDUCATIONAL INSTITUTION	42
7.	Shevchenko L. CURRENT STATUS OF CIRCUS DIRECTION AND ITS ADAPTATION IN THE EDUCATIONAL PROCESS OF A HIGHER EDUCATIONAL INSTITUTION IN THE FIELD OF CULTURE AND ART	46
8.	Радомський М.Т., Радомська А.М. ВІЗУАЛІЗАЦІЯ ТВОРУ МИСТЕЦТВА ЯК ІННОВАЦІЙНА СКЛАДОВА ТВОРЧОГО ПРОЦЕСУ	49

BIOLOGY		
9.	Lykholat T. XENOESTROGEN EFFECT ON PROTEOLYTIC PROCESSES IN BRAIN OF ANIMALS DEPENDING ON AGE	54
CHEMISTRY		
10.	Alabada R. THE DIMENSIONAL DEPENDENCE OF THE THERMODYNAMIC ANGLE OF GROWTH NANOCRYSTALS SEMICONDUCTORS	58
11.	Pozhitkova L., Velichko T., Kaprelyants L. ENZYMATIC BIOCONVERSION OF SOY POLYSSAHARIDES	60
ECONOMY		
12.	Hlushko A., Taranets B. REGULATORY AND LEGAL INSURANCE OF ECONOMIC SECURITY OF BUSINESS IN THE EU	63
13.	Miahkykh I., Dorofieiev D. ADAPTIVE MANAGEMENT OF CHANGES IN THE POTENTIAL OF THE ENTERPRISE IN A CRISIS	66
14.	Udovychenko D., Stanislavyk O., Kovalenko O. CONDITIONS AND FACTORS OF FORMATION OF SALES MECHANISMS OF FOOD GOODS IN THE CONSUMER MARKET	69
15.	Банашко О.О., Кудельський В.Е. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ МАЛИХ ПІДПРИЄМСТВ	73
16.	Гриб Є.С. ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ РИЗИКАМИ АГРАРНИХ ПІДПРИЄМСТВ	77
17.	Ждек В.М. РОЗВИТОК ТА ЗНАЧУЩІСТЬ ЕКОЛОГІЧНОГО СТРАХУВАННЯ	80
18.	Семенча І.Є., Патракова В.В. МЕТОДИ ОЦІНЮВАННЯ ФІНАНСОВИХ РИЗИКІВ ПІДПРИЄМСТВА	84

19.	Хом'як М.Л. НОВІ ТЕНДЕНЦІЇ У ФОРМУВАННІ МІЖНАРОДНОГО ІМІДЖУ УКРАЇНИ В УМОВАХ ГЕОПОЛІТИЧНИХ І ГЕОЕКОНОМІЧНИХ ЗМІН	87
20.	Чистобородова К.І. РОЛЬ ФІНАНСОВОГО КОНТРОЛІНГУ НА ПІДПРИЄМСТВАХ	92
GEOLOGY		
21.	Чернобук О.І., Ішков В.В., Козій Є.С., Пащенко П.С., Дрешпак О.С. ЗВ'ЯЗОК ВМІСТІВ ГЕРМАНІЮ ТА БЕРИЛІЮ У ВУГІЛЬНОМУ ПЛАСТІ С8В ШАХТИ "ДНІПРОВСЬКА"	95
HISTORY		
22.	Галемчук С.М. ЮРІЙ СОЛОМІЙЧУК (1857-1918) - ІДЕЙНИЙ НАТХНЕННИК ТА ОРГАНІЗАТОР ПОЛІТИЧНОГО ТА КУЛЬТУРНО - ПРОСВІТНИЦЬКОГО ЖИТТЯ УКРАЇНЦІВ ГАЛИЦЬКОЇ ГУЦУЛЬЩИНИ КІНЦЯ ХІХ- ПОЧАТКУ ХХ СТОЛІТТЯ	105
23.	Косенко В.С., Цибізов А.Л. УЧАСТЬ ВІЙСЬК У ЛІКВІДАЦІЇ НАСЛІДКІВ АВАРІЇ НА ЧОРНОБИЛЬСЬКІЙ АТОМНІЙ ЕЛЕКТРОСТАНЦІЇ	109
JOURNALISM		
24.	Стецик М.С., Стецик А.В. УНІВЕРСАЛІЗМ АФОРИСТИЧНОГО МОВОМИСЛЕННЯ ЛІНИ КОСТЕНКО (НА МАТЕРІАЛІ РОМАНУ "ЗАПИСКИ УКРАЇНСЬКОГО САМАШЕДШОГО")	113
JURISPRUDENCE		
25.	Salmanov O. ПРЕД'ЯВЛЕННЯ ТРУПА ДЛЯ ВПІЗНАННЯ З УРАХУВАННЯМ РЕАЛІЙ ВОЄННОГО СТАНУ	118
26.	Устюжанінова О.Т., Ворогушина А.О. ПРОБЛЕМИ РЕАЛІЗАЦІЇ ПРИНЦИПУ ДИФЕРЕНЦІАЦІЇ ТА ІНДИВІДУАЛІЗАЦІЇ ВИКОНАННЯ ПОКАРАНЬ	121

MANAGEMENT, MARKETING		
27.	Iastremska O. STRATEGIC ASPECT OF THE USE OF VIRTUAL BRANDS IN THE CONDITIONS OF THE EXPERIENCE ECONOMY	124
28.	Pantilieiev V., Danko Y. MODERN METHODS OF ASSESSING COMPETITIVENESS IN UKRAINE	134
29.	Василенко С.В., Нагорний В.Я. ПОКРАЩЕННЯ РІВНЯ ПРИБУТКОВОСТІ ТА ФІНАНСОВОГО СТАНУ СІЛЬСЬКОГОСПОДАРСЬКОГО ПІДПРИЄМСТВА	137
30.	Власюк Є.О. СОЦІАЛЬНІ-ПСИХОЛОГІЧНІ МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КОМУНІКАЦІЙ В ОРГАНІЗАЦІЇ	140
31.	Волківська А., Осовська Г., Серт І., Соляр В. КАДРОВИЙ МЕНЕДЖМЕНТ НА ПІДПРИЄМСТВІ ТА ОЦІНКА ЙОГО ЕФЕКТИВНОСТІ	143
32.	Летюка В.М. ДЕРЖАВНЕ РЕГУЛЮВАННЯ ТУРИЗМУ В УКРАЇНІ	154
33.	Соколов М.О., Василенко С.В. МЕТОДИЧНІ ОСНОВИ ПРОЦЕСУ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ НА ПІДПРИЄМСТВІ	157
34.	Соколов М.О., Василенко С.В. УПРАВЛІННЯ РЕЗЕРВАМИ ПОКРАЩЕННЯ ПРИБУТКОВОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА	159
35.	Чупайленко О., Козлов А., Колесник Ю. ВИКОРИСТАННЯ МИТНОГО КОНТРОЛІНГУ В УПРАВЛІННІ МИТНИМИ ОРГАНАМИ	161
MEDICINE		
36.	Geldiyeva S.A., Nurnepesov B.S. TREATMENT OF BILIARY DYSKINESIA BY MEANS OF ELECTROTYPE-MUD THERAPY AND DRINKING OF HYDROGEN SULFIDE MINERAL WATER	167

37.	Kovalyova O., Shapkin V., Obykhvyst O. IMPLEMENTATION OF THE BIOETHICS PRINCIPLES IN PALLIATIVE MEDICINE	169
38.	Meibaliev M.T., Korenyako L.B. 100 YEARS SINCE THE BIRTH OF HEYDAR ALIYEV	172
39.	Slonetskyi B., Verbitskiy I., Kotsiubenko V.O. ОЦІНКА ДИНАМІЧНИХ ЗМІН ГРИЖОВОЇ ВОДИ В ЗАЛЕЖНОСТІ ВІД ТРИВАЛОСТІ ЗАЦЕМЛЕННЯ ДІЛЯНКИ ТОНКОЇ КИШКИ ПРИ ЗАЦЕМЛЕНИХ ГРИЖАХ ЖИВОТА	175
40.	Yarova S., Novikova K., Novykova O. ОСОБЛИВОСТІ ПРОФІЛАКТИКИ ПІДВИЩЕНОГО РІВНЯ БЛЮВОТНОГО РЕФЛЕКСУ ПРИ ПРОВЕДЕННІ СТОМАТОЛОГІЧНИХ МАНІПУЛЯЦІЙ	179
41.	Алиєва С.В., Пустова Н. ДОСЛІДЖЕННЯ РОЗВИТКУ АЛЕРГІЧНОГО РИНИТУ ТА АБО БРОНХІАЛЬНОЇ АСТМИ У ДІТЕЙ ХВОРИХ НА АТОПІЧНИЙ ДЕРМАТИТ	183
42.	Біловол А.М., Собко О.А. ОСОБЛИВОСТІ МІКРОФЛОРИ ШКІРИ У ХВОРИХ З АТОПІЧНИМ ДЕРМАТИТОМ	185
43.	Біловол А.М., Пустова Н.О., Гиль М.К. ПРОБЛЕМА ДЕЗІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ ЩОДО ДОГЛЯДУ ЗА ШКІРОЮ	187
44.	Геник Н.І., Бігун Р.В., Жукуляк О.М., Перхулин О.М., Поліщук І.П. ЛОКАЛЬНИЙ ІМУНОЛОГІЧНИЙ СТАТУС У ПАЦІЄНТОК З ЕНДОМЕТРІОМАМИ НА ФОНІ ХРОНІЧНИХ ЗАПАЛЬНИХ ЗАХВОРЮВАНЬ ОРГАНІВ МАЛОГО ТАЗУ	190
45.	Данилюк І.О., Пустова Н.О. МЕЗОТЕРАПІЯ В ЕСТЕТИЧНІЙ МЕДИЦИНІ	192

46.	Кіюн І.Д. ДИНАМІКА ПОКАЗНИКІВ БІОХІМІЧНИХ МАРКЕРІВ ЗАПАЛЕННЯ РОТОВОЇ РІДИНИ ТА ІМУНОЛОГІЧНИХ ПАРАМЕТРІВ ЕНДОТЕЛІАЛЬНОЇ ДИСФУНКЦІЇ КРОВІ ПІСЛЯ ПРОВЕДЕННЯ ЛІКУВАННЯ У ХВОРИХ З ПОЧАТКОВИМИ ФОРМАМИ ГЕНЕРАЛІЗОВАНОГО ПАРОДОНТИТУ, ЩО ПАЛЯТЬ Е-СИГАРЕТИ	198
47.	Лопушанський О.М., Шевченко А.В., Сурсаєва Л.М., Пашкова Ю.П. РОЛЬ КИШКОВОЇ МІКРОБІОТИ В РОЗВИТКУ ПОРУШЕНЬ ПУРИНОВОГО ОБМІНУ	202
48.	Римша С.В., Лук'янович І.Л., Король В.А., Давидюк В.О. ВЗАЄМОВПЛИВ КОГНІТИВНИХ ТА ЕМОЦІЙНИХ ПОРУШЕНЬ У ХВОРИХ РІЗНИХ ВІКОВИХ ГРУП, ЩО ЗВЕРНУЛИСЬ ЗА МЕДИЧНОЮ ДОПОМОГОЮ ЧЕРЕЗ ЗНИЖЕННЯ ІНТЕЛЕКТУ	207
49.	Студена О.О., Ясніковська С.М. ЛІКУВАННЯ ПОЗАМАТКОВОЇ ВАГІТНОСТІ КОМБІНАЦІЄЮ ПРЕПАРАТІВ МЕТОТРЕКСАТУ ТА ГЕФІТІНІБУ	213
50.	Сухін Ю.В., Топор В.П., Павличко Ю.Ю., Корнієнко С.В., Вадатурський М.М. БІОЕЛЕКТРИЧНА АКТИВНІСТЬ ДОВГОГО ДОЛОННОГО М'ЯЗУ ПРИ ХВОРОБІ ДЮПЮІТРЕНА	217
51.	Чиняков В.Ю., Бусилков С.А., Русначенко Т.В., Корж А.В., Видиборець С.В. ПОКАЗНИКИ ПЕРИФЕРИЧНОЇ КРОВІ ТА ОБМІНУ ЗАЛІЗА У ПЕРВИННИХ ДОНОРІВ КРОВІ: ЗНАЧЕННЯ, ІНТЕРПРЕТАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ	219
52.	Човганюк О.С., Скрипник Н.В., Костіцька І.О., Чернявська І.В., Василечко М.М. ЦИТОКІНОВИЙ ПРОФІЛЬ У ХВОРИХ НА АРТЕРІАЛЬНУ ГІПЕРТЕНЗІЮ ЗАЛЕЖНО ВІД СТУПЕНЯ ІНСУЛІНОРЕЗИСТЕНТНОСТІ	225
53.	Шевченко О.О., Левон М.М., Назар П.С., Левон В.Ф. УЛЬТРАСТРУКТУРНІ ОСОБЛИВОСТІ БУДОВИ МІКРОСУДИН ТИПУ ПРОТОКАПЛЯРІВ В ПЕРЕДЦИРКУЛЯЦІЙНУ ФАЗУ РОЗВИТКУ СИСТЕМИ МІКРОЦИРКУЛЯЦІЇ НА РАННІХ СТАДІЯХ ПРЕНАТАЛЬНОГО ОНТОГЕНЕЗУ ЛЮДИНИ	228

54.	Шерстюк С.О., Гафт К.Л., Наконечна С.А., Іваненко М.О., Зубова Є.О. ІНТЕГРАЦІЯ У ВИКЛАДАННІ БАЗОВИХ ДИСЦИПЛІН ЯК ОДИН ІЗ ШЛЯХІВ ОПТИМІЗАЦІЇ НАВЧАЛЬНОЇ ДІЯЛЬНОСТІ СТУДЕНТІВ МЕДИЧНИХ ВНЗ.	231
PEDAGOGY		
55.	Boumous M. THE EFFECTIVENESS OF INCORPORATING TASK-BASED APPROACH IN LITERATURE CLASSES	235
56.	Nikolaeva S. ELECTRONIC PRESENTATIONS ON METHODS OF TEACHING FOREIGN LANGUAGES AND CULTURES: YOUNG SCIENTISTS' DIFFICULTIES	237
57.	Salmanov V.K. AZƏRBAYCAN SİLAHLI QÜVVƏLƏRİNİN II QARABAĞ MÜHARİBƏSİNDƏ GÖSTƏRDİKLƏRİ QƏHRƏMANLIQ SALNAMƏSİ	241
58.	Бабакова Л.М. ПРИНЦИПИ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ ТА ІНСТРУМЕНТИ ЇХ ПРАКТИЧНОГО ВПРОВАДЖЕННЯ	244
59.	Василенко О. РОЗВИТОК ФУНКЦІОНАЛЬНОЇ ГРАМОТНОСТІ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА	248
60.	Дзвонковська В.В., Земяк М.В., Човганюк О.С., Юрак М.З., Середюк Л.В. ОСОБЛИВОСТІ ДИСТАНЦІЙНОГО НАВЧАННЯ ПРИ ВИКЛАДАННІ МЕДИЧНИХ ДИСЦИПЛІН	252
61.	Калита Н.І., Говдриш М.В. ІНТЕГРОВАНЕ НАВЧАННЯ ЯК РЕСУРС РЕАЛІЗАЦІЇ КОМПЕТЕНТНІСНОГО ПІДХОДУ НА УРОКАХ ЧИТАННЯ	255
62.	Корнева Н.М., Богданова О.Н. ВИВЧЕННЯ ЯВИЩА ДИФРАКЦІЇ НА ПРИКЛАДІ ДИФРАКЦІЙНОЇ КАРТИНИ ВІД МЕТАЛЕВОЇ ЛІНІЙКИ	259

63.	Нечитайло Л.Я., Крисак В., Олевич С. ПОПУЛЯРИЗАЦІЯ ПРИНЦИПІВ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ СЕРЕД УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ	262
64.	Нурпейсова С.А., Джумабаева С.Т., Аркабаева С.К., Сағындыков Р.Ш., Укешов Т.Р. СПОРТ ПСИХОЛОГИЯСЫ	265
65.	Олексієнко О. РОЛЬ ЗДОРОВ'ЯЗБЕРЕЖУВАЛЬНИХ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ У СТВОРЕННІПРОСТОРУ ОСВІТИУКРАЇНИ	269
66.	Садова П.О., Суліцький В.В. СОЦІАЛЬНО-ПЕДАГОГІЧНА ПРОФІЛАКТИКА ЖОРСТОКОГО ПОВОДЖЕННЯ З ДІТЬМИ В СІМ'Ї	274
67.	Тимків І.В., Ромаш І.Р., Тимків І.С., Близнюк М.В., Венгрович В.В. ОРГАНІЗАЦІЯ ВИРОБНИЧОЇ ПРАКТИКИ СТУДЕНТА- МЕДИКА	280
68.	Трофімчук Л.О., Семенчук С.С. ОСОБЛИВОСТІ УПРОВАДЖЕННЯ ХМАРНОГО СЕРВІСУ GOOGLE CLASSROOM В ІНФОРМАЦІЙНО-ОСВІТНЄ СЕРЕДОВИЩЕ ОБЛАСНОГО НАУКОВОГО ЛІЦЕЮ М. РІВНЕ	282
69.	Хоменко В. ДЕЦЕНТРАЛІЗАЦІЯ ОСВІТИ У ГРОМАДАХ	287
70.	Чубенко В.А. ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ ГЕЙМІФІКАЦІЇ В ОСВІТНЄ СЕРЕДОВИЩЕ	290
71.	Юе Цзунлянь ФОРМУВАННЯ ЦІННІСНИХ ОРІЄНТАЦІЙ МАЙБУТНІХ ВЧИТЕЛІВ МУЗИЧНОГО МИСТЕЦТВА	294
PHARMACEUTICS		
72.	Syrova G., Chalenko N., Levashova O., Khaustova M., Gaichjuk A. THE STUDYING OF ANALGESIC ACTIVITY OF NEW PHARMACEUTICAL COMPOSITION IN THE EXPERIMENT	297

PHILOLOGY		
73.	Alizade A.U.A.A. THE POWER OF THE WORD IN THE DEPICTION OF THE KNIGHTLY POWER OF RULERS IN THE WORK OF NIZAMI GANJAVI	304
74.	Bikezina A. THE NATIONAL PICTURE OF THE WORLD AND ITS SPECIFICITY	309
75.	Bikezina A. THE RELATIONSHIP OF THE LANGUAGE PICTURE OF THE WORLD AND THE NATIONAL MENTALITY	311
76.	Boshkov A.V. SCIENTIFIC DISCOURSE AS A TYPE OF INSTITUTIONAL DISCOURSE	313
77.	Klochko T. SOME PECULIARITIES OF UKRAINIAN SPEECH ETIQUETTE UNFAMILIAR TO FOREIGN STUDENTS	316
78.	Markovych K. STRATEGIES OF SPEAKING AND THEIR USE AMONG THE BEGINNERS IN ENGLISH LANGUAGE STUDYING	318
79.	Tokpanova A.A. CONTEMPORARY TRENDS IN LANGUAGE	321
80.	Ватченко С.О. "ДИВИСЬ, ЯК ПОРОК І ЧЕСНОТА, ГРИШНЕ ТА ПРАВЕДНЕ ЗМІШАЛИСЬ..." ГЕНРІ ФІЛДІНГ	325
81.	Лихачова А.В. ІНДОЄВРОПЕЙСЬКА МОВНА СПІЛЬНІСТЬ ЯК АРЕАЛЬНИЙ ФЕНОМЕН: ІСТОРІЯ ПИТАННЯ	328
82.	Максютенко О.В. ДОСЛІДНИКИ ПРО ПОЕТИКУ АВТОБІОГРАФІЗМУ В ПРОЗІ ЛОРЕНСА СТЕРНА	333

83.	Нестеренко О.О. СТРУКТУРНІ ОСОБЛИВОСТІ КЛІШЕ КИТАЙСЬКОМОВНОГО НАУКОВОГО ТЕКСТУ	337
84.	Требухова Н.Ю. ЗАПАХОВА ЛЕКСИКА У ТВОРЧОСТІ І. ДРАЧА: СЕМАНТИКО-СТИЛІСТИЧНИЙ АСПЕКТ	340
PHILOSOPHY		
85.	Ужва В.О. ПСИХОЛОГО-РЕАБІЛІТАЦІЙНА ДОПОМОГА ХРИСТІЯНСЬКИХ КОНФЕСІЙ В УМОВАХ РОСІЙСЬКО- УКРАЇНСЬКОЇ ВІЙНИ	344
PHYSICAL AND MATHEMATICAL SCIENCES		
86.	Trofimova L. MODELING THE FEATURES OF THE PROCESSES OF STRUCTURE FORMATION IN BUILDING COMPOSITES	349
87.	Аршава О.О., Заєць І.М. ЗАСТОСУВАННЯ ЧИСЕЛ ФІБОНАЧЧІ В КРИПТОГРАФІЧНИХ АЛГОРИТМАХ	351
POLITICS		
88.	Соломицький О.І., Слюсаренко М.О. УДОСКОНАЛЕНИЙ МЕТОД КОГНІТИВНОГО МОДЕЛЮВАННЯ ВОЄННО-ПОЛІТИЧНОЇ ОБСТАНОВКИ	356
PSYCHOLOGY		
89.	Spytska L. PECULIARITIES OF THE INFLUENCE OF BIOLOGICAL, PSYCHOLOGICAL AND SOCIO-CULTURAL FACTORS ON SEXUAL DESIRE	363
90.	Ахан Қ.О., Касымжанова А.А. БАҚЫТ ТҮСІНІГІ ТУРАЛЫ ШЕТЕЛДІК ЖӘНЕ ОТАНДЫҚ КӨЗҚАРАСТАР ЖҮЙЕСІ	365
91.	Добровольський Ю., Ярмольчик М. ЩОДО ПСИХОЛОГІЧНОГО СУПРОВОДУ ДІЯЛЬНОСТІ ПЕДАГОГІЧНИХ ТА НАУКОВО-ПЕДАГОГІЧНИХ ПРАЦІВНИКІВ В УМОВАХ ВІЙНИ В УКРАЇНІ	372

92.	Мамадалієва Л.В. ТЕОРЕТИЧНІ АСПЕКТИ ЕМОЦІЙНОГО ІНТЕЛЕКТУ УЧНІВСЬКОЇ МОЛОДІ	375
93.	Федик О.В. ЕМОЦІЙНА СТІЙКІСТЬ ЯК ОДНА З ДЕТЕРМІНАНТ ПОДОЛАННЯ СТРЕСУ	379
94.	Чайкіна Н.О. ПСИХОЛОГІЧНІ ОСОБЛИВОСТІ СПРИЙНЯТТЯ РИЗИКУ ЖИТТЄВИХ СИТУАЦІЙ ПІД ЧАС ВІЙСЬКОВИХ ДІЙ В УКРАЇНІ	382
95.	Шевченко Р.П., Котляр Л.І., Бондаревич С.М.С., Дащенко О.І., Антонова К.Ю. ПРОБЛЕМА СТРЕСУ ТА СОЦІАЛЬНОЇ ДЕПРИВАЦІЇ У СПЕЦІАЛІСТІВ МОРЕГОСПОДАРСЬКОЇ ГАЛУЗІ	387
96.	Яворська А.В. ОСОБИСТІСНІ ВЛАСТИВОСТІ СУЧАСНОГО ПСИХОТЕРАПЕВТА	391
SOCIOLOGY		
97.	Глушкова Н.М., Кашнян А.В. ГЕНДЕРНА ПРІОРИТЕТИЗАЦІЯ – ШЛЯХ ДО ЗАБЕЗПЕЧЕННЯ ГЕНДЕРНОЇ РІВНОСТІ В СФЕРІ УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ	394
TECHNICAL SCIENCES		
98.	Abdullayev V., Nariman A. CREATION OF AN INFORMATION SYSTEM FOR THE MANAGEMENT OF THE PERSONNEL DEPARTMENT	398
99.	Andrushchak I., Androshchuk I., Androshchuk O. MODELING METHODS OF DENYED ENCRYPTION WITH A SHARED KEY	403
100.	Antoshchuk S., Breskina A. CLASSIFICATION OF METRICS COMMONLY USED FOR EVALUATING MODELS OF HUMAN DETECTION	408
101.	Asgarova B., Aslanli N. APPLICATION OF BIG DATA TECHNOLOGIES IN EDUCATION	412

102.	Bochvarov M., Manasov S., Manasov I. PRACTICLE EXAMPLE OF MESURING VISUAL ATTENTION USING AN EYE TRACKING BIOSENSOR	416
103.	Dehtiar M. INCREASING THE EFFICIENCY OF WASTEWATER TREATMENT OF THE FOOD INDUSTRY	424
104.	Demchenko K., Piskarov O., Nechitailo J., Panov A., Radchenko S. METHODS OF IMPLEMENTATION OF ARITHMETIC OPERATIONS IN THE RESIDUAL NUMBER SYSTEM	426
105.	Rahimova N., Aliyev A. APPLICATION OF BIG DATA TECHNOLOGIES IN FINANCE AND BANKING INDUSTRY	428
106.	Polyvianchuk A., Zhang Le ANALYSIS OF THE CURRENT STATE AND DEVELOPMENT PROSPECTS OF URBAN CENTRAL HEATING IN CHINA	433
107.	Vardanian A., Haranina O., Red`ko Y., Romaniuk Y. THE INFLUENCE OF AN INTENSIFIER WITH ANTI- BACTERIAL EFFECT ON THE COLORING OF COTTON- POLYESTER TEXTILE MATERIALS	437
108.	Voytenko O., Strogonov D., Ilyashenko Y., Skachkov I., Ganushchak O. EQUIPMENT FOR THE AUTOMATIC QUALITY MONITORING SYSTEM OF PLASMA-ARC WELDING AND RELATED PROCESSES	440
109.	Zenkin M., Barabash V. THE METHOD OF OPTIMIZING THE PARAMETERS OF THE MECHANICAL DRIVE SYSTEM OF ROLL-TYPE PRINTING MACHINES	446
110.	Zhiguts Y., Lazar V. FEATURES OF CALCULATING THE RELIABILITY AND STRENGTH OF PRE-TENSIONED STRUCTURES	451
111.	Білюк І.С., Савченко О.В., Оружак І.В., Гудима І.П., Корзун Б.М. СПОСІБ МОДЕРНІЗАЦІЇ ТОКАРНО-РЕВОЛЬВЕРНОГО НАПІВ АВТОМАТА	453

112.	Каланча А.А. РОЗРОБКА СИСТЕМИ ЗАХИСТУ ВІД SQL-ІН'ЄКЦІЙ З ВИКОРИСТАННЯМ РОЗДІЛЕНОГО РЕЄСТРУ	457
113.	Кириченко О.С. ТЕРМОЕЛЕКТРИЧНІ МОДУЛІ З РІЗНИМ ТИПОМ КОМУТАЦІЙНОГО З'ЄДНАННЯ НАПІВПРОВІДНИКОВИХ ТЕРМОПАР	459
114.	Ковальова О.С., Почтар В.О. ОСОБЛИВОСТІ ЗНЕЗАРАЖЕННЯ МІКРОЗЕЛЕНІ РУКОЛИ	463
115.	Коменда Н.В., Коменда Т.І. ВИКОРИСТАННЯ МОРФОМЕТРИЧНИХ ПАРАМЕТРІВ ДЛЯ ХАРАКТЕРИСТИКИ НЕРІВНОМІРНОСТІ ГРАФІКА ЕЛЕКТРИЧНОГО НАВАНТАЖЕННЯ	467
116.	Крайнюк О.В., Буц Ю.В., Богатов О.І., Барбашин В.В. ЦИФРОВА ТРАНСФОРМАЦІЯ СИСТЕМИ УПРАВЛІННЯ ОХОРОНОЮ ПРАЦІ: МОЖЛИВОСТІ ТА ПРОТИРІЧЧЯ	470
117.	Матківський С.В. ПЕРСПЕКТИВИ ПІДВИЩЕННЯ КОЕФІЦІЄНТІВ ВИЛУЧЕННЯ КОНДЕНСАТУ З ВИКОРИСТАННЯМ СУХОГО ГАЗУ	475

TECHNICAL SCIENCES
MODERN METHODS OF APPLYING SCIENTIFIC THEORIES

MODELING METHODS OF DENYED ENCRYPTION WITH A SHARED KEY

Andrushchak Igor,

Doctor of Technical Sciences, Professor

Androshchuk Igor,

Candidate of Agricultural Sciences, Associate Professor
Lutsk National Technical University

Androshchuk Olena,

Head of the obstetrics-pharmaceutical department
Volyn Medical Institute
Lutsk, Ukraine

Criteria for the construction of deniable encryption algorithms for the implementation of information protection mechanisms such as deceptive traps are proposed, and the developed algorithms of this type are presented. The new implemented requirements are indistinguishability from probabilistic encryption and the identity of the decryption procedure and the use of all bits of the cryptogram for all possible key values. The proposed deniable encryption methods provide high performance and are promising for expanding the arsenal of cryptographic information protection mechanisms used in complex computer security systems.

Keywords: block ciphers, computer security, cryptography, deniable encryption, hash functions, probabilistic encryption, cryptogram.

.....

The concept of deniable encryption (DE) is associated with the problem of ensuring the strength of information encryption in the face of the possibility of so-called duress attacks. These types of attacks imply that the attacker of such resources has an impact on the sender and (or) recipient of messages that force the sender and (or) recipient to reveal the parameters of the encryption process (coercive attack on the message sender) or decryption (coercive attack on the message recipient), for example, the encryption key and random values used in the encryption process.

If it is assumed that the attacker can require both encryption and decryption parameters to be provided, then a two-way coercive attack takes place. Resistance to such attacks is provided by DE algorithms and protocols in that the output ciphertext (cryptogram) can be obtained from various meaningful source messages and (or) various decrypted meaningful texts can be obtained from the cryptogram. The attacker is given encryption parameters that associate the cryptogram with some fictitious meaningful text. The attacker checks that the use of the encryption parameters provided to him actually leads to the conversion of the bogus message into the given cryptogram and (or) to the decryption of the latter into the bogus message. If the check result is

positive and the attacker cannot prove the incompleteness of the disclosed text, then the DE algorithm (protocol) is considered secure [1].

In the known literature, the main attention of researchers is directed to DE methods related to public-key cryptoschemes. Such methods are based on the use of open encryption algorithms or public key distribution protocols. It is assumed that the sender and recipient do not have common secret information (shared secret key), and the recovery of a fictitious/real message depends on the random values used.

Interest in DE algorithms and protocols is associated with the prospects for their application in secure distributed computing and secret electronic voting systems. One of the limitations of the practical use of DE procedures is their low performance, which is especially characteristic of public key crypto schemes. The search for new DE algorithms and protocols has led to the development of more efficient DE methods, but practice requires further increase in the speed of crypto algorithms, especially in cases where DE methods are used as a special information protection mechanism in complex computer security tools based on deceptive traps.

Unlike DE schemes based on asymmetric encryption algorithms, DE based on shared key schemes implies the presence of a shared secret (shared secret key) that allows both the sender and the recipient to recover the real message. In this paper, we solve the problem of developing efficient deniable encryption algorithms while providing high resistance to a two-way duress attack based on DE with a shared secret. The combination of performance and durability removes significant restrictions on the practical application of DE algorithms for protecting information in information security tools. At the same time, special requirements are formulated for DE algorithms related to the use of DE to implement protection mechanisms such as deceptive traps. The proposed new requirements are not satisfied by the shared secret DE algorithms known in the literature [2].

The implementation of information protection mechanisms such as deceptive traps is based on the use of DE methods that provide the possibility of sufficiently fast joint encryption of two or more different messages on two or more different keys of a finite length. One of the messages is fictitious and is encrypted with a fictitious secret key, to which controlled access is organized by the intruder.

When decrypting a properly composed fictitious message, the offender is misled (misinformed). However, it should be assumed that the adversary knows the decryption algorithm used by the authorized user and can analyze the cryptogram and its application when performing the decryption procedure against the dummy key. This should not give him reasonable suspicions that, in addition to the fictitious key he received, there is also another key that decrypts the cryptogram into another meaningful message (fig.1)

In other words, the DE algorithm must have properties that will not allow an attacker to distinguish DE from probabilistic encryption based on the cryptogram, the dummy message, and the dummy key.

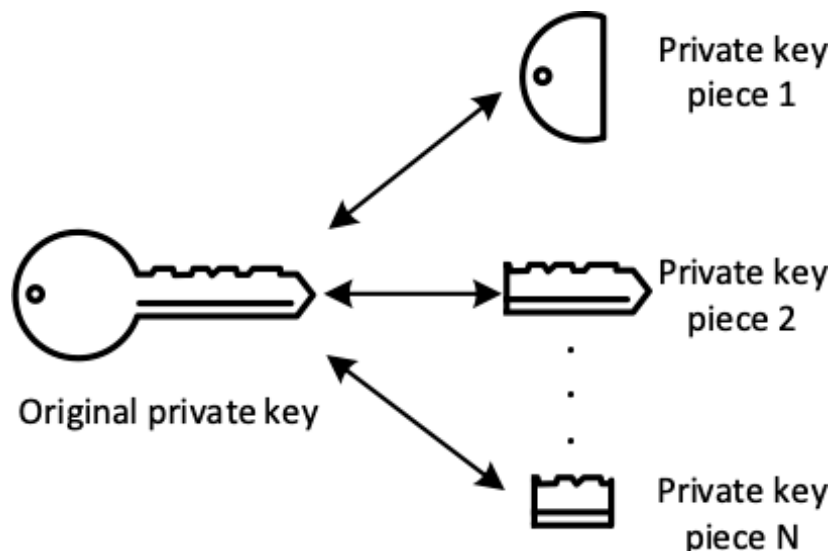


Figure.1 – Key Shards

This defines the following requirements for DE algorithms:

- 1) indistinguishability by cryptogram from probabilistic encryption;
- 2) the same decryption procedures for the various keys used;
- 3) equality (identity of use) of all bits of the cryptogram for all possible values of the decryption key.

These requirements are superimposed on the requirement to use keys of a finite size and provide a sufficiently high performance [3].

They are actually a continuation of the Kerckhoff principle formulated for symmetric encryption algorithms: the cipher must be strong, provided that all the details of the encryption procedure are known to the attacker. For DE algorithms, it is reasonable to supplement this principle with the requirements of computational indistinguishability from a probabilistic encryption algorithm with a known decryption procedure and a known cryptogram.

The meaning of this extension of the Kerckhoff principle is that the attacker cannot reasonably assert (suspect) that the cryptogram contains some other message than the message received using the decryption key he has. Of the three requirements for DE algorithms formulated earlier, the second and third are auxiliary. However, non-compliance with these requirements serves as a source of assumptions that, in addition to a fictitious message, the cryptogram contains other information. The formulated requirements are met if it is possible to specify a probabilistic encryption algorithm that converts a fictitious message using a fictitious key into a cryptogram obtained using the DE algorithm. In this case, the decryption algorithm is specified by some mathematical formula, in which the cryptogram and the decryption key are included as transformation parameters (fig.2).

The DE method based on the use of hash functions or block transformations and described in the section "Deniable encryption method using block transformations" satisfies the three requirements for DE algorithms stated in the "Requirements for shared secret deniable encryption algorithms" section. This is directly evident from the description of the algorithms implemented on the basis of this method.

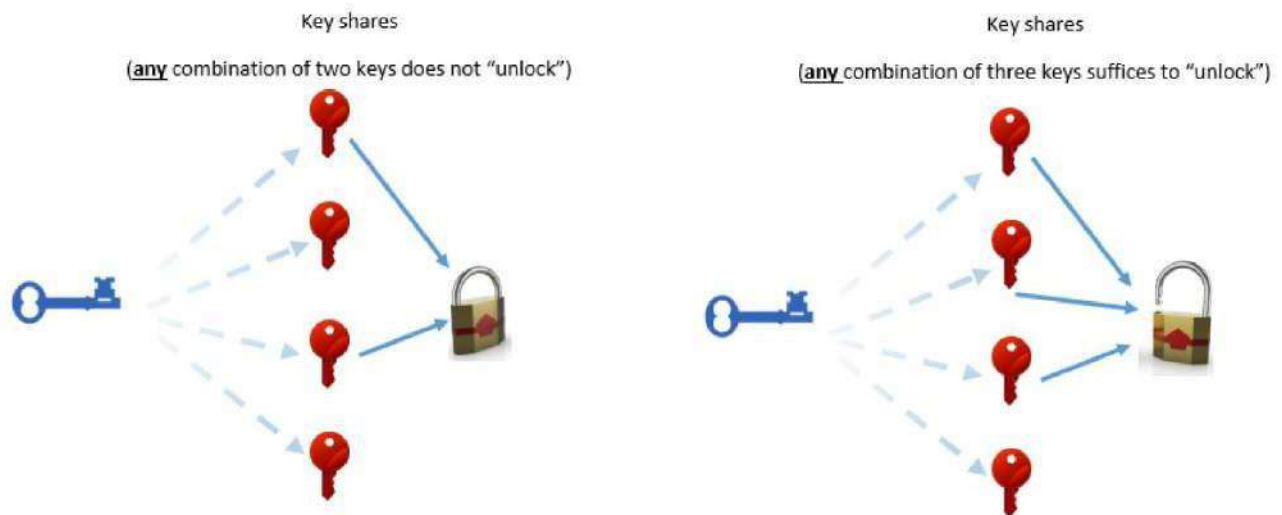


Figure.2 – Secret sharing: “Splitting” the key into several shares

The DE algorithms described in the previous section clearly satisfy the second and third requirements. Let us show that they also satisfy the requirement of being indistinguishable from probabilistic encryption. To do this, we specify a probabilistic encryption algorithm that, using a fictitious key, converts a fictitious message into a cryptogram. This algorithm will be called the associated probabilistic encryption algorithm [4].

Next, we consider the use of DE algorithms with a shared secret key as an information protection mechanism and formulate requirements for algorithms of this type, focused on use in protection mechanisms that allow the implementation of deceptive traps. This information protection mechanism is new for use in complex information and computer security systems. The developed methods and specific DE algorithms that meet the stated requirements are described. One of the formulated requirements is the indistinguishability of the cryptogram obtained using the DE procedure from the cryptogram obtained using the probabilistic encryption procedure.

The compliance of the developed algorithms with this requirement is justified by indicating the associated probabilistic cipher, for which the decryption procedure coincides with the procedure for decrypting a fictitious message using a fictitious key. The given associated probabilistic ciphers are interesting in that in the process of decrypting the cryptogram, the random values used in the encryption procedure are not uniquely restored, while for the known probabilistic block ciphers, the used random values are uniquely restored in the decryption process. This determines an independent interest in the considered probabilistic encryption algorithms. Also, an independent research task is the development of sufficiently fast DE algorithms with commutative properties [5].

Our preliminary results testify in favor of the possibility of solving the latter problem using the cryptogram generation mechanism based on the solution of the system of comparisons proposed in this paper. The considered algorithms refer to the case of simultaneous encryption of two messages, but they are easily extended to the case of simultaneous encryption of three or more messages.

References:

1. Bo Meng. A Secure Internet Voting Protocol Based on Noninteractive Deniable Authentication Protocol and Proof Protocol that Two Ciphertexts are Encryption of the Same Plaintext // J. of Networks. 2009. Vol. 4. N 5. P. 370–377.
2. Berezin A.N. Method of deniable encryption / A.N. Berezin, A.R. Birichevsky, N.A. Moldovyan, A.V. Ryzhkov // Issues of information security. 2013. No 2, pp. 18–21.
3. Ibrahim M. H. A Method for Obtaining Deniable Public-Key Encryption // Intern. J. of Network security. 2009 Vol. 8. No. 1. P. 1-9.
4. Martseniuk V. Competency-based challenges of applied artificial intelligence: project FAAI. / V.Marcenyuk, G.Dimitrov, D. Rancic, I.Luptakova, S. Tomovic, M.Bernas, A. Klos-Witkowska, T.Gancarczyk, A.Sverstiuk, I.Andrushchak // Abstracts of XXXVII International conference Problems of decision making under uncertainties «PDMU-2022». – Sheki-Lankaran, Azerbaijan, 23-25 November 2022. – P. 79-80.
5. Moldovyan A. A., Moldovyan N. A., Guts N. D., Izotov B. V. Cryptography: high-speed ciphers. - St. Petersburg: BHV-Petersburg, 2002. - 495 p.

TECHNICAL SCIENCES
MODERN METHODS OF APPLYING SCIENTIFIC THEORIES

Modern methods of applying scientific theories

Scientific publications

Proceedings of the X International Scientific and Practical Conference

«Modern methods of applying scientific theories»,

Lisbon, Portugal. 481 p.

(March 14 – 17, 2023)

UDC 01.1

ISBN – 979-8-88896-520-7

DOI – 10.46299/ISG.2023.1.10

Text Copyright © 2023 by the International Science Group (isg-konf.com).

Illustrations © 2023 by the International Science Group.

Cover design: International Science Group (isg-konf.com)©

Cover art: International Science Group (isg-konf.com)©

All rights reserved. Printed in the United States of America.

No part of this publication may be reproduced, distributed, or transmitted, in any form or by any means, or stored in a data base or retrieval system, without the prior written permission of the publisher.

The content and reliability of the articles are the responsibility of the authors. When using and borrowing materials reference to the publication is required. Collection of scientific articles published is the scientific and practical publication, which contains scientific articles of students, graduate students, Candidates and Doctors of Sciences, research workers and practitioners from Europe, Ukraine and from neighboring countries and beyond. The articles contain the study, reflecting the processes and changes in the structure of modern science. The collection of scientific articles is for students, postgraduate students, doctoral candidates, teachers, researchers, practitioners and people interested in the trends of modern science development.

The recommended citation for this publication is: Sharykov D., Orel D., Gorbachevskiy V., Romanova L. Features of the specifics of the program circus genres in the specialty performing arts at a higher educational institution. Proceedings of the X International Scientific and Practical Conference. Lisbon, Portugal. 2023. Pp. 42-45

URL: <https://isg-konf.com/modern-methods-of-applying-scientific-theories/>