



InterConf
Scientific Publishing Center

**May 26-28,
2020**

CHALLENGES IN SCIENCE OF NOWADAYS



**Proceedings of the 4th
International Scientific and
Practical Conference**

WASHINGTON, USA

26-28.05.2020



InterConf
Scientific Publishing Center

CHALLENGES IN SCIENCE OF NOWADAYS

Proceedings of the 4th International Scientific and Practical Conference

WASHINGTON, USA

26-28.05.2020

WASHINGTON
2020

UDC 001.1

C 43 Proceedings of the 4th International Scientific and Practical Conference «Challenges in Science of Nowadays» (May 26-28, 2020). Washington, USA: EnDeavours Publisher, 2020. 381 p.

ISBN 979-1-293-10109-3

EDITOR

Polina Vuitsik 
PhD in Economics
Jagiellonian University, Poland
@ p.vuitsik.prof@gmail.com

COORDINATOR

Mariia Granko 
Coordination Director in Ukraine
Scientific Publishing Center InterConf
@ info@interconf.top

EDITORIAL BOARD

Mark Alexandr Wagner (DSc. in Psychology)
University of Vienna, Austria
@mw6002832@gmail.com;

Dan Goltsman (Doctoral student)
Riga Stradiņš University, Republic of Latvia;

Katherine Richard (DSc in Law),
Hasselt University, Kingdom of Belgium
@katherine.richard@protonmail.com;

Richard Brouillet (LL.B.),
University of Ottawa, Canada;

Stanyslav Novak  (DSc in Engineering)
University of Warsaw, Poland
@ novaks657@gmail.com;

Yasser Rahrovani (PhD in Engineering)
Ivey School of Business, The University of Western
Ontario, Canada;

Elise Bant (LL.D.),
The University of Sydney, Australia;

Anna Svoboda  (Doctoral student)
University of Economics, Czech Republic
@ annasvobodaprague@yahoo.com;

Dr. Alben Yaneva (DSc. in Sociology and Antropology),
Manchester School of Architecture, UK;

Vera Gorak (PhD in Economics)
Karlovarská Krajská Nemocnice, Czech Republic
@ veragorak.assist@gmail.com;

Dmytro Marchenko  (PhD in Engineering)
Mykolayiv National Agrarian University
(MNAU), Ukraine;

Kanako Tanaka (PhD in Engineering),
Japan Science and Technology Agency, Japan;

George McGrown (PhD in Finance)
University of Florida, USA
@ mcgrown.geor@gmail.com;

Alexander Schieler (PhD in Sociology),
Transilvania University of Brasov, Romania

If you have any questions or concerns, please contact a coordinator Mariia Granko.

The recommended citation:

Surname N. Title of article or abstract. *Challenges in Science of Nowadays*: Proceedings of the 4th International Scientific and Practical Conference (May 26-28, 2020), Washington, USA: EnDeavours Publisher, 2020. pp. 21-27. URL: [https://interconf.top/...](https://interconf.top/)

PhD students, teachers, scientists, research workers of higher educational institutions, research institutes and industrial enterprises are invited to participate in the conference. The conference provides an interdisciplinary forum for researchers, practitioners and scholars to present and discuss the most recent innovations and developments in modern science. The aim of conference is to enable academics, researchers, practitioners and college students to publish their research findings, ideas, developments, and innovations.

©2020 EnDeavours Publisher
©2020 Scientific Publishing Center InterConf
©2020 Authors of the abstracts

TABLE OF CONTENTS

BUSINESS ECONOMICS		
Tytarenko S.A.	THE LOGISTICS. NOTION AND BASIC CHARACTERISTICS	9
Маркова Є.Ю. Надточій І.І.	ОЦІНКА ІНВЕСТИЦІЙНОЇ ПРИВАБЛИВОСТІ МОРСЬКИХ ПОРТІВ	15
REGIONAL ECONOMY		
Ахновська І.О.	ЗОВНІШНЄ СЕРЕДОВИЩЕ СІМЕЙНОЇ ОСВІТИ В УКРАЇНІ: УПРАВЛІНСЬКІ, ЕКОНОМІЧНІ, ОРГАНІЗАЦІЙНІ ФАКТОРИ ВПЛИВУ	19
INTERNATIONAL ECONOMICS AND INTERNATIONAL RELATIONS		
Gnidina V.	ASSESSMENT OF THE INNOVATION SECURITY LEVEL IN UKRAINE	24
MANAGEMENT		
Danylenko V.	EVALUATION OF LOGISTICS INNOVATIONS INTRODUCTION RESULTS	30
Догадайло Я.В. Суконна Н.Г.	АНАЛІЗ МЕТОДИЧНИХ ПІДХОДІВ ЩОДО ВИМІРЮВАННЯ РЕЗУЛЬТАТИВНОСТІ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА	33
Исамухамедов Б.Б. Исамухамедова Д.А.	СТРАТЕГИЧЕСКИЕ НАПРАВЛЕНИЯ УПРАВЛЕНИЯ СИСТЕМОЙ ПОДГОТОВКИ КАДРОВ ЭКОНОМИСТОВ	41
MARKETING, ADVERTISING AND PR		
Чикалова А.С.	СПЕЦИФІКА ВИКОРИСТАННЯ МАРКЕТИНГУ В ОРГАНІЗАЦІЇ ДІЯЛЬНОСТІ ПІДПРИЄМНИЦЬКИХ СТРУКТУР У НАДЗВИЧАЙНИХ УМОВАХ	48
FINANCE AND CREDIT		
Завальський А.А.	ІНСТРУМЕНТИ ГРОШОВО-КРЕДИТНОЇ ПОЛІТИКИ	51
Фролов С.М. Ясько К.В. Зіненко В.В.	ФОНДОВИЙ РИНОК В УКРАЇНІ ТА СВІТІ: ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ	55
ACCOUNTING AND AUDITING		
Степаник А.О. Коломієць Д.В.	ОСОБЛИВОСТІ ОБЛІКУ СТРОКОВИХ ДЕПОЗИТІВ КЛІЄНТІВ БАНКУ	60
PEDAGOGY AND EDUCATION		
Karimova K.V.	CHILD DEVELOPMENT BY MUSICAL ARTS IN THE PRENATAL PERIOD	64

Kindrat I.P. Savyak O.L. Melnychuk L.V. Kryvoviaz O.S. Kindrat H.V. Ersteniuk H.M.	RESOURCES TO PROVIDE DISTANCE STUDYING AT UNIVERSITY DURING CORONAVIRUS DISEASE (COVID-19)	68
Konysbek A.	FORMATION OF AN ARTIFICIAL CULTURAL-LINGUISTIC ENVIRONMENT WHEN TEACHING ENGLISH AS A FOREIGN LANGUAGE (IN THE MATERIAL OF ORIGINAL FILMS)	71
Usmanova M.F. Haydarova N.E.	ENGLISH GRAMMAR BASICS	80
Антонець Н.Б.	ШКОЛИ РОБІТНИЧОЇ ТА СІЛЬСЬКОЇ МОЛОДІ ЯК ПРЕДМЕТ УВАГИ НАУКОВЦІВ ІНСТИТУТУ ПЕДАГОГІКИ (КІНЕЦЬ 1950-х – ПОЧАТОК 1960-х рр.)	85
Джамалдинова Ш.О. Бекирова Э.С.	ОБУЧЕНИЕ НАВЫКАМ РЕШЕНИЯ ПРОБЛЕМ НА ЗАНЯТИЯХ	88
Ибраймов А.Е. Нодиров Д.И.	ЭФФЕКТИВНОСТЬ ДИСТАНЦИОННЫХ КУРСОВ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ, ОРГАНИЗОВАННЫХ НА ОСНОВЕ ПРОФЕССИОНАЛЬНОЙ ДИАГНОСТИКИ	92
Маматова Ш. Шарабова Н.	ПОДХОДЫ И МЕТОДЫ В ПРЕПОДАВАНИИ РУССКОГО ЯЗЫКА	95
Шеремет І.В. Василенко К.С. Кірсанова Н.В.	ПРАКТИЧНІ АСПЕКТИ ВАЛЕОЕКОЛОГІЧНОЇ РОБОТИ З ВИХОВАНЦЯМИ ЗАКЛАДІВ ПОЗАШКІЛЬНОЇ ОСВІТИ	100
Шеремет І.В. Василенко К.С. Кравченко О.В.	ВДОСКОНАЛЕННЯ ОРГАНІЗАЦІЇ ПОЗАКЛАСНОЇ РОБОТИ ЩОДО ФОРМУВАННЯ НАВИЧОК ЗДОРОВОГО СПОСОБУ ЖИТТЯ У ДІТЕЙ МОЛОДШОГО ШКІЛЬНОГО ВІКУ	103
Шеремет І.В. Челнокова М.С. Василенко К.С. Макарова Г.С.	ОРГАНІЗАЦІЯ ПСИХОЛОГО-ПЕДАГОГІЧНОГО СУПРОВІДУ ДІТЕЙ З ОСОБЛИВИМИ ОСВІТНИМИ ПОТРЕБАМИ В УМОВАХ ЗАГАЛЬНООСВІТНЬОГО НАВЧАЛЬНОГО ЗАКЛАДУ	106
PHILOSOPHY AND COGNITION		
Kovtun N. Polishchuk O. Ventsel N. Kovalenko O.	SOCIAL RISKS OF COUNTRIES WITH EMERGING ECONOMIES AMID INDUSTRY 4.0 MODERNISATION CHALLENGES	111
Titova M.K.	DANTE'S PHILOSOPHY	114
SOCIOLOGY AND SOCIETY		
Мартинов Ю.І. Мартинов І.Б.	ТЕОРІЇ ТА ПРОБЛЕМИ КОНЦЕПТУ «СУСПІЛЬСТВО СПОЖИВАННЯ»	117
PSYCHOLOGY AND PSYCHIATRY		
Михайлишин У.Б.	ТЕОРЕТИЧНИЙ АНАЛІЗ ГЕНДЕРНИХ ВІДМІННОСТЕЙ УПРОЯВАХ КОМПОНЕНТІВ ЕМОЦІЙНОГО ІНТЕЛЕКТУ	120
Середа І.О.	СТИЛІ УПРАВЛІННЯ ВІЙСЬКОВИМ ПІДРОЗДІЛОМ	125

Ткаченко Н.В.	ПРОФЕСІЙНА ІДЕНТИЧНІСТЬ ВЧИТЕЛІВ ЯК РЕСУРС СТАНОВЛЕННЯ ТА РЕАЛІЗАЦІЇ ОСОБИСТІСНОГО ПОТЕНЦІАЛУ В ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ	131
---------------	--	-----

PHILOLOGY AND LINGUISTIC

Kozubai I.V. Khadzhy A.Y.	FEATURES OF SLANG IN AMERICAN RAP SONG LYRICS	139
Бабакулов И.Т.	КОНТРАСТ СЛОВООБРАЗОВАТЕЛЬНЫХ СИСТЕМ РУССКОГО И УЗБЕКСКОГО ЯЗЫКОВ В АСПЕКТЕ ЯЗЫКОВОЙ ДЕТЕРМИНАНТЫ	142
Строганова Г.М. Гудована Н.Ю.	ВИКОРИСТАННЯ ЦИФРОВОГО СТОРІТЕЛІНГУ НА УРОКАХ МОВЛЕННЕВОГО РОЗВИТКУ	146
Масеева М.К.	УПОТРЕБЛЕНИЕ ПРЕДЛОГОВ В РУССКОМ ЯЗЫКЕ, СВЯЗЬ С АНГЛИЙСКИМ И РОДНЫМ ЯЗЫКАМИ ДЛЯ СТУДЕНТОВ – МЕДИКОВ	150
Рогова Ю.В. Грак К.А.	СПЕЦИФИКА КОМПОНЕНТОВ «ДЕНЬ» И «НОЧЬ» НА МАТЕРИАЛЕ РУССКИХ ФРАЗЕМ	155
Ходжаева Н.А.	ТЕРМИНЫ ЛАТИНСКОГО ПРОИСХОЖДЕНИЯ: «ЖИВОЙ» ЛАТЫНИ	160
Хусаинова Г.Ш.	ОСОБЕННОСТИ ПРЕПОДАВАНИЯ УЗБЕКСКОГО ЯЗЫКА КАК ВТОРОГО ЯЗЫКА ИНОСТРАННЫМ СТУДЕНТАМ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ	165

JOURNALISM AND TELECOMMUNICATIONS

Mussayeva B. Shyngyssova N. Mukhametkaliyeva S.	MEDIA LITERACY IN KAZAKHSTAN: DEVELOPMENT AND PROSPECTS	168
---	---	-----

LAW AND INTERNATIONAL LAW

Cisko Lukáš	SEVERAL CONSIDERATIONS TO THE UNIFICATION OF PRIVATE LAW IN THE EUROPEAN UNION	176
Дмитренко	ІНДИВІДУАЛЬНЕ ПОПЕРЕДЖЕННЯ ЗЛОЧИНІВ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ: ПОНЯТТЯ, МЕТА ТА ЗАВДАННЯ	180
Дриголь О.О.	КОНФЛІКТ ІНТЕРЕСІВ В СФЕРІ ОСВІТИ	184
Иванчикова Л.Д.	СУЩНОСТЬ И СОДЕРЖАНИЕ АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ НЕСОВЕРШЕННОЛЕТНИХ В РЕСПУБЛИКЕ БЕЛАРУСЬ	188
Кота Я.Ф.	ІМПЛЕМЕНТАЦІЯ МІЖНАРОДНИХ НОРМ ІСАО ЩОДО АВІАПЕРЕВЕЗЕНЬ ВАНТАЖУ ДО НАЦІОНАЛЬНИХ ЗАКОНОДАВСТВ	194
Лахова О.В.	ДОСЛІДЖЕННЯ ЛІНГВІСТИКИ ПОНЯТТЯ «ТЯЖКІ НАСЛІДКИ» В ЗАКОНІ ПРО КРИМІНАЛЬНУ ВІДПОВІДАЛЬНІСТЬ УКРАЇНИ	199
Наев В.С.	ІСТОРИКО-ПРАВОВИЙ АНАЛІЗ РАБОВЛАСНИЦТВА НА ТЕРИТОРІЇ США	203
Савицька В.М.	ПОНЯТТЯ ЗАВІДОМОСТІ У КРИМІНАЛЬНОМУ ПРАВІ УКРАЇНИ	206

Шевчук В.М.	КРИМІНАЛІСТИЧНА ТАКТИКА: СУЧАСНЕ РОЗУМІННЯ ТА МЕЖІ ЗАСТОСУВАННЯ	211
GEOGRAPHY AND LOCAL HISTORY		
Шкурко К.Н.	КОМПЛЕКСНЫЙ АНАЛИЗ СОСТОЯНИЯ ОБЪЕКТОВ РАСТИТЕЛЬНОГО МИРА, ПРОИЗРАСТАЮЩИХ НА ЗЕМЛЯХ ОБЩЕГО ПОЛЬЗОВАНИЯ В ПРЕДЕЛАХ ГОРОДСКИХ ТЕРРИТОРИЙ (НА ПРИМЕРЕ Г. МОГИЛЕВА И ОКРЕСТНОСТЕЙ)	222
ARTS, CULTURAL STUDIES AND ETHNOGRAPHY		
Salaev I.B.	THE SPECIFICITY AND GENERAL ASPECTS OF CUSTOMS, TRADITIONS AND RITUALS IN HOUSING CONSTRUCTION OF THE POPULATION OF THE KHOREZM OASIS AND FERGHANA VALLEY	230
Олексенко И.В. Мельникова А.Ю.	К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ АНДРАГОГИЧЕСКИХ ПРИНЦИПОВ ОБУЧЕНИЯ В ФОРТЕПИАННОЙ ПЕДАГОГИКЕ	233
BIOLOGY AND BIOTECHNOLOGY		
Клименко О.А.	ОЦЕНКА ХОЛОДОУСТОЙЧИВОСТИ МУЖСКОГО ГАМЕТОФИТА ЛИНИЙ И ГИБРИДОВ КУКУРУЗЫ.	241
Сотников Е.Б. Сидорова М.В. Богданов А.О. Туркин А.В. Доминова И.Н..	ЭКСПРЕССИЯ ТЕНАСЦИНОВ В НЕЙРОНАХ В ОТВЕТ НА ЛИПОПОЛИСАХАРИД IN VITRO	245
MEDICINE AND PHARMACY		
Mavlyanova Z.F. Khusinova Sh.A.	DIAGNOSTICS PROTEIN AND ENERGY INSUFFICIENCY CEREBRAL PALSI	249
Абдусаломова М.А. Равшанова М.З.	ОСОБЕННОСТИ РЕАБИЛИТАЦИОННЫХ МЕРОПРИЯТИЙ ПРИ БОЛЯХ В ПОЯСНИЦЕ У СПОРТСМЕНОВ, ЗАНИМАЮЩИХСЯ СПОРТОМ СО СКОРОСТНЫМИ И СИЛОВЫМИ КАЧЕСТВАМИ.	255
Аскарова Н.К.	ЧАСТО БОЛЕЮЩИЕ ДЕТИ ДОШКОЛЬНОГО ВОЗРАСТА: ИНФЕКЦИОННЫЕ ЗАБОЛЕВАНИЯ ВЕРХНИХ ДЫХАТЕЛЬНЫХ ПУТЕЙ И ЛОР-ОРГАНОВ.	259
Аскарова Ф.К. Аскарова Н.К.	ПИТАНИЕ БЕРЕМЕННОЙ И КОРМЯЩЕЙ МАТЕРИ С ЖЕЛЕЗОДЕФИЦИТНОЙ АНЕМИЕЙ	266
Ахматова Ю.А. Ахматов А. Нажимов Ш. Р. Сирожова Н.А.	ВЗАИМООТНОШЕНИЕ ДИСФУНКЦИИ ПОЧЕК И КАРДИОВАСКУЛЯРНЫХ ИЗМЕНЕНИЙ У ДЕТЕЙ ПРИ ЯВЛЕНИЯХ С ХРОНИЧЕСКОЙ ПОЧЕЧНОЙ НЕДОСТАТОЧНОСТЬЮ В ДОДИАЛИЗНОЙ СТАДИИ	273
Левинська Н.І. Гончарюк М.В. Соловей В.М.	СТРАТИФІКАЦІЯ ФАКТОРІВ РИЗИКУ ГІПЕРПЛАСТИЧНИХ ПРОЦЕСІВ ЕНДОМЕТРІУ МАТКИ	279
Гошовська А.В. Сергій І.В.	ДОПЛЕРОМЕТРИЧНІ ПОКАЗНИКИ КРОВОТОКУ МАТКОВИХ АРТЕРІЙ В ПЕРШОМУ ТРИМЕСТРІ ВАГІТНОСТІ У ЖІНОК НА ФОНІ БАКТЕРІАЛЬНОГО ВАГІНОЗУ	282

Гошовська А.В. Мігайчук Д.М.	ЕФЕКТИВНІСТЬ РЕЗУЛЬТАТІВ ПРОФІЛАКТИКИ ПОРУШЕНЬ ПЛАЦЕНТАРНОГО КОМПЛЕКСУ У ЖІНОК ГРУП РИЗИКУ.	286
Зулфикарова Э.Т. Каусова Г.К. Сабиргалиева Ж.Р.	ПСИХООБРАЗОВАНИЕ ПРИ ПСИХИЧЕСКИХ РАССТРОЙСТВАХ	294
Камалова Ё.А.	ОСОБЕННОСТИ ФИЗИЧЕСКОЙ РЕАБИЛИТАЦИИ ОСТЕОХОНДРОЗА ПОЯСНИЧНОГО ОТДЕЛА ПОЗВОНОЧНИКА	301
Пенькова А.А. Умарова К.Р.	РОЛЬ ТРЕНИНГА В СНИЖЕНИИ ПОВЕДЕНЧЕСКИХ РИСКОВ ВИЧ ИНФИЦИРОВАННЫХ	304
Рустамов А.А. Атабекова Ш.Н..	ПРИМЕНЕНИЕ ПАСТЫ GRANULOTEC ПРИ ЛЕЧЕНИИ ХРОНИЧЕСКОГО ГРАНУЛЕМАТОЗНОГО ПЕРИОДОНТИТА	312

NATURE MANAGEMENT, RESOURCE SAVING AND ECOLOGY

Ковалев Р.Н. Еналеева-Бандура И.М. Штерн С.С. Астапкович К.В. Бровкин С.А. Шувалова В.А.	ОЦЕНКА ВЕЛИЧИНЫ ЭКОЛОГО-ЭКОНОМИЧЕСКОГО УЩЕРБА ОТ ПОЖАРОВ ЛЕСНЫМ ЭКОСИСТЕМАМ	315
Ковалев Р.Н. Еналеева-Бандура И.М. Штерн С.С. Астапкович К.В. Бровкин С.А. Шувалова В.А.	МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОГНОЗИРОВАНИЯ ЛЕСНЫХ ПОЖАРОВ	321

CHEMISTRY AND MATERIALS SCIENCE

Аскарров К.А. Аскарова Н.К.	ПРИМЕНЕНИЕ ПОРФИРИНОВ В МЕДИЦИНЕ	325
--------------------------------	----------------------------------	-----

GENERAL ENGINEERING AND MECHANICS

Marchenko D.D. Zubiekhina Khaliat Oleksandra V. Matvyeyeva K.S.	RESERCH ON RIGIDITY OF THE SYSTEM "MACHINE TOOL-TOOL-DETAIL" WHEN RUNNING BY ROLLERS	332
--	--	-----

RADIO ENGINEERING, ELECTRONICS AND ELECTRICAL ENGINEERING

Eshquvatov H. E. Tillayev. Y. A. Asatov O'.T.	CALCULATE OF IONOSPHERIC TEC AND SCINTILLATION S4 INDEX FROM THE MAIDANTAL GPS STATION	342
---	--	-----

INFORMATION AND WEB TECHNOLOGIES

Голубничий Д.Ю. Северінов О.В. Соловйова О.І. Солдатенко І.В. Семеренко Ю.О.	АНАЛІЗ ВИМОГ ДО ФОРМУВАННЯ ЗАСОБІВ КОНТРОЛЮ В СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ПРОЦЕСНОГО ПІДХОДУ	346
--	---	-----

Давыдова А.Л. Буркина А.А. Тарасенко Е.Ю. Чесакова С.А.	АНАЛИЗ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ЗАКУПОЧНОЙ ЛОГИСТИКИ В ЛЕСНОЙ ОТРАСЛИ	356
Коломійцев О.В. Полтавський Е.М. Топчій В.Л.	МЕТОД ВИМІРЮВАННЯ ПАРАМЕТРІВ РУХУТРАНСПОРТНИХ ЗАСОБІВ	361
Плакасова Ж.М. Метелеап В.В.	МОДУЛЬ ОБРОБКИ ТА АНАЛІЗУ ЗОБРАЖЕНЬ ДЕФЕКТІВ КАРБОНАТНИХ ПЛИТ	367

MILITARY AFFAIRS AND NATIONAL SECURITY

Шемчук В.А.	ОРГАНІЗАЦІЙНО-МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ПО УДОСКОНАЛЕННЮ НОРМАТИВНО-ПРАВОВИХ ДОКУМЕНТІВ ОРГАНІЗАЦІЇ ТА ФУНКЦІОНУВАННЯ ФІЗИЧНОЇ ПІДГОТОВКИ ВІЙСЬКОВОСЛУЖБОВЦІВ ЗБРОЙНИХ СИЛ УКРАЇНИ	372
-------------	--	-----

INFORMATION AND WEB TECHNOLOGIES

UDC 681.51

Голубничий Дмитро Юрійович

ORCID ID: 0000-0002-6873-7004

кандидат технічних наук, доцент, доцент кафедри інформаційних систем
Харківський національний економічний університет імені Семена Кузнеця, Україна

Сєверінов Олександр Васильович

ORCID ID: 0000-0002-6327-6405

кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій інституту цивільної авіації
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

Соловйова Ольга Ігорівна

ORCID ID: 0000-0003-4403-9532

кандидат технічних наук,
завідувач кафедри інформаційних технологій інституту цивільної авіації
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

Солдатенко Ірина Володимирівна

викладач кафедри інформаційних технологій інституту цивільної авіації
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

Семеренко Юлія Олександрівна

старший викладач кафедри інформаційних технологій інституту цивільної авіації
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

АНАЛІЗ ВИМОГ ДО ФОРМУВАННЯ ЗАСОБІВ КОНТРОЛЮ В СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ПРОЦЕСНОГО ПІДХОДУ

Анотація. виконано аналіз вимог до формування засобів контролю в системах інформаційної безпеки на основі процесного підходу.

Ключові слова: інформація, загроза, процес, контроль, безпека.

Інформація завжди виступає одним з головних ділових ресурсів, що забезпечує організації додану вартість. Внаслідок цього інформація потребує

захисту. Слабкі місця, які є в захисті інформації можуть призводити до фінансових втрат, нести збиток комерційним операціям. Сьогодні питання розробки системи управління інформаційною безпекою та її впровадження в організації є вельми важливою, а можливо сказати й концептуальною [1-2].

Інформація існує в різних формах. Її можна зберігати на комп'ютерах, передавати по обчислювальних мережах, роздруковувати або записувати на папері, а також озвучувати в розмовах. З погляду безпеки всі види інформації, включаючи паперову документацію, бази даних, плівки, мікрофільми, моделі, магнітні стрічки, дискети, розмови й інші способи, які використовуються для передачі знань і ідей, вимагають належного захисту.

Стандарт ISO 27001 визначає інформаційну безпеку як: "збереження конфіденційності, цілісності та доступності інформації" [1]. ISO 27001:2005 є переліком вимог до системи менеджменту інформаційної безпеки, обов'язкових для сертифікації, а стандарт ISO 27002:2005 виступає в якості керівництва по впровадженню, що може застосовуватися при проектуванні механізмів контролю, вибраних організацією для зменшення ризиків інформаційної безпеки.

Загальний процес управління системою інформаційної безпеки з використанням нотаций стандарту IDEF0 [2], може бути описаний наступним чином (рис. 1).



Рисунок 1 – Контекстна діаграма процесу управління системою інформаційної безпеки

Декомпозиція процесу управління системою інформаційної безпеки призводить до формування наступних процесів (рис.2):

1. Формування засобів контролю (рівень А1).
2. Захист немашинних інформаційних ресурсів (рівень А2).
3. Забезпечення безпеки персоналу (рівень А3).
4. Забезпечення фізичної безпеки (рівень А4).
5. Забезпечення безпеки навколишнього середовища (рівень А5).
6. Адміністрування комп'ютерних систем і обчислювальних мереж (рівень А6).
7. Додаткові засоби охорони системи (рівень А7).
8. Планування забезпечення безперервної діяльності у випадку позаштатних ситуацій (рівень А8).

Кожен з рівнів має свої особливості, особисте призначення та також підвергається декомпозиції.

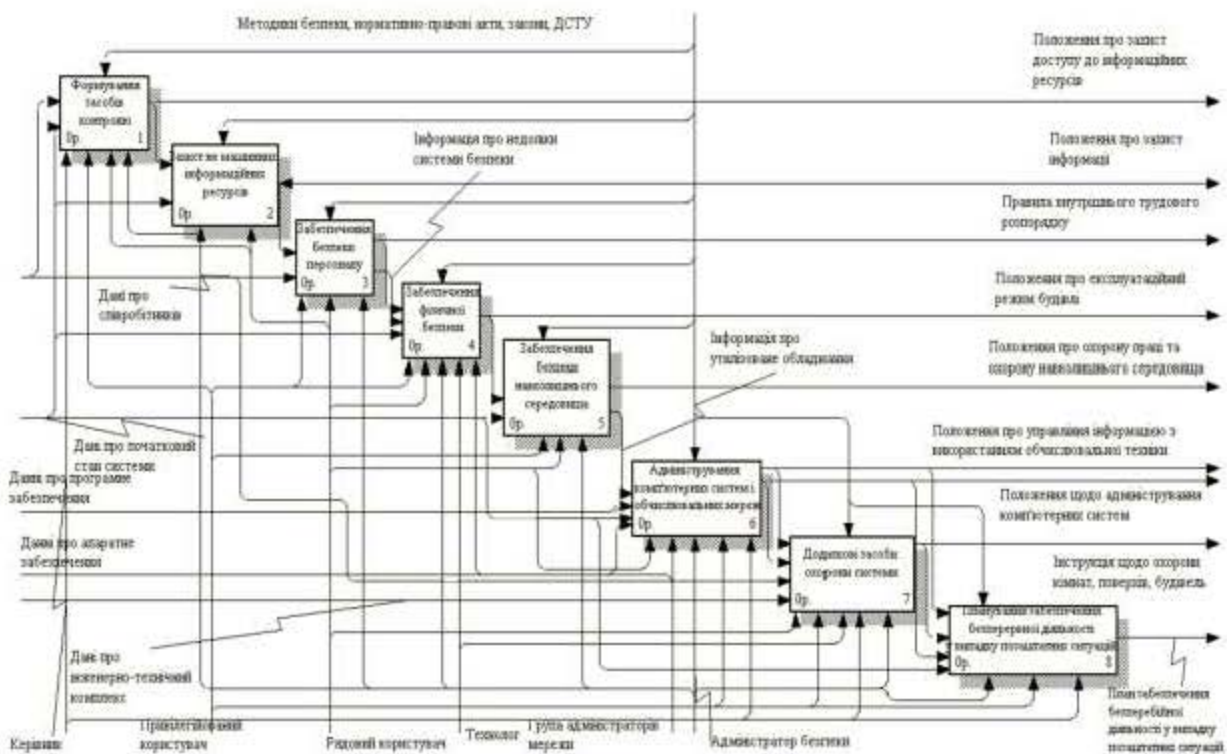


Рисунок 2 – Діаграма функціональної декомпозиції процесу управління системою інформаційної безпеки

Декомпозиція процесу формування засобів контролю визначає такі процеси, як рис. 3: виявлення загроз інформаційної безпеки; аналіз причин необхідності використання системи інформаційної безпеки; розробка стратегії усунення погроз інформаційної безпеки; формування засобів контролю системи; створення документа про політику інформаційної безпеки.

Виявлення загроз інформаційної безпеки. Загроза – це ситуація (стан), яка підвищує ймовірність реалізації однієї або декількох атак та підвищує рівень загроз безпеки (рис. 4). В системі та середовищі безпеки потенційно існують загрози та інші небезпечні події. Під загрозою розуміються події, джерелом яких є людина (агент загроз). Настання небезпечної події може призвести до нещасного випадку, а реалізація загрози – є атакою агента загроз.

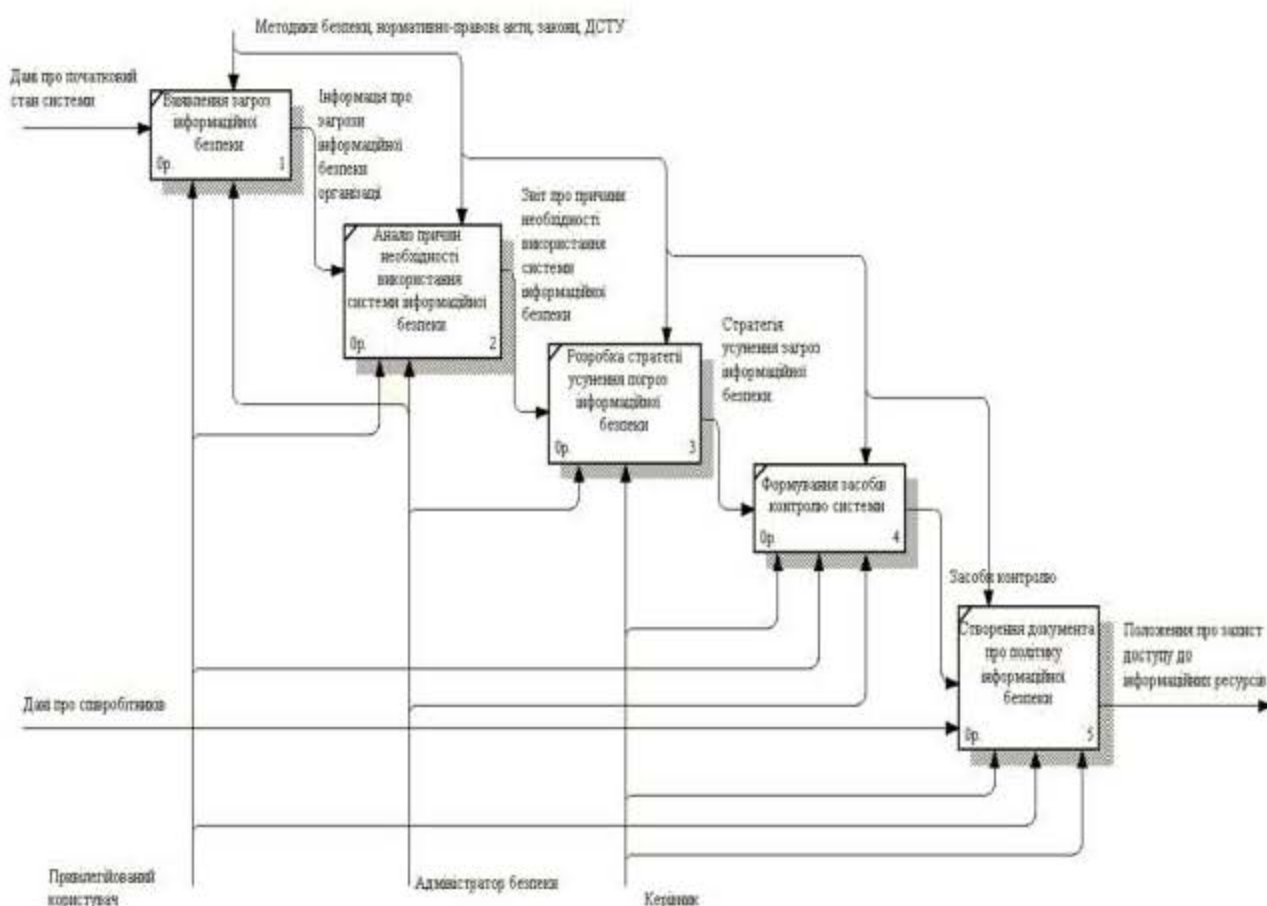


Рисунок 3 – Діаграма функціональної декомпозиції процесу формування засобів контролю (ТО-ВЕ)



Рисунок 4 – Діаграма понять "небезпечна подія – загроза"

Аналіз причин необхідності використання системи інформаційної безпеки. Інформація й підтримуючі її інформаційні системи та мережі є коштовними виробничими ресурсами організації. Їхня доступність, цілісність і конфіденційність можуть мати особливе значення для забезпечення конкурентоздатності, руху готівки, рентабельності, відповідності правовим нормам і іміджу організації.

Розробка стратегії усунення погроз інформаційної безпеки. Сучасні організації можуть зіткнутися зі зростаючою погрозою порушення режиму безпеки, що виходить від цілого ряду джерел. Інформаційним системам і мережам можуть загрожувати такі небезпеки, як комп'ютерне шахрайство, шпигунство, саботаж, вандалізм, а також інші джерела відмов і аварій. З'являються всі нові погрози, здатні завдати шкоди організації, такі, як, широко відомі комп'ютерні віруси або хакери. Передбачається, що такі погрози інформаційної безпеки згодом стануть більш розповсюдженими, небезпечними й витонченими. У той же час через зростаючу залежність організацій від інформаційних систем і сервісів, вони можуть стати більше уразливими стосовно погроз порушення захисту. Поширення обчислювальних мереж надає нові можливості для несанкціонованого доступу до комп'ютерних систем, а тенденція до переходу на розподілені обчислювальні системи зменшує можливості централізованого контролю інформаційних систем фахівцями.



Захисні міри виявляються значно більш дешевими й ефективними, якщо вони вбудовані в інформаційні системи й сервіси на стадіях завдання вимог і проектування. Ніж скоріше організація розробить стратегію захисту своїх інформаційних систем, тим більше дешевими й ефективними вони будуть для неї згодом.

Формування засобів контролю системи. Не всі засоби контролю можна застосовувати до кожного з інформаційних середовищ. Їх варто використовувати вибірково з урахуванням місцевих умов. Однак більшість засобів контролю, описаних у даному документі, широко застосовуються великими організаціями зі значним досвідом роботи, і їхнє використання рекомендується для всіх ситуацій, зрозуміло, з урахуванням обмежень, які накладаються технологією й навколишнім середовищем. Ці загальноприйняті засоби контролю часто називають базовими засобами управління безпекою, оскільки всі вони в сукупності визначають базовий промисловий стандарт на підтримку режиму безпеки.

Десять ключових засобів контролю являють собою або обов'язкові вимоги, наприклад, вимоги чинного законодавства, або вважаються основними структурними елементами інформаційної безпеки, наприклад, навчання правилам безпеки. Ці засоби контролю застосовуються до усіх організацій, середовищ і відзначаються символом ключа. Вони служать основою для організацій, що приступають до реалізації засобів управління інформаційною безпекою. Ключовими є наступні засоби контролю:

- документ про політику інформаційної безпеки;
- розподіл обов'язків по забезпеченню інформаційної безпеки;
- навчання й підготовка персоналу по підтримці режиму інформаційної безпеки;
- повідомлення про випадки порушення захисту;



- засоби захисту від вірусів;
- процес планування безперервної роботи організації;
- контроль за копіюванням програмного забезпечення, захищеного законом про авторське право;
- захист документації організації;
- захист даних;
- відповідність політиці безпеки.

Результатом процесу є створення документа про політику інформаційної безпеки, який визначається у вигляді положення про захист доступу до інформаційних ресурсів.

Положення розробляється для виключення несанкціонованого доступу до інформаційних ресурсів з метою виключення витоку конфіденційної інформації, а також несанкціонованої модифікації або знищення даних.

Автентифікація легальних суб'єктів доступу здійснюється за допомогою парольного захисту, персонального коду доступу, електронних ключів і інших програмно-технічних засобів розмежування доступу користувачів.

Спосіб автентифікації легальних користувачів визначається відповідно до рівня конфіденційності інформації. Рівень конфіденційності даних визначається власником ресурсу за узгодженням зі службою безпеки.

Активне мережне обладнання (маршрутизатори і мережні принтери) не повинне допускати можливості несанкціонованої переконфігурації, у зв'язку з чим, кожен активний мережний пристрій повинен бути захищений унікальним паролем.

Операційні системи серверів комп'ютерної мережі повинні будуватися таким чином, щоб блокувати вхід у мережу (на 5-15 хвилин) після троекратної помилки в наборі пароля.

Якщо дозволяють можливості операційної системи, необхідно заборонити



вибір користувачем простих паролів засобами операційної системи.

Порядок закладу і реєстрації засобів розмежування користувачів визначає такі дії:

1. При введенні нового користувача адміністратор інформаційного ресурсу повинний призначити для нього однократний пароль, персональний код або іншу унікальну інформацію для доступу до інформаційних ресурсів комп'ютерної мережі.

2. Користувач зобов'язаний замінити однократний пароль – особистим при першому ж підключенні до інформаційного ресурсу комп'ютерної мережі.

3. Користувач зобов'язаний зберігати в таємниці пароль, код і інші засоби доступу до інформаційних ресурсів.

Вимоги до періоду дії паролів і кодів доступу користувачів наступні:

1. Періодичність зміни пароля задається адміністратором інформаційного ресурсу централізовано, для всіх користувачів.

2. Період дії паролів для мережних комп'ютерів не повинен перевищувати 3 місяці, для не мережних комп'ютерів – 6 місяців.

3. При повідомленні комп'ютерної системи про закінчення терміну дії особистого пароля користувач зобов'язаний замінити його на новий, що раніше не застосовувався.

4. Період дії паролів для входу на автоматизоване робоче місце не повинний перевищувати 3 місяців.

5. Персональні коди, електронні ключі й інші засоби розмежування доступу змінюються за вимогою користувача не рідше встановленого періоду.

Конфіденційність паролів і кодів доступу повинна мати наступні ознаки:

1. Інформація про паролі користувачів є конфіденційною інформацією.

2. Операційні системи, сервери і робочі станції повинні бути побудовані таким чином, щоб виключити можливість ознайомлення користувачів і адміністраторів з діючими і минулими паролями.



3. Автоматизовані інформаційні системи повинні бути збудовані таким чином, щоб виключити можливість ознайомлення користувачів і адміністраторів з діючими і минулими паролями.

4. Інформація про персональні коди, електронні ключі й інші засоби доступу користувачів до інформаційного ресурсу є конфіденційною інформацією і розголошенню не підлягає, повинна містити захист від доступу сторонніх осіб.

Принципи вибору і формування особистих паролів наступні:

1. В якості пароліної інформації варто вибрати послідовність букв верхнього і нижнього регістра, цифр і службових символів довжиною не менш восьми знаків.

2. Для паролю категорично забороняється використання послідовностей символів, що вгадуються легко, типу: назви облікового запису, номерів телефонів, імен своїх і родичів, послідовно розташовані на стандартній клавіатурі символи, табельний номер і т.п. Забороняється також використання в якості паролю слів розповсюджених світових мов, незалежно від розкладки клавіатури, у якій воно набирається (наприклад, слово МАШИНА – VFIBYF).

3. У паролі, крім буквених послідовностей, обов'язково повинні бути присутніми цифри і спеціальні символи.

4. Якщо дозволяють можливості системи автентифікації рекомендується поряд з англійськими буквами використовувати букви російського алфавіту (з переключенням набору символів на клавіатурі).

5. Рекомендується у виді пароля вибрати послідовності типу “X0P0sh#1”, “!1риб@lk” або “Def*en\$6”

6. При зміні пароля користувачам забороняється використовувати раніше використані паролі.

7. Вибір одноразових паролів здійснюється по тим же вимогам.

8. Довжина пароля адміністратора інформаційного ресурсу повинна бути

не менш 11 символів. Пароль не повинен містити, ні якої логіки. Наприклад “k\$iu^sd26Fx”. Глибина історії пароля не менш 20.

Таким чином, в роботі сформульовані вимоги до формування засобів контролю в системах інформаційної безпеки на основі процесного підходу.

Список джерел:

1. ISO/IEC 27001:2005. Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимоги. – British Standards, 2006. – 57 с.
2. IDEF0. Методология функционального моделирования IDEF0. Руководящий документ. – Госстандарт России, Москва, 2000. – 68 с.
3. Третяк В.Ф., Місюра О.М., Більчук В.М. Метод оптимізації структури розподіленої бази даних у вузлах інфокомунікаційної мережі хмарного середовища // Наука і техніка Повітряних Сил Збройних Сил України. – 2017. – № 1. – С. 92-96.
4. Третяк В.Ф., Пашнева А.А. Оптимізація структури сховища даних у вузлах інфокомунікаційної мережі хмарного середовища // Системи управління, навігації та зв'язку. – 2017. – №. 4 (44). – С. 122-128.
5. Пономаренко В.С., Голубничий Д.Ю., Третяк В.Ф. Цілочисельне програмування в економіці. – Харків: Вид. ХНУ, 2005. – 204 с.
6. Альошин, Г., Коломійцев, О., Третяк, В. Особливості оптимального синтезу багатоскальних інформаційно-вимірювальних систем. Збірник наукових праць ЛОГОС, 81-84. <https://doi.org/10.36074/24.04.2020.v2.23>

SCIENTIFIC EDITION

BN 979-1-293101-09



9 791293 101093

**Proceedings of the 4th International Scientific and
Practical Conference**

CHALLENGES IN SCIENCE OF NOWADAYS

**WASHINGTON, USA
26-28.05.2020**



InterConf

Scientific Publishing Center