SCIENTIFIC COLLECTION «INTERCONF»

№ 2 (38)

December, 2020

THE ISSUE CONTAINS:

Proceedings of the 1st International Scientific and Practical Conference

SCIENCE, EDUCATION, INNOVATION: TOPICAL ISSUES AND MODERN ASPECTS

TALLINN, ESTONIA

16-18.12.2020

InterConf
Scientific Publishing Center

SCIENTIFIC COLLECTION «INTERCONF»

№ 2 (38) | December, 2020

THE ISSUE CONTAINS:

Proceedings of the 1st International Scientific and Practical Conference

SCIENCE, EDUCATION, INNOVATION: TOPICAL ISSUES AND MODERN ASPECTS

TALLINN, ESTONIA

16-18.12.2020

TALLINN
2020

UDC 001.1

S 40 *Scientific Collection «InterConf»*, (38): with the Proceedings of the 1st International Scientific and Practical Conference «Science, Education, Innovation: Topical Issues and Modern Aspects» (December 16-18, 2020). Tallinn, Estonia: Uhingu Teadus juhatus, 2020. 1376 p.

ISBN 978-5-7983-4322-5

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. Albena 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. (2020). Title of article or abstract. *Scientific Collection «InterConf»,* (38): with the Proceedings of the 1st International Scientific and Practical Conference «Science, Education, Innovation: Topical Issues and Modern Aspects» (December 16-18, 2020) in Tallinn, Estonia; pp. 21-27. Available at: https://interconf.top/...

This issue of Scientific Collection «InterConf» contains the International Scientific and Practical 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 Uhingu Teadus juhatus
©2020 Authors of the abstracts
©2020 Scientific Publishing Center InterConf

TABLE OF CONTENTS

BUSINESS ECONOMICS

Aristanbekova Zh. Minisheva A. Kuznetsova S.	THE ESSENCE OF LABOUR MOTIVATION OF PERSONNEL	17
Fostolovych V. Hurtovyi O.	ANALYTICAL ASSESSMENT OF ENTERPRISE PERFORMANCE INDICATORS USING AUTOMATED ACCOUNTING AND MANAGEMENT SYSTEMS	20
Levkovich L.L.	CONTEMPORARY CONCEPTS IN HIGHER EDUCATION SYSTEM MANAGEMENT IN CONTEXT OF INTERNATIONALIZATION	31
Tongxin Yu Khalid Nadeem Umair Ahmed	BUSINESS CLIMATE AND IMPLICATIONS FOR FOREIGN ENTREPRENEURSHIP DEVELOPMENT IN KAZAKHSTAN	37
Vasil'eva T.S.	SOCIAL RESPONSIBILITY AS THE MAIN COMPONENT IN THE MARKET OF TRANSPORT SERVICES IN THE FIELD OF PASSENGER TRANSPORTATION	46
Вітюнін В.О.	КАДРОВА ПОЛІТИКА В КОНТЕКСТІ РЕАЛІЗАЦІЇ КОМПЕТЕНЦІЙ ПЕРСОНАЛУ ПІДПРИЄМСТВА	51
Гавриш О.М. Сідікі Р.Н.	ВИЗНАЧЕННЯ СУТНОСТІ ДІАГНОСТИКИ РИНКОВОЇ ВАРТОСТІ БІЗНЕСУ	54
Гапак Н.М. Бойко Я.М.	АКТУАЛЬНІ ПИТАННЯ ІННОВАЦІЙНОГО РОЗВИТКУ ПІДПРИЄМСТВ РЕГІОНУ	57
Ярова Н.В. Ліщенко В.С.	ФОРМУВАННЯ МЕТОДИЧНИХ ПОЛОЖЕНЬ ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ КОНТЕЙНЕРНОГО ТЕРМІНАЛУ	61
Мостенська Т.Л. Юрій Е.О.	ХАРАКТЕРИСТИКА ЕТАПІВ РЕСТРУКТУРИЗАЦІЇ ПІДПРИЄМСТВ	66
Павлова В.А. Чукова І.П.	ПІДПРИЄМНИЦЬКІ АСПЕКТИ НАДАННЯ ДОДАТКОВИХ ПОСЛУГ У СФЕРІ ТОРГІВЛІ	70
Пронкіна Л.І. Прищепа Р.О.	ДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ІНВЕСТИЦІЙ	73
Ризакулов Ш.Ш. Хужамкулов Э.Г.	РИСК НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ НА ПРИМЕРЕ ПАРКА ПРИЕМА ТЕХНИЧЕСКОЙ СТАНЦИИ	75
Тімченко О.Д.	ВПЛИВ СОЦІАЛЬНО-ЕКОНОМІЧНИХ ЧИННИКІВ ТА ГЛОБАЛЬНИХ ЗМІН НА РОЗВИТОК ПРОЦЕСІВ УПРАВЛІННЯ ПІДПРИЄМСТВАМИ СФЕРИ ХАРЧУВАННЯ	85
Шилова Т.О.	ГЕНЕРАТОРИ ВАРТОСТІ ПІДПРИЄМСТВ ТРАНСПОРТНО-ЛОГІСТИЧНОЇ ГАЛУЗІ	94

REGIONAL ECONOMY

Cisko L.	SUPPORT OF THE BUSINESS SECTOR FOR EFFECTIVE DEVELOPMENT OF THE NATIONAL ECONOMY	98
Kachurka V. Kachurka P.	INNOVATION AND EDUCATIONAL CLUSTER AS AN ELEMENT OF DEVELOPMENT OF PUBLIC-PRIVATE PARTNERSHIP IN BREST REGION OF THE REPUBLIC OF BELARUS	102

Умарова Б.Х. Таирова Д.Р. Нурулоева З.К.	ФОРМИРОВАНИЕ МЕЖПРЕДМЕТНЫХ СВЯЗЕЙ В ПРЕПОДАВАНИИ РУССКОГО ЯЗЫКА	1318

ARCHITECTURE, CONSTRUCTION AND DESIGN

Oros A. Iusco I.	ANALYSIS OF PERSONALITY THEORIES FROM THE PERSPECTIVE OF ESSENTIALIZING THE CONCEPT OF CONSTRUCTIVE COMPETENCE IN THE FORMATION OF SOCIAL COMPETENCES IN STUDENTS	1324

PHYSICAL EDUCATION AND SPORTS

Chobotko M.A. Chobotko I.I. Lastovkin V.A. Schastlyvets V.I.	IMPROVING COMPETENCIES IN JUDO JUDGING	1328
Базилевич Н.О. Божко С.А. Тонконог О.С.	ОРГАНІЗАЦІЙНО-МЕТОДИЧНІ ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ОЗДОРОВЧОЇ ФІТНЕС-ТЕХНОЛОГІЇ «FITCURVS» В ПРОЦЕСІ ФІЗИЧНОГО ВИХОВАННЯ СТУДЕНТОК	1335
Горбенко О.В. Лисенко А.О.	ПІДГОТОВКА СПОРТСМЕНІВ У СПОРТИВНИХ ТАНЦЯХ НА СУЧАСНОМУ ЕТАПІ (ЛАТИНОАМЕРИКАНСЬКА ПРОГРАМА)	1345
Набиев Т.Э.	ЗНАЧЕНИЕ ФИЗИЧЕСКИХ УПРАЖНЕНИЙ В МАКСИМАЛЬНОМ ПОТРЕБЛЕНИИ КИСЛОРОДА	1352
Скирта О.С. Домащенко В.В. Копкін Б.В.	АНАЛІЗ РУХУ УДАРНОЇ БІОЛАНКИ КІКБОКСЕРІВ (ІСКА) В РОЗДІЛІ К-1	1360

MILITARY AFFAIRS AND NATIONAL SECURITY

Голубничий Д.Ю. Коломійцев О.В. Третяк В.Ф. Запара Д.М. Новіченко С.В. Євстрат Д.І.	ВИЗНАЧЕННЯ ФАЗ ПРОВЕДЕННЯ АУДИТУ ТА КАТЕГОРІЇ ПОРУШНИКІВ КІБЕРБЕЗПЕКИ	1367

MILITARY AFFAIRS AND NATIONAL SECURITY

UDC 681.3

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

Коломійцев Олексій Володимирович

ORCID ID: 0000-0002-3476-2666

Заслужений винахідник України

доктор технічних наук, старший науковий співробітник, професор кафедри

Національний технічний університет "Харківський політехнічний університет", Україна

Третяк Вячеслав Федорович

ORCID ID: 0000-0003-2599-8834

кандидат технічних наук, старший науковий співробітник, доцент,

науковий співробітник наукового центру Повітряних Сил

Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

Запара Денис Михайлович

ORCID ID: 0000-0003-3949-7555

начальник науково-дослідного відділу наукового центру Повітряних Сил

Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

Новіченко Сергій Володимирович

ORCID ID: 0000-0001-7043-446X

кандидат технічних наук, доцент, старший науковий співробітник, старший науковий

співробітник науково-дослідного відділу наукового центру Повітряних Сил

Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

Євстрат Дмитро Іванович

ORCID ID: 0000-0001-8393-6063

кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки

Харківський національний університет внутрішніх справ, Україна

ВИЗНАЧЕННЯ ФАЗ ПРОВЕДЕННЯ АУДИТУ ТА КАТЕГОРІЇ ПОРУШНИКІВ КІБЕРБЕЗПЕКИ

Аудит кібербезпеки – системний процес одержання об'єктивних якісних і кількісних оцінок про поточний стан кібербезпеки комп'ютерної мережі компанії у відповідності з визначеними критеріями та показниками кібербезпеки.

Фази проведення аудиту кібербезпеки:

– збір інформації про систему;

– мережевий аудит;

– локальний аудит (АРМ, сервера, мережевого обладнання);

– інші види аудиту.

Мережевий аудит поділяється, на:

– трасування, дослідження топології системи;

– сканування сервісів;

– інвентаризація ресурсів;

– сканування вразливостей, мережевий аудит паролів;

– перехоплення трафіку, проведення атак типу MitM (людина-посередині).

Локальний аудит поділяється, на:

– збір інформації про поточну програмно-апаратну конфігурацію персонального комп'ютера або пристрою;

– аудит локальних паролів;

– пошук залишкової інформації на носіях, контроль роботи механізмів;

– гарантованого знищення інформації.

Інші види аудиту поділяються, на:

– аудит бездротових комп'ютерних мереж;

– аудит web-вразливостей на Інтернет ресурсах.

Роботи з аудиту кібербезпеки інформаційної системи (ІС) включають в себе ряд послідовних етапів, які в цілому відповідають етапам проведення комплексних інформаційних технологій (ІТ) – аудиту автоматизованої системи,

що включає в себе:

– ініціювання процедури аудиту;

– збір інформації аудиту;

– аналіз даних аудиту;

– вироблення рекомендацій;

– підготовку аудиторського звіту.

На етапі ініціювання процедури аудиту повинні бути вирішені наступні організаційні питання:

– права та обов'язки аудитора повинні бути чітко визначені і документально закріплені в його посадових інструкціях, а також у положенні про внутрішній (зовнішній) аудит;

– аудитором повинен бути підготовлений і узгоджений з керівництвом план проведення аудиту;

– у положенні про внутрішній аудит має бути закріплено, зокрема, що співробітники компанії зобов'язані сприяти й надавати аудитору всю необхідну для проведення аудиту інформацію.

На етапі ініціювання процедури аудиту мають бути визначені межі проведення обстеження. План і межі проведення аудиту обговорюються на робочому зборах, в яких беруть участь аудитори, керівництво компанії і керівники структурних підрозділів (табл. 1).

Таблиця 1

Системна класифікація загроз кібербезпеки інформації

Параметри класифікації	Значення параметрів	Зміст значення параметра
1. Види	1.1. Фізична цілісність	Знищення (спотворення)
	1.2. Логічна структура	Спотворення структури
	1.3. Зміст	Несанкціонована модифікація
	1.4. Конфіденційність	Несанкціоноване отримання
	1.5. Право власності	Привласнення чужого права
2. Природа походження	2.1. Випадкова	Відмови, збої, помилки, стихійні лиха, побічні впливи
	2.2. Навмисна	Зловмисні дії людей

Продовження таблиці 1

Параметри класифікації	Значення параметрів	Зміст значення параметра
3. Передумови появи	3.1. Об'єктивні	Кількісна недостатність елементів системи, якісна недостатність елементів системи
	3.2. Суб'єктивні	Розвідка іноземних держав, промислове шпигунство, карні елементи, недобросовісні робітники
4. Джерела загроз	4.1. Люди	Сторонні особи, користувачі, персонал
	4.2. Технічні пристрої	Реєстрації, передачі, збереження, переробки, видачі
	4.3. Моделі, алгоритми, програми	Загального призначення, прикладні, допоміжні
	4.4. Технологічні схеми обробки	Ручні, інтерактивні, внутрішньо машинні, мережеві
	4.5. Зовнішнє середовище	Стан атмосфери, стороні шуми, побічні сигнали

Етап збору інформації аудиту є найбільш складним і тривалим. Це пов'язано з відсутністю необхідної документації на ІС і з необхідністю щільної взаємодії аудитора з багатьма посадовими особами організації.

Всі порушники діляться на дві категорії зовнішні та внутрішні. У свою чергу, внутрішні порушники діляться на зареєстрованих і незареєстрованних користувачів у системі. Зареєстровані користувачі діляться, відповідно до наявних прав, на простих користувачів, привілейованих користувачів і адміністраторів. Зовнішні порушники діляться на користувачів компанії і користувачів мережі Internet [3]. Для наочності класифікація порушників представлена на рис.1.

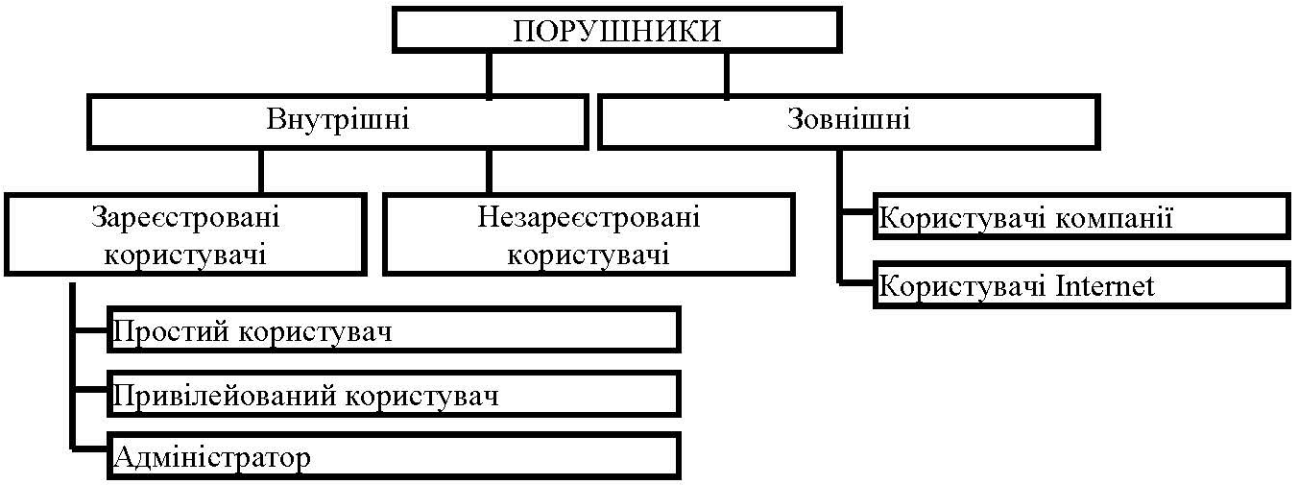

Рис.1. Класифікація порушників

Внутрішнім порушником може бути особа з наступних категорій співробітників:

– користувачі компанії;

– обслуговуючий персонал (системні адміністратори, адміністратори КМ, інженери, що обслуговують обладнання компанії);

– співробітники-програмісти, що супроводжують системне й прикладне програмне забезпечення;

– технічний персонал (робітники підсобних спеціальностей, прибиральниці), що працює в будинках, у яких розміщується обладнання компанії;

– інші співробітники підрозділів, що мають санкціонований доступ у будинки, де розташоване обладнання передачі й обробки інформації компанії.

Передбачається, що несанкціонований доступ на об'єкти компанії сторонніх осіб виключається організаційними мірами (охорона території, організація пропускного режиму) [3].

Припущення про кваліфікації внутрішнього порушника формулюються таким чином.

Внутрішній порушник:

– є висококваліфікованим фахівцем в області розробки й експлуатації програмного забезпечення й технічних засобів, знає специфіку завдань, розв'язуваних у мережі компанії, є системним програмістом, здатним програмно модифікувати роботу операційних, у тому числі мережних операційних систем;

– правильно представляє функціональні особливості роботи мережі компанії і закономірності формування в ній масивів інформації й потоків запитів до них;

– може використати тільки штатне обладнання й технічні засоби, наявні в складі компанії.

Внутрішні порушники підрозділяються на чотири категорії (від A до D) залежно від способу доступу й повноважень доступу.

Категорія А: Не зареєстровані мережі компанії особи, що мають санкціонований доступ у приміщення з обладнанням.

Особи, що ставляться до категорії А:

– можуть мати доступ до будь-яких фрагментів інформації про термінальне й серверне обладнання компанії і встановленому на них програмному забезпеченні;

– можуть мати у своєму розпорядженні будь-які фрагменти інформації про топологію мережі (комунікаційної частини підмережі) і про використовувані комунікаційні протоколи і їх сервісах.

Категорія В: зареєстрований користувач мережі компанії, що здійснює доступ до системи по КМ і з вилученого робочого місця. Особа, що ставиться до категорії В:

– знає щонайменше одне легальне ім'я доступу (спосіб доступу);

– має всі необхідні атрибути, що забезпечують доступ до мережі компанії (наприклад, паролем);

– має інформацію про топологію КМ компанії, технічних і програмних засобах обробки інформації у компанії;

– має можливість прямого (фізичного) доступу до фрагментів технічних засобів компанії.

Категорія С: зареєстрований користувач із повноваженнями системного адміністратора. Особа, що ставиться до категорії С:

– має всі можливості осіб категорії В;

– має повну інформацію про системному й прикладному програмному, забезпеченні компанії;

– має повну інформацію про технічні засоби й конфігурацію мережі компанії;

– має доступ до всіх технічних засобів обробки інформації й даним, має права конфігурування й адміністративного настроювання технічних і програмних засобів обробки інформації.

Категорія D: адміністратори обладнання (програмного забезпечення) компанії [2]. Особа, що ставиться до категорії D:

– має можливості внесення помилок, програмних "закладок", "троянських коней", вірусів у ПЗ компанії на стадії впровадження й супроводу ПЗ;

– може мати у своєму розпорядженні будь-які фрагменти інформації про топологію КМ компанії і технічних засобах обробки компанії.

Зовнішній порушник. Припущення про кваліфікації зовнішнього порушника формулюються таким чином:

– є висококваліфікованим фахівцем в області розробки й експлуатації програмного забезпечення й технічних засобів, знає специфіку завдань, розв'язуваних у мережі компанії, є системним програмістом, здатним програмно модифікувати роботу операційних, у тому числі мережних операційних систем ;

– знає мережне і канальне обладнання, протоколи передачі даних, використовуваних у компанії;

– знає особливості системного й прикладного програмного забезпечення, а також технічних засобів компанії;

– знає функціональні особливості роботи системи й закономірності формування в ній масивів інформації й потоків запитів до них.

Зовнішній порушник - це особи, що мають можливість впливати на мережу компанії і її ресурси тільки зовні. Зовнішні порушники діляться на дві категорії A и B.

Категорія A: всі користувачі компанії, які не входять в число внутрішніх користувачів компанії.

Категорія B: користувачі загальнодоступної мережі Internet.

В якості потенційного порушника кібербезпеки об'єкта захисту розглядатимемо особа або групу осіб, які перебувають або не перебувають у змові, які в результаті умисних або ненавмисних дій можуть реалізувати різноманітні загрози кібербезпеки, спрямовані на інформаційні ресурси

комп'ютерної мережі та завдати моральної та/або матеріальної шкоди інтересам власника інформації.

Як загроз інформаційній безпеці розглядаються базові загрози порушення конфіденційності та цілісності інформації, а також загроза відмови в обслуговуванні інфраструктури інформаційної системи. Зведена характеристика ймовірного порушника приведена в табл. 2.

Таблиця 1

Характеристика ймовірного порушника

Класифікація	Характеристика
За мотиву порушення ІС	Порушення загрози цілісності, конфіденційності, доступності в корисливих чи інших цілях
За рівнем інформованості та кваліфікації порушника	Порушник має високий рівень знань в області програмування та обчислювальної техніки, проектування і експлуатації автоматизованих інформаційних систем
	Порушник має достатні знання для збору інформації, застосування відомих експлойтів і написання власного програмного забезпечення для здійснення атаки
	Порушник не є авторизованим користувачем інформаційної системи
За місцем дії	Без безпосереднього (фізичного) доступу на територію об'єкта (зовнішній порушник). Порушник діє віддалено, через мережу Інтернет

Дослідження показують, що забезпечення кібербезпеки інформації об’єктів критичної інфраструктури держави є актуальною проблемою сьогодення і для її вирішення необхідно віднести наступні заходи:

– розробка нормативного, правового регулювання у сфері забезпечення кібербезпеки інформації в комп’ютерній мережі;

– визначення загроз кібербезпеки інформації і виявлення вразливостей в програмному і апаратному забезпеченні комп’ютерній мережі;

– оцінка реальної захищеності комп’ютерній мережі;

– розробка вимог по забезпеченню кібербезпеки інформації в комп’ютерній мережі;

– розробка та реалізація заходів по забезпеченню кібербезпеки інформації

в комп'ютерній мережі;

– підготовка фахівців в області забезпечення кібербезпеки інформації в комп'ютерній мережі;

– здійснення контролю і нагляду в галузі забезпечення кібербезпеки інформації в комп'ютерній мережі;

– здійснення інформаційного, матеріально-технічного і науково-технічного забезпечення кібербезпеки інформації в комп'ютерній мережі;

– запровадження відповідного управлінського впливу щодо забезпечення кібербезпеки інформації об'єктів комп'ютерній мережі.

Таким чином, на основі приведених вище результатів досліджень можливо сформулювати основні завдання, рекомендації та базові пропозиції щодо підходів до забезпечення кібербезпеки інформації, яка циркулює на об'єктах комп'ютерної мережі.

Список джерел:

1. Борисенко О. А., Бережна О. В., Новгородцев А. І., Сердюк В. В. & Яковлев М. М. (2019) "Система передачі та відображення інформації із захистом числових даних", Системи обробки інформації, вип. 2, с. 103 – 108.
2. Коломійцев, О., Третяк, В., Закіров, З., Кукобко, С., Калачова, В., & Мартовицький, В. (2020). Оптимізація завантаження файлів сховища даних в olap-файли на основі рангового підходу. InterConf, (25), 108-117. вилучено із https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/4300.
3. Кучернюк П. В., (2018) "Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні)", Мікросистеми, Електроніка та Акустика, т. 22, № 6(101), с. 64 – 70
4. Коломійцев, О., Рябуха, Ю., Калачова, В., & Третьяк, В. (2020). Аналіз методів і процедур шкального оцінювання в задачах прийняття рішень при проектуванні і супроводженні розподілених автоматизованих інформаційних систем. InterConf, (15). вилучено із https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/2309.

SCIENTIFIC EDITION

BN 978-5-798343-22
9 785798 343225

SCIENTIFIC COLLECTION «INTERCONF»

№ 2 (38) | December, 2020

The issue contains:

Proceedings of the 1st International Scientific and Practical Conference

SCIENCE, EDUCATION, INNOVATION: TOPICAL ISSUES AND MODERN ASPECTS

TALLINN, ESTONIA
16-18.12.2020

Contacts of the editorial office:

Scientific Publishing Center «InterConf»
E-mail: info@ interconf.top
URL: https://www.interconf.top

InterConf
Scientific Publishing Center