



Львівський державний університет
безпеки життєдіяльності



Львівська
міська
рада



softserve

Under Defense

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

30 листопада 2022 року

Міністерство освіти і науки України
Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет “Львівська політехніка”

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

30 листопада 2022 року

Львів
Растр-7
2022

УДК 351.746:007:004

I 74

Інформаційна безпека та інформаційні технології: збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. – Львів: Растр-7, 2022. – 380 с.

ISBN 978-617-8134-79-2

У збірнику опубліковано матеріали IV Міжнародної науково-практичної конференції “Інформаційна безпека та інформаційні технології”. На основі теоретичних та експериментальних досліджень представлено інноваційні підходи у сфері кібербезпеки та інформаційних технологій. Обговорено та запропоновано сучасні шляхи щодо захисту інформації як на особистому, так і на державному рівнях.

УДК 351.746:007:004

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

© Автори статей, 2022

© ЛДУ БЖД, 2022

© Видавництво “Растр-7”, 2022

ISBN 978-617-8134-79-2

РЕДКОЛЕГІЯ:

Мирослав КОВАЛЬ – д.пед.н., професор, ректор Львівського державного університету безпеки життєдіяльності з науково-дослідної роботи;

Василь ПОПОВИЧ – д.т.н., професор, т.в.о.проректора з науково-дослідної роботи, начальник навчально-наукового інституту цивільного захисту Львівського державного університету безпеки життєдіяльності;

Ростислав ТКАЧУК – д.т.н., професор, начальник кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Олександр ПРИДАТКО – к.т.н., доцент, начальник кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Валерій ДУДИКЕВИЧ – д.т.н., професор, завідувач кафедри захисту інформації Національного університету “Львівська політехніка”;

Володимир МАКСИМОВИЧ – д.т.н., професор, завідувач кафедри кафедри безпеки інформаційних технологій Національного університету “Львівська політехніка”;

Zbigniew KOKOSIŃSKI – dr hab. Inż., prof. PK kierownik Katedry Politechnika Krakowska im. Tadeusza Kościuszki;

Volodymyr SAMOTYY – prof. dr hab. inż., professor, Katedra Automatyki i Informatyki Politechnika Krakowska im. Tadeusza Kościuszki;

Sergii TELENYK – prof. dr hab. inż., professor, Department of automatic control and computer engineering Cracow University of Technology;

Володимир РОМАКА – д.т.н., професор, професор кафедри захисту інформації Національного університету “Львівська політехніка”;

Іван ОПРСЬКИЙ – д.т.н., професор, професор кафедри захисту інформації Національного університету “Львівська політехніка”;

Любомир СІКОРА – д.т.н., професор, професор кафедри автоматизованих систем управління Національного університету “Львівська політехніка”;

Наталя ЛИСА – д.т.н., доцент, доцент кафедри кафедри автоматизованих систем управління Національного університету “Львівська політехніка”;

Тетяна ГОВОРУЩЕНКО – д.т.н., професор, завідувач кафедри комп’ютерної інженерії та інформаційних систем Хмельницького національного університету;

Ольга МЕНЬШИКОВА – к.ф.-м.н., доцент, заступник начальника навчально-наукового інституту цивільного захисту Львівського державного університету безпеки життєдіяльності з навчально-наукової роботи;

Андрій Івануса – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валентина ЯЩУК – к.е.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Орест ПОЛОТАЙ – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валерія БАЛАЦЬКА – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Ігор МАЛЕЦЬ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Назарій БУРАК – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Ольга СМОТР – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Юрій БОРЗОВ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Роман ГОЛОВАТИЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Олександр ХЛЕВНОЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

онлайн. Для цього також можуть бути задіяні асинхронні елементи навчання, такі як онлайн курс та попередньо записані відео.

Корисним є досвід університету Маннгайм з впровадження гібридного формату навчання.

Підготовлені ними методичні рекомендації з планування гібридних занять, спілкування аудиторії та віртуального класу, поєднання синхронних та асинхронних методів взаємодії дозволять налагодити гібридний формат в наших умовах.

Таким чином, комбінація очних та дистанційних форм навчання, синхронної та асинхронної взаємодії дозволяє забезпечити безперервність фахової підготовки в умовах військового часу.

Інформаційні джерела

1. Навчальні ресурси СумДУ – URL: <https://elearning.sumdu.edu.ua/> (дата звернення: 09.11.2022)

2. The Teaching and Learning Center (ZLL) – URL: <https://www.uni-mannheim.de/en/teaching-and-learning-center-zll/> (дата звернення: 09.11.2022)

3. Каталог курсів URL: <https://portal2.uni-mannheim.de/> (дата звернення: 09.11.2022)

4. Білоус О.А. Впровадження моделі змішаного навчання при вивченні математичних дисциплін / Інженерні та освітні технології. 2020. –Т. 8. № 1. – С. 8–18. doi: <https://doi.org/10.30929/2307-9770.2020.08.01.01>.

УДК 378.147:004.4

ДОСЛІДЖЕННЯ ПРОБЛЕМАТИКИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ГЕЙМІФІКАЦІЇ У СИСТЕМУ ОСВІТИ

***Христина Мечус¹, Ольга Смотр¹,
Наталія Вовчиста², Марія Рашкевич²***

***¹Львівський державний університет безпеки життєдіяльності,
м. Львів, Україна***

***²Національний університет “Львівська політехніка”,
м. Львів, Україна***

Анотація. Робота присвячена дослідженню проблеми впровадження технологій гейміфікації у систему освіти. На підставі проведеного аналізу зроблені рекомендації щодо систематизації досліджено в цій царині, з використанням підходів машинного навчання та інструментарію інтелектуального аналізу даних.

Ключові слова: гейміфікація освіти, інструментарій гейміфікації, машинне навчання.

Abstract. *The paper is devoted to the study of the problem of introducing gamification technologies into the education system. Based on the analysis, recommendations were made for the systematization of research in this area, using machine learning approaches and tools intelligent data analysis.*

Keywords: *gamification of education, gamification tools, machine learning.*

Гейміфікація (ігровізація, геймізація, англ. gamification) – використання ігрових практик та механізмів у неігровому контексті з метою залучення кінцевих користувачів до розв’язання проблеми [1, 2]. Цей термін з’явився у 80-х роках ХХ сторіччя та був введений завдяки шаленій популярності багатокористувацької відеогри MUD1, що поєднувала елементи рольової гри, hack and slash, інтерактивної літератури та надавала змогу у режимі реального часу одночасно взаємодіяти декільком гравцям і спілкуватися при цьому у чаті. З початку 2010-х років ідея гейміфікації стала одним із ключових трендів мотивації персоналу у багатьох бізнес-структурах. Джейн Мак-Гонал у своїй книзі “Reality Is Broken: Why Games Make us Better and How they Can Change the World” спрогнозував, що до 2015 року ринок гейміфікації досягне \$15 млрд, й вона проникне в усі сфери людської діяльності, у тому числі й в освіту [3].

Можемо з певністю стверджувати, що прогноз Джейна Мак-Гонала справдився. Поступово процес гейміфікації (ігровізації) набув поширення в усіх сферах нашої життєдіяльності і, звісно ж, сфера сучасної освіти не стала винятком. У 2020 році експерти компанії Growth Engineering засвідчили, що гейміфікацію використовують понад 70% компаній зі списку компаній Global 2000 та в подальшому прогнозують, що глобальний ринок гейміфікації зросте до 30,7 мільярда доларів США до 2025 року при середньорічному темпі зростання (CAGR) у 27,4%. [4]. При цьому, на сьогоднішній день найбільше використовує гейміфіковані рішення роздрібна торгівля, займаючи 28,6% ринку, освіта ж слідує за нею як наступний за популярністю сектор [4].

Очевидно, що проблеми, впровадження елементів гейміфікації в освітній процес, не оминули зацікавленості вітчизняних та зарубіжних учених. Для прикладу, у своїх роботах Лі Шелдон (Lee Sheldon) досліджував використання прототипів багатокористувацької гри для створення навчальних курсів закладів освіти [5]; вплив ефекту ігор на мотивацію в навчанні, у своїх роботах розглядали Дональд Кларк (Donald Clark), Ничкало Н., Матяш Н., Смотр О. [6–9]; гейміфікацію як сучасний напрям вітчизняної освіти досліджували Переяславська С, Смагіна О. [10] та інші.

Проте, не зважаючи на значну кількість публікацій у цій царині, можемо стверджувати, що знання про те, як гейміфікувати діяльність відповідно до специфіки освітнього контексту, все ще обмежені. Інколи складається враження, що стрімкий процес впровадження гейміфікації у найрізноманітніших її проявах в освітній процес, випередив дослідників у розумінні її механізмів і методів. Адже різноманіття форм гейміфікації, реалізованих на сьогодні в освітньому процесі дійсно вражає. Для прикладу, наведемо лише частину найбільш популярних з них:

- гра, як інструмент психологічного впливу;
- гра, як інструмент отримання знання з окремих галузей;
- гра, як інструмент оволодіння практичними навичками;
- гра, як інструмент командної роботи
- гра, як інструмент для створення інновації;
- гра, як симуляція;
- гра як засіб дискусії;
- гра, як інструмент для досліджень тощо.

Однак, на сьогодні все ж не вистачає систематизованих та обґрунтованих досліджень щодо того, які елементи гри, у яких її проявах та для якого контингенту, можуть бути найбільш прийнятними, та за яких обставин стимулюватимуть бажану поведінку.

На нашу думку, одним з найперспективніших напрямків проведення таких досліджень є використання підходів машинного навчання та інструментарію інтелектуального аналізу даних. Для прикладу, на рис. 1 відображено, частину результатів багатокласової класифікації за допомогою AutoML (Pusaret) рівня адаптивності груп, до онлайн-гри, як симуляції.

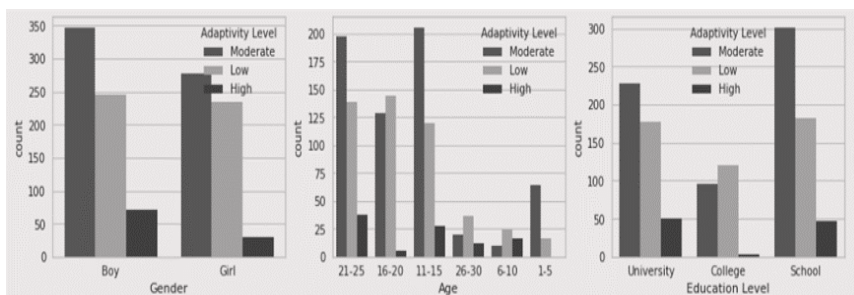


Рисунок 1. – Частина результатів Multiclass Classification AutoML

З наведеного рисунка видно, що найкращий рівень адаптивності у школярів, вікова категорія – 11-15 років, стать – чоловіча.

Інформаційні джерела

1. Huotari, K., & Hamari, J. (2012). Defining Gamification – A Service Marketing Perspective. Proceedings of the 16th International Academic MindTrek Conference 2012, Tampere, Finland, October 3–5.

2. Zichermann, Gabe; Cunningham, Christopher (August 2011). Introduction. Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps (вид. 1st). Sebastopol, California: O'Reilly Media. с. xiv. ISBN 1449315399.

3. Gartner Says By 2015, More Than 50 Percent of Organizations That Manage Innovation Processes Will Gamify Those Processes / Egham, UK, April 12, 2011. – [Електронний ресурс]. – Режим доступу : <http://www.gartner.com/newsroom/id/1629214>

4. 19 GAMIFICATION TRENDS FOR 2022-2025: TOP STATS, FACTS & EXAMPLES. [Електронний ресурс]. – Режим доступу: <http://www.british-legends.com/CMS/index.php/about-mud1-bl/history>

5. Sheldon, L. The Multiplayer Classroom: Designing Coursework as a Game / Sheldon, L., – 1 изд. – Boston: Course Technology, 2011. – 284 p.

6. Donald Clark. Learning Experience Design: How to Create Effective Learning that Works – Kindle... Edition. 1st. Publisher. Kogan Page. Publication date. November 3, 2021, 320 p.

7. Смотри О.О. Використання інструментарію інформаційних технологій для підвищення мотивації студента до навчання у форматі змішаної освіти / О. Смотри, М. Рашкевич, Р. Головатий, Х. Мечус // Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи : Збірник наукових праць. Випуск 6. / За ред. М. С. Ковалю, Н. Г. Ничкало. – Львів : ЛДУ БЖД, 2021. – С.214–217.

8. Купчак М.І. Тенденції та проблеми впровадження інформаційних технологій в управління університетом / М.І. Купчак, О.О. Смотри, М.Я. Купчак // Вісник Львівського державного університету безпеки життєдіяльності : зб. наук. праць. – Львів : Вид-во ЛДУ БЖД. – 2013. – № 7. – С. 28–32

9. Жолубак Л.В. Гейміфікація як інструмент підвищення мотивації студента донавчання / Л.В. Жолубак, Х.В. Мечус, О.О. Смотри // збірник матеріалів Десятої Міжнародної наукової конференції студентів та молодих вчених “Сучасні інформаційні технології – 2020” “Modern Information Technology – 2020” (14–15 травня 2020 р., м.Одеса) / МОН України; Одес. Нац. політех. ун-т ; Ін-т комп’ют. систем. Одеса : Наука і техніка, 2020. –с. 220–221.

10. Переяславська С. Гейміфікація як сучасний напрям вітчизняної освіти / С. Переяславська, О. Смагіна // Відкрите освітнє е-середовище сучасного університету. – 2019. – Вип. спецвип.. – С. 250–260.

З М І С Т

СЕКЦІЯ 1

КІБЕРБЕЗПЕКА

НАПРЯМ 1.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Sakovych B., Zharikova M. HYBRID ATTACK RISK ANALYSIS ...	5
Polishevskiy O., Pet'ko L. COMPUTER VIRUS: WHAT ARE COMPUTER VIRUSES?	8
Гавриленко І., Корякіна С. ІНФОРМАЦІЙНА БЕЗПЕКА	14
Гурник А., Ядченко Д. ДО ПИТАННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПРИ ОРГАНІЗАЦІЇ АЕРОМЕДИЧНОЇ ЕВАКУАЦІЇ	17
Іванова Д., Клєба А. НЕГАТИВНИЙ ВПЛИВ ІНФОРМАЦІЙНОЇ ПРОПАГАНДИ ТА ЗАХИСТ ВІД НЕЇ ПІД ЧАС ВІЙНИ	20
Івануса З., Івануса А. ТЕНДЕНЦІЇ РОЗВИТКУ НОРМАТИВНО-ПРАВОВОЇ БАЗИ УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ	24
Кушнірук М., Ящук В., Репетило Т. МЕТОДИ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ВЕБ-ДОДАТКІВ	27
Мних М.-М., Ткачук Р., Федина Б. ОРГАНІЗАЦІЯ ОПЕРАТИВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ КОМПАНІЇ	30
Лагун А., Небельський А. АНАЛІЗ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІТ ПІДПРИЄМСТВА	33
Ориник С., Ящук В., Навитка М. СИСТЕМА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	36
Пановик У., Кутас С., Брич Т. КЕРУВАННЯ БЕЗПЕКОЮ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ ІНДЕКСУ ДОВІРИ	39
Пасічник І., Полотай О., Брич Т. ДОСЛІДЖЕННЯ МЕТОДІВ ЗБОРУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ КІБЕРРОЗВІДКИ ТА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ З МЕТОЮ МОДЕЛЮВАННЯ ДІЙ ЗЛОВМИСНИКА	42
Полотай О., Меньшикова О. АНАЛІЗ МОТИВАЦІЇ ПОРУШНИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ В ЕЛЕКТРОННОМУ КУРСІ НАВЧАЛЬНОГО СЕРЕДОВИЩА	44

Порожній І., Отенко В., Лужецька Н. ВАЖЛИВІСТЬ ПРОВЕДЕННЯ ІТ-АУДИТІВ В УМОВАХ СЬОГОДЕННЯ	47
Рибальченко Л. ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ КРАЇНИ	49
Романчук Л., Гарасимчук О. ПІДВИЩЕННЯ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ В ОРГАНІЗАЦІЇ	52
Савуляк Д., Полотай О., Лагун А. СТВОРЕННЯ БЕЗПЕЧНОГО ЖИТТЄВОГО ЦИКЛУ РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	55
Сікора Л., Кунченко – Харченко В., Сабат В. ІГРОВІ І СИСТЕМНІ МОДЕЛІ МЕТОДІВ РОЗВ'ЯЗАННЯ КОНФЛІКТНИХ СИТУАЦІЙ ТА КІБЕРБЕЗПЕКА ІНФРАСТРУКТУРИ В УМОВАХ АКТИВНИХ ЗАГРОЗ	58
Смик Д., Ткачук Р., Івануса А. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ІТ – ПРОЄКТІВ З ВИКОРИСТАННЯМ МЕТОДИКИ DEVSECOPS	61
Фединець Н. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА НА ОСНОВІ СУЧАСНИХ ТЕХНОЛОГІЙ АУТЕНТИФІКАЦІЇ	64
Ящук В., Ткачук Р., Івануса А. ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	67

НАПРЯМ 2.

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Василишин С., Опірський І. СИСТЕМА ЕЛЕКТРОННОГО УПРАВЛІННЯ НА ОСНОВІ БЛОКЧЕЙНУ	70
Дебре В., Гречинкін Д. ПІДВИЩЕННЯ РІВНІВ БЕЗПЕКИ КОРИСТУВАЦЬКИХ ДАНИХ ЗА ДОПОМОГОЮ ПЕРЕХОДУ НА HTTPS ПРОТОКОЛ ПЕРЕДАЧІ ДАНИХ	73
Лаврик Т., Кіхтенко Д. СТВОРЕННЯ ФІКТИВНИХ ВЕБСЕРВЕРІВ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ КІБЕРБЕЗПЕКИ	76
Пашук В., Жуковицький І. ВИКОРИСТАННЯ МЕХАНІЗМІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АУТЕНТИФІКАЦІЇ ВАНТАЖНИХ ЗАЛІЗНИЧНИХ ВАГОНІВ	78
Петько С. РОЛЬ ЦЕНТРІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЗАХИСТІ ІТ-ІНФРАСТРУКТУРИ КОМПАНІЙ	81
Побережник В., Опірський І. АНАЛІЗ ЗАГРОЗ ПРИВАТНОСТІ У ПРОГРАМАХ МИТТЄВОГО ОБМІНУ ПОВІДОМЛЕННЯМИ НА ПРИКЛАДІ ПОПУЛЯРНИХ МЕСЕНДЖЕРІВ В УКРАЇНІ	84

Толкачова А., Гарасимчук О. БЕЗПЕЧНА РЕАЛІЗАЦІЯ ПРОТОКОЛУ OAuth 2.0.	87
Фарбінник В., Полотай О. МЕТОДИ ЗАХИСТУ ВІД DDOS-АТАК НА ВЕБ-СЕРВІСИ	89
Шасц Є., Лунгол О. ВИКОРИСТАННЯ ХАНПОТІВ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК	93

НАПРЯМ 3.

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Дорожинський С. АНАЛІЗ ПРОТОКОЛІВ КВАНТОВОГО ПРЯМОГО БЕЗПЕЧНОГО ЗВ'ЯЗКУ	96
Рудик А., Рудик Ю., Фединець Н. КІБЕРЗАХИСТ В ІНТЕГРОВАНИХ СИСТЕМАХ САНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ	99
Смілевський М. ДО ПИТАННЯ ПЕРЕВАГ СИСТЕМ ВІДЕОНАГЛЯДУ У ГРОМАДСЬКИХ МІСЦЯХ	102
Стефанів Т., Ткачук Р., Балацька В. ВПРОВАДЖЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕХНОЛОГІЯХ РОЗУМНОГО БУДИНКУ	105
Тичина Ю., Ящук В., Полотай О. МОДЕЛЬ СИСТЕМИ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	108
Філіпчук Б., Ткачук Р., Репетило Т. ПОТЕНЦІЙНІ ВРАЗЛИВОСТІ БРАНДМАУЕРА	111

НАПРЯМ 4.

БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

Rapovuk Ulyana, Sharadze A. THE GROWTH OF CLOUD COMPUTING IN THE EDUCATIONAL PROCESS UNDER TODAY'S CONDITIONS	115
Горон В., Полотай О., Пановик У. БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ	118
Гумен О., Селіна І., Василенко А. ЗБЕРЕЖЕННЯ КРЕСЛЕНИКІВ У ВЕКТОРНІЙ ГРАФІЦІ	120
Дацків Н., Полотай О. ОСНОВНІ ПРОБЛЕМИ БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ	123
Клочков В., Вахула А., Горак І. ЗАСОБИ ЗАХИСТУ ДАНИХ У ВЕБ-СИСТЕМАХ	127
Пожичкевич К., Ящук В., Фединець Н. МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПРОЄКТУВАННІ WEB-ДОДАТКА УНІВЕРСИТЕТУ	130

Рошинець І., Ящук В., Федина Б. АКТУАЛЬНІСТЬ ВИКОРИСТАННЯ ВІРТУАЛЬНИХ ТА ХМАРНИХ ТЕХНОЛОГІЙ	133
Чурілова А., Прокопов С. ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАННИХ В ЕЛЕКТРОННОМУ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ	136

Напрямок 5.

**КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ
ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ**

Антонюк В., Сидорова М. ЗАСТОСУВАННЯ СТЕГАНОГРАФІЇ ДЛЯ ЗАХИСТУ ПРОГРАМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ	140
Кіх М., Шабатура М. ДОСЛІДЖЕННЯ НАБОРУ СТАТИСТИЧНИХ ТЕСТІВ TESTU01 ДЛЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ	143
Овчинікова К., Полотай О., Лагун А. КРИПТОГРАФІЧНІ ТА СТЕНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ	146

Напрямок 6.

ІНФОРМАЦІЙНІ ВІЙНИ

Pohorila V., Klyumenko D. POSSESSION OF ACCOUNTS OF UKRAINIANS IN MESSAGING SERVICE	149
Басій Н., Коник М. ГОЛОВНІ ОСОБИСТОСТІ РОСІЙСЬКОЇ ІНФОРМАЦІЙНОЇ ВІЙНИ ПРОТИ УКРАЇНИ: ДУГІН	151
Івкова В. КІБЕРПОЛІЦІЯ: РОБОТА В УМОВАХ ВІЙНИ	154
Лозинський О. ІДЕОЛОГІЧНЕ ОБҐРУНТУВАННЯ ЗБРОЙНОЇ СПЕЦОПЕРАЦІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ	156
Любчак В., Підлісна А. ЛАНДШАФТ КІБЕРЗАРОЗ ТА ТРЕНДИ 2022 РОКУ	159
Пінчук А., Одарченко Р., Самойленко В., Дика Т. РОСІЙСЬКО-УКРАЇНСЬКА КІБЕРВІЙНА: ДОСЛІДЖЕННЯ ДІЯЛЬНОСТІ ІТ ВІЙСЬКА УКРАЇНИ	162
Самойленко В., Одарченко Р., Пінчук А., Лавриненко О. РОСІЙСЬКО-УКРАЇНСЬКА КІБЕРВІЙНА: ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ ТА ПРОПАГАНДОЮ ...	165
Федорова Н. АВТОРСЬКЕ ПРАВО ЧЕРЕЗ ПРИЗМУ ВОЄННОГО СТАНУ В УКРАЇНІ	168
Чупахін А., Корякіна А. ІНФОРМАЦІЙНІ ВІЙНИ ТА ЇХ ВПЛИВ НА СУСПІЛЬСТВО	171

Секція 2

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

НАПРЯМ 7.

ПРИКЛАДНЕ ТА СИСТЕМНЕ ПРОГРАМУВАННЯ

Bondarenko V., Sydorova M. DEVELOPMENT OF SOFTWARE FOR COUNTING THE NUMBER OF REPETITIONS OF PHYSICAL EXERCISES WITH VOICE CONTROL	175
Hembara N. “TEMPERATURKA BOT”: A CHAT-BOT IS LAUNCHED THAT HELPS MONITOR YOUR HEALTH	178
Vakulchuk S., Sydorova M. RESEARCH OF THE PROBLEM AND CREATION OF A WEB-BASED DECISION SUPPORT APPLICATION BASED ON EXPERT EVALUATION	181
Головата О., Попитак С., Навитка М. ДОСЛІДЖЕННЯ СУЧАСНИХ АСПЕКТІВ КЛАСИФІКАЦІЇ ДОДАТКІВ	184
Гриченко Д., Синиця О., Навитка М. АНАЛІЗ ВЕРТИКАЛІ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	186
Гречка А, Науменко Н. ПРОГРАМНИЙ МОДУЛЬ НЕПРЯМИХ МЕТОДІВ ПОБУДОВИ ФУНКЦІЙ НАЛЕЖНОСТІ	188
Івануса А., Репетило Т., Кашуба Д. ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОЄКТАХ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ ПРИ РОЗРАХУНКУ ЧАСУ ЕВАКУАЦІЇ ЛЮДЕЙ .	191
Навитка М., Стецик К., Івануса А. НАЙВАЖЛИВІШІ ПЕРЕВАГИ СУЧАСНИХ ФРЕЙМВОРКІВ ДЛЯ ПОБУДОВИ WEB-ДОДАТКІВ ..	194

НАПРЯМ 8.

МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Бойко В., Бурак Н. СУЧАСНІ ПІДХОДИ ВИРІШЕННЯ ПРОБЛЕМ ПЕРЕВАНТАЖЕННЯ СЕРВЕРІВ	196
Герговський О., Буряк Н. АНАЛІЗ ФУНКЦІОНАЛЬНИХ ОСОБЛИВОСТЕЙ КОМУТАТОРІВ LAYER 2 ТА LAYER 3	199
Дудикевич В., Микитин Г., Галунець М., Кутень Р. КІБЕРФІЗИЧНА СИСТЕМА “РОЗУМНИЙ ДІМ”: СТРУКТУРА – ЗАГРОЗИ – БЕЗПЕКА	202

Карлінський Я., Гавриць А. ПЕРЕВАГИ ТА НЕДОЛІКИ НОВОЇ СИСТЕМИ ОПОВІЩЕННЯ ПРО НАДЗВИЧАЙНІ СИТУАЦІЇ	205
Павлишин А., Полотай О. СТВОРЕННЯ СИСТЕМИ АНАЛІЗУ МЕРЕЖЕВИХ АТАК НА БАЗІ МАШИНОГО НАВЧАННЯ	208
Пахомова В. ОРГАНІЗАЦІЯ МАРШРУТИЗАЦІЇ В MPLS ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ З ВИКОРИСТАННЯМ НЕЙРОМЕРЕЖНИХ ТЕХНОЛОГІЙ	212
Придатко О., Борзов Ю., Придатко В., Дідушок С. МОДЕЛЮВАННЯ СИСТЕМИ МАРШРУТИЗАЦІЇ ОПЕРАТИВНОЇ ІНФОРМАЦІЇ З МІСЦЯ НАДЗВИЧАЙНОЇ ПОДІЇ	215

НАПРЯМ 9.

3D МОДЕЛЮВАННЯ ТА 3D ДРУК

Гумен О., Селіна І., Глеба Д. 3D ЛАЗЕРНЕ СКАНУВАННЯ В МОДЕЛЮВАННІ ОБ'ЄКТІВ БУДІВНИЦТВА	218
Хлевной О., Райга Д. ЗГОРТКОВА НЕЙРОННА МЕРЕЖА ДЛЯ ВИЗНАЧЕННЯ ГРУП МОБІЛЬНОСТІ УЧАСНИКІВ ЗА ДАНИМИ КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ	221

НАПРЯМ 10.

МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СИСТЕМ

Muliarevych O. THE MODEL OF AUTOMATED WAREHOUSE DESIGN SYSTEM	224
Гембара Т. МАТЕМАТИЧНІ МЕТОДИ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ВІЗУАЛІЗАЦІЇ ФАЗОВО-ЧАСТОТНИХ ХАРАКТЕРИСТИК АКУСТИЧНИХ СИГНАЛІВ	228
Карабин О., Кусій М., Яницький Р. МАТЕМАТИЧНА МОДЕЛЬ ТЕМПЕРАТУРНОГО ПОЛЯ РУХОМОГО ОБ'ЄКТА	231
Рудаков С., Рудаков І. КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ МЕТОДУ БАГАТОКАНАЛЬНИХ ВИМІРЮВАНЬ ДЛЯ СИСТЕМ КОНТРОЛЮ ТА ПОПЕРЕДЖЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ	234
Смаковська Г. ІНФОРМАЦІЙНІ МОДЕЛІ СПІВРОЗМІРНОСТІ ПОВЕРХОНЬ ТЕНТОВИХ КОНСТРУКЦІЙ	237

НАПРЯМ 11.**ОРГАНІЗАЦІЯ БАЗ ДАНИХ І ЗНАТЬ**

Melnyk Y., Pet'ko L. THE BIRTH OF THE INFORMATION AGE: PAUL OTLET	240
Аль Хадж Р. ЗАСТОСУВАННЯ АДАПТИВНИХ СЕМАНТИЧНИХ АНАЛІЗАТОРІВ ПРИ ДИНАМІЧНІЙ ОБРОБЦІ ВЕЛИКИХ ОБСЯГІВ ТЕКСТОВОЇ ІНФОРМАЦІЇ	254
Медяник Є. ОБРОБКА ВЕЛИКИХ ДАНИХ ДЛЯ ПРОГНОЗУВАННЯ ОБСЯГУ АКЦІЙ ЗА ДОПОМОГОЮ ІНСТРУМЕНТІВ DEEP LEARNING	256
Стасьо О., Бурак Н. ДОСЛІДЖЕННЯ ПРОБЛЕМ ОБРОБКИ НЕСТРУКТУРОВАНИХ ДАНИХ	260

НАПРЯМ 12.**ТЕХНОЛОГІЇ ВІЗУАЛІЗАЦІЇ ДАНИХ**

Дам-Васильєва Чанг А., Ріпний В. ВІЗУАЛІЗАЦІЯ ДАНИХ	263
Кузик О., Придатко О., Бурак Н. АНАЛІЗ ЗАСОБІВ ТА СИСТЕМ ОПТИЧНОГО ДОСЛІДЖЕННЯ ПРОСТОРУ	266
Мельникова І., Бойко Д. ВІЗУАЛІЗАЦІЯ ГЕОГРАФІЧНИХ ДАНИХ ДЛЯ ПОТРЕБ НАСЕЛЕННЯ	268
Плотніков М., Рудніченко М., Шибасва Н. ВИКОРИСТАННЯ ВЕБ-ЗАСТОСУВАННЯ ДЛЯ ВІЗУАЛІЗАЦІЇ ОБРОБЛЕНИХ ДАНИХ ДЛЯ ВІРУСНИХ ЗАХВОРЮВАНЬ НА ПРИКЛАДІ COVID-19 .	272
Семчук І. РОЗРОБКА ОДНОСТОРІНКОВОГО ВЕБЗАСТОСУНКУ З ЕЛЕМЕНТАМИ ВЕБСКРАПІНГУ ТА ВІЗУАЛІЗАЦІЇ ГЕОПРОСТОРОВИХ ДАНИХ ЗАСОБАМИ RUTRON	275

НАПРЯМ 13.**ОПЕРАЦІЙНІ СИСТЕМИ**

Makeyeva K., Pet'ko L. AMERICAN COMPANY “THE MICROSOFT CORPORATION”	278
Балацька В., Брич Т., Полотай О. ОСОБЛИВОСТІ ПОТРЕБ У ЗАХИСТІ ОПЕРАЦІЙНИХ СИСТЕМ	286
Балацька В., Полотай О., Пузир А. АВТЕНТИФІКАЦІЯ, ЯК ОДИН З МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОПЕРАЦІЙНИХ СИСТЕМ	288
Проценко П., Гавриленко І. ВИДИ ОПЕРАЦІЙНИХ СИСТЕМ ...	291

НАПРЯМ 14.**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ ПРОЄКТАМИ**

Panovyk R., Ardon C. CYBER SECURITY IN BUSINESS PROCESSES	294
Антіпенко А., Басюк Т. ІНФОРМАЦІЙНА СИСТЕМА ДИСТАНЦІЙНОГО МОНІТОРИНГУ КЛІМАТИЧНИХ УМОВ	297
Беген Д., Ємельяненко С. БЕЗПЛОТНІ ЛІТАЛЬНІ АПАРАТИ ДЛЯ ПІДВИЩЕННЯ ФУНКЦІОНУВАННЯ КРИЗОВОГО ЦЕНТРУ ЦИВІЛЬНОГО ЗАХИСТУ	300
Гончар В., Мартинюк Г. АНАЛІЗ МЕТОДИК ТА ПРИСТРОЇВ СКАНУВАННЯ РАЙДУЖНОЇ ОБОЛОНКИ ОКА ДЛЯ ВИКОРИСТАННЯ В ГАЛУЗІ ПАСАЖИРСЬКИХ ПЕРЕВЕЗЕНЬ	303
Кокотко Б., Придатко О., Головатий Р. ОБГРУНТУВАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ ЩОДО МАТЕРІАЛЬНОГО ЗАБЕЗПЕЧЕННЯ СПЕЦІАЛІЗОВАНИХ ФОРМУВАНЬ	306
Мантуленко О., Бабаджанова О. ВЕБ-РОЗРОБКА “BUSINESS INTELLIGENCE” ЗАСОБІВ	309
Недільська М., Суринович О. ЧАТ-БОТИ ЯК ЗАСОБИ СПІЛКУВАННЯ ІЗ КОРИСТУВАЧЕМ	312
Pavliuk O., Lysa N., Fedina B. КОГНІТИВНІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ В УМОВАХ РИЗИКУ	316
Погуда Н. СУЧАСНІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ТУРИЗМІ	320

НАПРЯМ 15.**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ**

Vlasiuk R. Pet'ko L. ALAN TURING: A FOUNDING FATHER OF COMPUTER SCIENCE, ARTIFICIAL INTELLIGENCE AND MODERN COGNITIVE SCIENCE	323
Гелешко І., Ящук В. СУЧАСНІ ТЕНДЕНЦІЇ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ ПІДГОТОВЦІ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ	339

Гончаров Д., Мєшков Д. ІНФОРМАТИЗАЦІЯ ОСВІТИ	342
Гончарова І. ЦИФРОВІЗАЦІЇ ОСВІТНЬОЇ ДІЯЛЬНОСТІ ЗАКЛАДІВ ПРОФЕСІЙНОЇ ОСВІТИ	345
Коваль І. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ ЗВО ДСНС УКРАЇНИ	348
Любчак В., Мартинова Н. ОРГАНІЗАЦІЯ НАВЧАННЯ СТУДЕНТІВ ЗА ЗМІШАНИМ ФОРМАТОМ З УРАХУВАННЯМ ДОСВІДУ УНІВЕРСИТЕТУ З НІМЕЧЧИНИ	351
Мечус Х., Смотр О., Вовчаста Н., Рашкевич М. ДОСЛІДЖЕННЯ ПРОБЛЕМАТИКИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ГЕЙМІФІКАЦІЇ У СИСТЕМУ ОСВІТИ	353
Мєшков Д., Гончаров Д. РОЗВИТОК ТЕХНОЛОГІЙ ОСВІТИ	357
Рижиков В., Юрков А. СУТЬ ТА ПРАКТИЧНЕ ЗНАЧЕННЯ ЗАПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТНІЙ ПРОЦЕС ВИЩИХ ВІЙСЬКОВИХ НАВЧАЛЬНИХ ЗАКЛАДІВ В СУЧАСНИХ УМОВАХ ВІЙСЬКОВОГО СТАНУ	360
Трусевич О. ВІРТУАЛЬНЕ НАВЧАННЯ В УМОВАХ СЬОГОДЕННЯ: АНАЛІЗ, ТЕНДЕНЦІЇ, ПЕРСПЕКТИВИ	362
Філіппова В., Гаврись А. ОСОБЛИВОСТІ ПІДГОТОВКИ ОПЕРАТОРІВ БЕЗПЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ	365
Юденкова О. ЦИФРОВА КОНТЕНТНА ТВОРЧІСТЬ ЯК ВАЖЛИВА СКЛАДОВА ДИДЖИТАЛІЗАЦІЇ ОСВІТИ	368

Наукове видання

**ІНФОРМАЦІЙНА БЕЗПЕКА
ТА ІНФОРМАЦІЙНІ
ТЕХНОЛОГІЇ**

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

Відповідальні за випуск **Ростислав ТКАЧУК**
Олександр ПРИДАТКО

Оригінал-макет **Ростислав ТКАЧУК,**
Андрій ІВАНУСА

Видано в авторській редакції

Підписано до друку 30.11.2022 р.
Формат 60×84/16. Папір офсетний. Друк цифровий.
Умовн. друк. арк. 22,09. Обл.-вид. арк. 20,55.
Наклад 100 прим.

Видавець і виготовлювач: ТОВ “Растр-7”
79005, м. Львів, вул. Кн. Романа, 9/1.
Тел./факс: (032) 235 72 13. E-mail: rastr.sim@gmail.com
www.rastr-7.com.ua

Свідоцтво суб'єкта видавничої справи
ЛВ № 22 від 19.11.2002 р.

1 0 1 0 1



IV International Scientific and Practical Conference CYBERSECURITY AND INFORMATION TECHNOLOGY

CIT 2022

November 30 - 2022 Lviv - Ukraine

1 0 1 0 0 0 1 1 0 1 0 1



PACTP-7

ISBN 978-617-8134-79-2



9 786178 134792