

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

24 листопада 2023 року



**З НАГОДИ 5-Ї РІЧНИЦІ ЗАСНУВАННЯ
ФАКУЛЬТЕТУ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

КІБЕРПРОСТІР В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: ТЕОРІЯ ТА ПРАКТИКА

**МАТЕРІАЛИ
МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРПРОСТІР В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: ТЕОРІЯ ТА ПРАКТИКА

**МАТЕРІАЛИ МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

24 листопада 2023 року, м. Одеса

Одеса, 2023

УДК 340.12:316.3

ББК 67.0

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій,
кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу
несуть учасники конференції, їхні наукові керівники,
які рекомендували ці матеріали до друку.

Друкується згідно з наказом ректора
Національного університету «Одеська юридична академія»
(№ 3449-62 від 19.10.2023 р.)

Матеріали Міжнародної науково-практичної конференції «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика» (м. Одеса, 24 листопада 2023 р.). Одеса, 2023. 301 с.

Міжнародна науково-практична конференція «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика» присвячена 5-ї річниці заснування факультету кібербезпеки та інформаційних технологій.

До участі у конференції запрошені студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

Шановні учасники міжнародної науково-практичної конференції «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика»!

В епоху стрімких змін та викликів кіберпростір став невід'ємною частиною людського життя, але разом з тим він приносить нові загрози та виклики, особливо в умовах війни та глобальних криз. Він вражає своєю багатогранністю та охоплює не тільки технологічні питання, а й соціально-психологічні, нормативно-правові, управлінські та інші аспекти.

Кожен з напрямів досліджень кіберсередовища є багатовекторним і всі вони є взаємопов'язаними. Кібербезпека та захист інформації є основою сучасного суспільства, адже кібератаки завдають значних збитків, як приватним компаніям, так і державним установам. Тому фахівці у галузі кібербезпеки повинні мати глибокі знання та навички не тільки в сфері технічного захисту інформації, але й в інших областях, таких як: законодавство у сфері кібербезпеки; економіка кібербезпеки; психологія кібербезпеки; організаційні аспекти кібербезпеки.

На рівні суспільства зміни в кіберсередовищі приносять, як користь, виявлену в забезпеченні прав людей на інформацію та задоволенні їхніх інформаційних потреб, так і потенційні ризики, пов'язані з неправомірним використанням інформації та шкодою інформаційним правам та інтересам осіб. У період воєнних дій особливо актуальними стають проблеми вибору достовірної інформації та запобігання неконтрольованому розповсюдженню інформації.

В умовах війни інформаційно-комунікаційні системи також переживають значні трансформації. Особливої уваги заслуговує сегмент Military Technologies, що зосереджується на підсиленні оборонних можливостей нашої держави.

Не менш важливою є роль правових принципів у регулюванні кібернетичного простору, тому актуальним є питання вдосконалення законодавчої бази, що викликає зростаючий інтерес серед юридичної наукової спільноти. Окрім того, кібертехнології мають значний вплив на управлінські процеси, соціальну взаємодію та психологічний стан людей у сучасному світі.

В цілому, більшість сучасних питань прямо чи опосередковано пов'язані з інформаційними технологіями та кіберпростіром. Одеса входить до числа лідерів у цій галузі, маючи всі необхідні умови для розвитку: матеріально-технічну базу, високий науковий потенціал, значний кадровий ресурс та розвинену ІТ спільноту.

Ми сподіваємося на подальшу плідну роботу, продуктивний обмін знаннями, ідеями та досвідом щодо подальшого розвитку кіберпростору в умовах війни та глобальних викликів сьогодення.

*Президент Національного університету
“Одеська юридична академія”,
академік НАПрН України, академік НАПН України
доктор юридичних наук, професор,
Заслужений юрист України*

Сергій КІВАЛОВ

СЕКЦІЯ 2. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В УМОВАХ ВІЙНИ

АНАЛІЗ ПОТЕНЦІЙНИХ ВИТОКІВ ДАНИХ В ПРИСТРОЯХ КОМУНІКАЦІЇ

Задерейко Олександр

доцент кафедри інформаційних технологій, факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Логінова Наталія

завідувач кафедри інформаційних технологій, факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», кандидат педагогічних наук, доцент

Троянський Олександр

директор інституту інформаційної безпеки, радіоелектроніки та телекомунікацій Національного університету «Одеська політехніка», кандидат технічних наук, доцент

Переважна більшість користувачів не можуть відмовитися від використання засобів комунікації інтегрованих в глобальну мережу Інтернет. Внаслідок цього, повністю виключити витoki конфіденційних даних користувачів не є можливим. Найбільш поширеним способом запобігання витоків конфіденційних даних користувачів є різні способи моніторингу і подальшого контролю мережевого трафіку пристроїв комунікації.

Тому актуальним завданням є виявлення ймовірних витоків конфіденційних даних, заснованих на методиках (алгоритмах) їх виявлення і подальшого блокування. Рішення цього завдання може бути реалізовано з використанням моніторингу всього мережевого трафіку пристроїв комунікації користувачів і подальшому виявленні в ньому даних, які можна віднести до конфіденційних (або надлишкових) і даних, що передаються в незашифрованому вигляді [1].

На практиці організація моніторингу мережевого трафіку пристроїв комунікації може бути виконана з використанням спеціалізованого програмного забезпечення – сніферів [2]. Реалізація такого підходу дозволяє виконувати детальний аналіз протоколів мережевого трафіку (на рівні пакетів) пристроїв комунікації на предмет наявності з'єднань, які можуть призвести до потенційних витоків даних, керуючись нижче наведеною методикою (рис. 1).

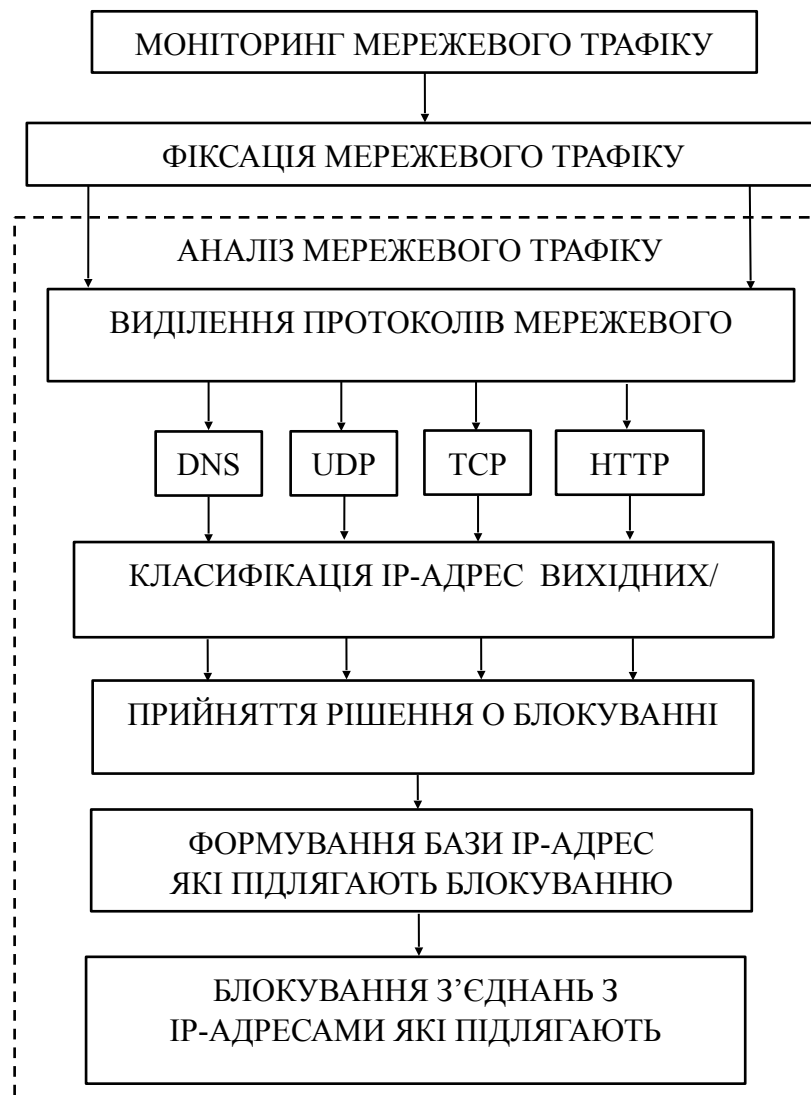


Рис. 1. Методика захисту пристроїв комунікації від потенційних витоків конфіденційних даних.

Завдання аналізу і класифікації трафіку, який може бути віднесений до конфіденційних даних з пристрою комунікації слід вирішувати, ґрунтуючись на таких критеріях [3]:

1. Заборону вихідних/вхідних з'єднань з сервісами інтернет статистики [4];
2. Заборону незахищених вихідних/вхідних з'єднань системного і прикладного програмного забезпечення, що здійснюються через всі порти, крім 443 (з обов'язковою перевіркою збереження його функціональності, після блокування);
3. Заборону вихідних/вхідних з'єднань необхідно виконувати на (L4) і (L7) рівнях моделі OSI (табл. 1) [5].

Таблиця 1. Модель OSI з розкладкою протоколів за рівнями

Рівень (L)	Назва	Протоколи
1	Application	SSH, HTTP, FTP, LPD, SMTP, TELNET, TFTP, EDI, POP3, IMAP, SNMP, NNTP, S-RPC, SET
2	Presentation	Encryption protocol types and format, such as ASCII, EBCDICM, TIFF, JPEG, MPEG, MIDI
3	Session	SMB, RPC, NFS, SQL
4	Transport	SPX, SSL, TLS, TCP, UDP
5	Network	ICMP, RIP, OSPF, BGP, IGMP, IP, IPSec, IPX, NAT, SKIP
6	Data link	ARP, SLIP, PPP, L2F, L2TP, PPTP, FDDI, ISDN
7	Physical	EIA/TIA-232, EIA/TIA-449, X. 21, HSSI, SONET, V. 2.4, V. 35, BLUETOOTH, 802.11, ETHERNET

Практична реалізація заборони вихідних/вхідних з'єднань повинна бути здійснена з використанням стандартних міжмережевих екранів і/або міжмережевих екранів нового покоління класу NGFW [6]. Такі міжмережеві екрани, дозволяють здійснювати глибоку фільтрацію трафіку, засновану на роботі засобів аналізу на рівні додатків (L7), таким чином, що "вміст" кожного пакета аналізується, починаючи від рівня L3 та закінчуючи рівнем L7 моделі OSI, у тому числі пакети, що містять зашифрований SSL(TLS) трафік.

Висновки

Апробація запропонованого підходу заснованого на аналізі мережевого трафіку на різних стаціонарних і мобільних пристроях комунікації дозволила ефективно виявляти і блокувати збір конфіденційних даних користувачів, що дозволило знизити ймовірність витоку їх конфіденційних даних.

Список використаних джерел:

1. ACSAC '10: Proceedings of the 26th Annual Computer Security Applications Conference. December 2010. Pages 261–269. DOI: <https://doi.org/10.1145/1920261.1920300>.
2. Pughazhendhi K. Amutha N. Packet sniffer. URL: https://www.irjmets.com/uploadedfiles/paper/issue_3_march_2023/35048/final/fin_irjmets1680097820.pdf/. (Дата звернення 6.11.2023).
3. Задерейко О.В., Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Кухаренко С.В. [Аналіз витоків даних у інформаційних системах](#). Сучасна спеціальна техніка. № 3 (66), 2021, С. 16-30. URL: <http://dspace.onua.edu.ua/handle/11300/23298>.

4. Zadereyko O., Trofymenko O., Prokop Y., Loginova N., Dyka A., Kukharenko S. [Research of potential data leaks in information and communication systems.](#) Radioelectronic and Computer Systems. 2022. No 4. P.64-84. DOI: <https://doi.org/10.32620/reks.2022.4.05>. URL: https://dSPACE.onua.edu.ua/bitstream/handle/11300/23361/doslidjena_potenciynuh_vutokiv_danuh.pdf.
5. Задерейко О.В., Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Кухаренко С.В. Дика А.І. [Захист даних користувачів в інформаційних системах.](#) Сучасна спеціальна техніка. № 1 (68), 2022, С. 23-33. URL: <https://hdl.handle.net/11300/23313>.
6. Know, what you need to. "Defining the Next-Generation Firewall." (2009). URL: <https://media.paloaltonetworks.com/documents/Gartner-NGFW-Research-Note.pdf>. (Дата звернення 6.11.2023).

Ключові слова: пристрої комунікації, аналіз протоколів мережевого трафіку, аналіз пакетів мережевого трафіку, аналіз витоків даних, конфіденційні дані користувачів, моніторинг мережевого трафіку, міжмережевий екран, міжмережевий екран NGFW, глибока фільтрація трафіку, база конфіденційних даних, база IP адрес, блокування з'єднань

Keywords: communication devices, network traffic protocol analysis, network traffic packet analysis, data leak analysis, confidential user data, network traffic monitoring, firewall, NGFW firewall, deep traffic filtering, confidential data database, IP address database, connection blocking

ЗМІСТ

ПЕРЕДМОВА	4
<i>Секція 1. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ ЯК ОСНОВА СУЧАСНОГО СУСПІЛЬСТВА.....</i>	<i>6</i>
ТЕНДЕНЦІЇ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ: СУЧАСНІ ВИКЛИКИ	
Дикий Олег	6
<i>РОЛЬ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ В СЬОГОДЕННІ: ПРОБЛЕМАТИКА, ВИКЛИКИ ТА ЗАХОДИ ЗАХИСТУ</i>	
Ісмайлов Карен	8
АНАЛІЗ СУЧАСНИХ СТЕГANOГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ	
Самойлов Станіслав	11
ДОСЛІДЖЕННЯ АЛГОРИТМУ ФОРМУВАННЯ СТЕГANOГРАФІЧНОГО КЛЮЧА ДЛЯ ПОБУДОВИ ЗМІННИХ КРИПТОГРАФІЧНИХ S-БЛОКІВ	
Ахмамет'єва Ганна	13
ВПЛИВ КІБЕРЗАГРОЗ НА ЕФЕКТИВНІСТЬ УПРАВЛІННЯ ПІДПРИЄМСТВОМ	
Пунченко Наталія, Златова Марія.....	17
СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ	
Кухаренко Сергій.....	21
ДОСЛІДЖЕННЯ КІБЕРЗАГРОЗ ТА ОЦІНКА РИЗИКІВ КІБЕРБЕЗПЕКИ ЗАСОБАМИ PYTHON / JUPYTERLAB	
Бойко Віктор.....	24
ОГЛЯД МЕТОДІВ ВБУДОВУВАННЯ ІНФОРМАЦІЇ В ЗВУКОВІ ФАЙЛИ	
Овчинников Микола.....	27
УРАЗЛИВОСТІ СТЕКА ХАМРР	
Стаднік Денис.....	30
ТЕХНОЛОГІЇ ПРИХОВУВАННЯ ПРИСУТНОСТІ В СИСТЕМІ	
Соловйов Артем.....	33
БЕЗПЕЧНЕ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ БОЙОВИХ ДІЙ	
Спесівцев Микола	35

ВИДИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	
Орел Анастасія	38
СПОСОБИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ЗА ДОПОМОГОЮ ЛОГ-ФАЙЛІВ	
Раєв Олександр	41
АВТОМАТИЗАЦІЯ ПЕНТЕСТИНГУ ВЕБ-САЙТІВ ЗА ДОПОМОГОЮ МОВИ PYTHON	
Жук Максим	44
КІБЕРБЕЗПЕКА ЯК ФАКТОР ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА	
Тишко Ілонна	46
ВИЯВЛЕННЯ ЗЛОВМИСНОЇ АКТИВНОСТІ В КОРПОРАТИВНИХ ЛОКАЛЬНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ АНАЛІЗУ DNS-ЗАПИТІВ	
Гуренко Марк	49
ДОСЛІДЖЕННЯ MALWARE З ВИКОРИСТАННЯМ МЕТОДІВ ВКЛАДЕНОЇ ВІРТУАЛІЗАЦІЇ	
Величканич Юрій	51
HOLOMORPHIC IMMERSIONS OF COMPLEX MANIFOLDS	
Josef Mikeš	53
БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ В АРХІТЕКТУРІ СИСТЕМИ ОРКЕСТРАЦІЇ КЛАСТЕРІВ	
Астахов Даниїл	57
ШЛЯХИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ	
Кіфа Константин	59
ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ	
Вінник Мирослава	62
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІННОВАЦІЙНИХ ПРОЕКТІВ В УМОВАХ СЬОГОДЕННЯ	
Громов Ігор	66
БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ	
Чеховський Андрій	69
THE STRESS-ENERGY TENSOR AND LCK-MANIFOLDS RESPECT TO CONFORMAL MAPPINGS	
Patrik Peška, Olena Chepurna	71

КРИТИЧНА ІНФРАСТРУКТУРА ЯК ОБ'ЄКТ КІБЕРЗАХИСТУ	
Саврацький Олександр.....	76
СТАНДАРТ АВТЕНТИФІКАЦІЇ FIDO2	
Даниловська Каріна	78
БЕЗПАРОЛЬНА АВТЕНТИФІКАЦІЯ (PASSWORDLESS AUTHENTICATION)	
Сіянко Кіріл	81
КРИТИЧНИЙ АНАЛІЗ МЕТОДОЛОГІЧНИХ ПІДХОДІВ ДО ОЦІНКИ КІБЕРРИЗИКІВ	
Грезіна Олена	85
CYBER SECURITY CHALLENGES AND ITS EMERGING TRENDS ON LATEST TECHNOLOGIES	
Paige Nikita Andrew	87
ЗАХИСТ ІНФОРМАЦІЇ ЩОДО УПРАВЛІННЯ ПЕРСОНАЛОМ: ВАЖЛИВИЙ ФАКТОР ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМСТВА	
Шатунова Ксенія	90
ГЕНДЕРНІ АСПЕКТИ У КІБЕРБЕЗПЕЦІ: РОЛЬ СТАТЕВИХ СТЕРЕОТИПІВ У СВІДОМОМУ ТА БЕЗПЕЧНОМУ КОРИСТУВАННІ ІНФОРМАЦІЙНИМИ ТЕХНОЛОГІЯМИ	
Осадчук Анастасія.....	92
ARTIFICIAL INTELLIGENCE: CHALLENGES AND HOW WE COULD DEAL WITH	
Yevhen Cherevko, Yevheniia Kuleshova.....	95
КІБЕРПРОСТІР В УМОВАХ ВІЙНИ	
Парамонова Юлія.....	97
ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ	
Арнаут Аліна	100
ВИКОРИСТАННЯ БІБЛІОТЕКИ SCAPY ДЛЯ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ	
Дрига Артем	102

Секція 2. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В УМОВАХ ВІЙНИ	105
АНАЛІЗ ПОТЕНЦІЙНИХ ВИТОКІВ ДАННИХ В ПРИСТРОЯХ КОМУНІКАЦІЇ Задерейко Олександр, Логінова Наталія, Троянський Олександр	105
СУЧАСНІ ІНСТРУМЕНТИ UI/UX ДИЗАЙНУ Манаков Сергій	108
БІОМЕТРИЧНІ ТЕХНОЛОГІЇ У СИСТЕМАХ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ Грезіна Олена	110
ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ В РІЗНИХ СФЕРАХ ДІЯЛЬНОСТІ Задерейко Олександр, Толокнов Анатолій, Черненко Олександра	113
GEOINT: МОЖЛИВОСТІ ГЕОПРОСТОРООВОЇ РОЗВІДКИ Задерейко Олександр, Долінко Ксенія	118
ДОСЛІДЖЕННЯ ПОТУЖНОСТЕЙ МНОЖИН НЕЛІНІЙНИХ ПЕРЕТВОРЕНЬ ІЗ ЗАДАНИМИ ЗНАЧЕННЯМИ ПЕРІОДІВ ПОВЕРНЕННЯ У ВИХІДНИЙ СТАН Баландіна Наталія	123
РОЗПОДІЛЕНІ МЕРЕЖІ ТА ЇХ РОЛЬ У БЛОКЧЕЙН-ТЕХНОЛОГІЯХ Сметана Владислав	127
ЧИСЛА, ЩО НЕ ПІДДАЮТЬСЯ НАУКОВОМУ ПОЯСНЕННЮ Шляхтицький Дмитро	131
СУЧАСНІ МЕТОДИ ДОСЛІДЖЕННЯ ТА ОЦІНКИ DDOS-АТАК Щербина Юрій, Казакова Надія	136
МОЖЛИВОСТІ МОВИ C# ДЛЯ ОРГАНІЗАЦІЇ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ Чикунів Павло	140
ШТУЧНИЙ ІНТЕЛЕКТ У ВІЙСЬКОВІЙ СФЕРІ Трофименко Олена, Яремчук Максим	144
АЛГОРИТМИ У BACK-END ЗАСОБАМИ JAVA Трофименко Олена, Старіков Ігор	148
ПРОГРАМНІ ЗАСОБИ ДЛЯ ARDUINO Усатенко Ярослав	152

ПРОЕКТИ ОБРОБКИ ВІЗУАЛЬНИХ ДАНИХ	
Пучков Владислав	155
РОЛЬ СИСТЕМНОГО АНАЛІЗУ В РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	
Ревацький Олександр	158
ДИСТАНЦІЙНИЙ КОНТРОЛЬ СИСТЕМ ЕНЕРГОЗАБЕЗПЕЧЕННЯ СЕРВЕРНОГО ОБЛАДНАННЯ ЗА УМОВ ЗБОЇВ ЕНЕРГОПОСТАЧАННЯ	
Пшеничний Євгеній	161
ЦИФРОВА ТРАНСФОРМАЦІЯ ОСВІТНЬОГО ПРОЦЕСУ В ЗВО ПІД ЧАС ВІЙНИ	
Кульбабський Анатолій	164
ЗАСТОСУВАННЯ МАТЕМАТИКИ В ПРОГРАМУВАННІ	
Ковальський Олександр	168
СТВОРЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗА ДОПОМОГОЮ AGILE	
Гурін Євген	170
ШТУЧНИЙ ІНТЕЛЕКТ У ВЕБРОЗРОБЦІ: РЕВОЛЮЦІЯ ПЕРСОНАЛІЗАЦІЇ КОРИСТУВАЧА	
Дика Анастасія, Максименко Артем	174
РЕАЛІЗАЦІЯ АЛГОРИТМІВ MACHINE LEARNING У БАЗАХ ДАНИХ СІМЕЙСТВА NOSQL	
Лобода Юлія	176
ХАРАКТЕРИСТИКА ФРЕЙМВОРКІВ ДЛЯ КРОСПЛАТФОРМНОЇ РОЗРОБКИ	
Касян Павло	179
ВИКОРИСТАННЯ КОЛЕКЦІЇ TIDYVERSE В АНАЛІЗІ ДАНИХ	
Сітько Анастасія	182
ВЕБРОЗРОБКА ЗАСОБАМИ ASP.NET CORE	
Солом'яний Олексій	185
АНАЛІЗ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ УПРАВЛІННЯ	
Фомічов Дмитро	187
РОЗРОБКА ЧАТ-БОТА ДЛЯ ПОШУКУ НЕРУХОМОСТІ	
Петрушенко Мілена	190

Секція 3. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ КІБЕРПРОСТОРУ	193
ЩОДО ОBOB'ЯЗKOBOCТІ РЕЄСТРАЦІЇ ЮРИДИЧНИХ ОСІБ ПРИВАТНОГО ПРАВА В ЕЛЕКТРОННОМУ СУДУ Купенко Артем	193
РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ В ПРОЦЕСІ МЕДІАЦІЇ Блатін Стівен	195
ІНФОРМАЦІЙНА ПОСЛУГА У СФЕРІ ГОСПОДАРЮВАННЯ: ПОНЯТТЯ ТА ОЗНАКИ Деренюк Ангеліна	197
ЩОДО КІБЕРБЕЗПЕКИ ГОСПОДАРСЬКИХ ПРАВОВІДНОСИН Ляховецький Олександр	201
ДЕЯКІ АСПЕКТИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ЗМІН Грезіна Олена	204
ВИКОРИСТАННЯ АЛГОРИТМІВ YOUTUBE ДЛЯ ОРГАНІЗАЦІЇ ТЕРОРИСТИЧНИХ НАПАДІВ. Динту Валерія	206
THE BLETONLEY DECLARATION ТА ПРОБЛЕМИ МІЖНАРОДНОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ Чанишев Рашид	209
ПРАВОВА ПРИРОДА ШТУЧНОГО ІНТЕЛЕКТУ Бааджи Наталія	213
СУЧАСНІ ПРОБЛЕМИ ВЗАЄМОДІЇ ЛЮДИНИ І КІБЕРСЕРЕДОВИЩА Руденко Каріна	218
РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ У СИСТЕМІ МІСЦЕВОГО САМОВРЯДУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ Холостенко Світлана, Ровинська Катерина	220

Секція 4. УПРАВЛІНСЬКІ ТА СОЦІАЛЬНО-ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРСЕРЕДОВИЩА	223
ПАРИТЕТ ТРАНСПАРЕНТНОСТІ ТА КІБЕРБЕЗПЕКИ У ХОЛОКРАТИЧНІЙ МОДЕЛІ УПРАВЛІННЯ БІЗНЕСОМ Горбаченко Станіслав	223
ІНТЕГРАЦІЯ КРИТИЧНИХ КОМПОНЕНТІВ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВОДНОГО ТРАНСПОРТУ Пунченко Наталія	225
СТРАТЕГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ ТА ІННОВАЦІЙНОГО УПРАВЛІННЯ ДЛЯ СТАЛОГО РОЗВИТКУ СУСПІЛЬСТВА Котлубай Вячеслав.....	229
ЗАСТОСУВАННЯ ІНСТРУМЕНТІВ КІБЕРБЕЗПЕКИ В ЕКОНОМІЦІ ЗАМКНУТОГО ЦИКЛУ Клевцевич Наталія	232
ВИКОРИСТАННЯ КОМПЛЕКСНИХ ЧИСЕЛ У РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ Гурін Євген	236
ОСОБЛИВОСТІ ПРОСУВАННЯ БРЕНДІВ В КІБЕРСЕРЕДОВИЩІ Рева Аніта	238
КІБЕРРИЗИКИ ФУНКЦІОНУВАННЯ ЕЛЕКТРОМОБІЛЬНОЇ ІНФРАСТРУКТУРИ Разінкін Нікіта.....	242
ПЕРСПЕКТИВИ РОЗВИТКУ СЕГМЕНТУ ГЕЙМДЕВ В УКРАЇНІ Скідан Владислав.....	246
СУЧАСНІ ТРЕНДИ ІНТЕРНЕТ-МАРКЕТИНГУ Наumenko Аліна	250
КІБЕРБЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ ШЛЯХОМ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ Грезіна Олена	254
СУТНІСТЬ ТА НЕОБХІДНІСТЬ УПРАВЛІННЯ РИЗИКОМ Дем'янова Тетяна	256

ВПЛИВ ІНФОРМАЦІЙНИХ ВІЙН НА СОЦІАЛЬНУ ПСИХОЛОГІЮ СУЧАСНИХ СУСПІЛЬСТВ	
Чепурна Олена, Козловський Ігор	260
СТРАТЕГІЯ УПРАВЛІННЯ РИЗИКАМИ ПІД ЧАС ВОЄННОГО СТАНУ	
Ничипорук Анастасія	262
ВПЛИВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ПОВЕДІНКУ КОРИСТУВАЧІВ: АНАЛІЗ МЕТОДІВ ТА ЗАХОДІВ ЗАХИСТУ	
Нігуренко Аміна	265
СУЧАСНИЙ ПІДХІД ДО УПРАВЛІННЯ ФІНАНСОВИМИ РИЗИКАМИ	
Шамес Владислава	268
ОСНОВНІ ФОРМИ ПРОФІЛАКТИКИ РИЗИКІВ НА ПІДПРИЄМСТВІ	
Муль Валерій	272
СУЧАСНІ ПРОБЛЕМИ ВЗАЄМОДІЇ ЛЮДИНИ І КІБЕРСЕРЕДОВИЩА	
Руденко Каріна	275
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УПРАВЛІННІ ПЕРСОНАЛОМ	
Снігур Ксенія	277
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В АНАЛІЗІ ФІНАНСОВОГО СТАНУ ПІДПРИЄМСТВ	
Кедік Олена	281
КІБЕРКУЛЬТУРА: СТІЙКІСТЬ В УМОВАХ СЬОГОДЕННЯ	
Горбанець Катерина	283
МЕТОДОЛОГІЧНІ ПІДХОДИ ДО УПРАВЛІННЯ РИЗИКАМИ	
Музика Герман	285
ПЕРЕФОРМАТУВАННЯ ІТ-СЕКТОРУ УКРАЇНИ В УМОВАХ ВІЙНИ	
Баланюк Ростислав	290
ЗМІСТ	293

КІБЕРПРОСТІР В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: ТЕОРІЯ ТА ПРАКТИКА

**МАТЕРІАЛИ МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

*24 листопада 2023 року
м. Одеса*

Відповідальній редактор: О.В. Дикий

Дизайн та верстка:
М.Ю. Овчинников