МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Інститут модернізації змісту освіти МОН України
ННІ «Дніпровський металургійний інститут (ДМетІ)
Українського державного університету науки і технологій (УДУНТ), м. Дніпро
Українська асоціація управління проєктами «УКРНЕТ», м. Київ
Науково-дослідний інститут інтелектуальної власності (НДІІВ)
Національної академії правових наук України (НАПрН України), м. Київ
Державна установа «Інститут економіко-правових досліджень імені В.К.Мамутова НАН України»
Київський національний університет імені Тараса Шевченка, м. Київ
Національний технічний університет України «Харківський політехнічний інститут»
Національний технічний університет України «Київський політехнічний університет імені Ігоря Сікорського», м. Київ
Одеський національний морський університет (ОНМУ), м. Одеса
Честоховський політехнічний університет, Польща
Uniwersytet Warszawski, Warszawa, Polska Rzeczpospolita, Польща;
Вища школа менеджменту у Варшаві, (WSM), Польща
Вища економіко-гуманітарна школа (WSEH) м. Бєльсько-Бяла, Польща
Вища школа управління охороною праці в місті Катовіце, (WSZOP), Польща
Університет в Мішкольце, Угорщина
Astana IT University, Kazakhstan
Варнський вільний університет імені Чорноризця Хороброго, Республіка Болгарія, м. Варна
Компанія та видавництво «E-SCIENCE SPACE», Республіка Польща, м. Варшава
Інститут освітнього та професійного розвитку, Будапешт, Угорщина
за підтримки:
Центр Українсько-європейського наукового співробітництва
Видавничий дім «Гельветика»
Дніпропетровський науково-дослідний експертно-криміналістичний центр МВС України
Юридична компанія «ЮРСЕРВІС», м. Дніпро

ЗБІРНИК НАУКОВИХ ПРАЦЬ

VII Міжнародної науково-практичної інтернет-конференції
МІСТ «КИЇВ-ДНІПРО»
«УПРАВЛІННЯ ПРОЄКТАМИ. ПЕРСПЕКТИВИ РОЗВИТКУ ПРОЄКТНОГО ТА НЕЙРОМЕНЕДЖМЕНТУ, ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ УПРАВЛІННЯ, ТЕХНОЛОГІЙ СТВОРЕННЯ ТА ВИКОРИСТАННЯ ОБ'ЄКТІВ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ, ТРАНСФЕР ТЕХНОЛОГІЙ»,
27-28 березня 2025 р.

ДНІПРО
УДУНТ 2025

ЗБІРНИК НАУКОВИХ ПРАЦЬ

VII Міжнародної науково-практичної інтернет-конференції
МІСТ «КИЇВ-ДНІПРО»

УПРАВЛІННЯ ПРОЄКТАМИ. ПЕРСПЕКТИВИ РОЗВИТКУ ПРОЄКТНОГО ТА НЕЙРОМЕНЕДЖМЕНТУ, ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ УПРАВЛІННЯ, ТЕХНОЛОГІЙ СТВОРЕННЯ ТА ВИКОРИСТАННЯ ОБ'ЄКТІВ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ, ТРАНСФЕР ТЕХНОЛОГІЙ

27-28 березня 2025 р.

ДНІПРО
УДУНТ
2025

COLLECTION OF SCIENTIFIC PAPERS

VII International Scientific and Practical Internet Conference

KYIV-DNIPRO BRIDGE

PROJECT MANAGEMENT. PROSPECTS FOR THE DEVELOPMENT OF PROJECT AND NEUROMEGRANATION, INFORMATION TECHNOLOGIES OF MANAGEMENT, TECHNOLOGIES FOR CREATING AND USING OBJECTS OF INTELLECTUAL PROPERTY RIGHTS, TECHNOLOGY TRANSFER

March 27-28, 2025

DNIPRO
USUST
2025

УДК 005.8:[005.3+004.9+347.77]
У 67

Конференція запроваджена МОН України, Інститутом модернізації змісту освіти МОН України та зареєстрована Державною науковою установою «Український інститут науково-технічної експертизи та інформації МОН України», посвідчення № 282 від 27.02.25 р. Рекомендовано до видання Вченою радою УДУНТ, протокол № 11 від 23.04.2025 року

Управління проєктами. Перспективи розвитку проєктного та нейроменеджменту, інформаційних технологій управління, технологій створення та використання об’єктів права інтелектуальної власності, трансфер технологій : зб. наук. пр. VII Міжнар. наук.-практ. інтернет-конф. (27–28 берез. 2025 р.) / за ред. В. О. Петренка, В. М. Молоканової, П. Г. Перерви, Г. К. Дорожка ; УДУНТ, УКРНЕТ, НДІІВ НАПрН України. – Електрон. вид. – Дніпро : УДУНТ, 2025. – 1153 с.

ISBN 978-617-8314-50-7 (PDF)

У збірнику наукових праць наведені матеріали VII Міжнародної науково-практичної інтернет-конференції «Управління проєктами. Перспективи розвитку проєктного та нейроменеджменту, інформаційних технологій управління, технологій створення та використання об’єктів права інтелектуальної власності, трансферу технологій». Збірник наукових праць становить інтерес для наукових працівників, викладачів, фахівців з інтелектуальної власності та управління проєктами, економіки та менеджменту, інформаційних технологій, а також студентів.

УДК 005.8:[005.3+004.9+347.77]

ISBN 978-617-8314-50-7 (PDF)
DOI 10.15802/978-617-8314-50-7

UDC 005.8:[005.3+004.9+347.77]
P 93

The conference was initiated by the Ministry of Education and Science of Ukraine, the Institute for Modernization of Educational Content of the Ministry of Education and Science of Ukraine and registered by the State Scientific Institution "Ukrainian Institute of Scientific and Technical Expertise and Information of the Ministry of Education and Science of Ukraine", certificate No. 282 dated 02/27/25. Recommended for publication by the Academic Council of the USUST, protocol No. 11, 23.04.2025

Project Management. Prospects for the Development of Project and Neuromegranation, Information Technologies of Management, Technologies for Creating and Using Objects of Intellectual Property Rights, Technology Transfer : Coll. Sci. Pap. of the VII Int. Sci. Pract. Internet Conf. (March 27–28, 2025) / ed. by V. O. Petrenko, V. M. Molokanova, P. G. Pererva, G. K. Dorozhko ; USUST, UKRNET, NDIIV NAPRN of Ukraine. – Electronic edition. – Dnipro : USUST, 2025. – 1153 p.

ISBN 978-617-8314-50-7 (PDF)

The collection of scientific papers contains materials from the VII International Scientific and Practical Internet Conference "Project Management. Prospects for the Development of Project and Neuromanagement, Information Management Technologies, Technologies for the Creation and Use of Intellectual Property Rights, and Technology Transfer." The collection of scientific papers is of interest to researchers, teachers, specialists in intellectual property and project management, economics and management, information technologies, and students.

UDK 005.8:[005.3+004.9+347.77]

ISBN 978-617-8314-50-7 (PDF)
DOI 10.15802/978-617-8314-50-7

ЗМІСТ
УПРАВЛІННЯ ПРОЄКТАМИ ТА ПРОГРАМАМИ

S. BUSHUYEV, V. BUSHUIEVA, D. BUSHUIEV, A. PUZIYCHUK, G. MUROVANSKIY
***THE EVOLVING LANDSCAPE OF INNOVATION PROJECTS EDUCATION UNDER THE INFLUENCE OF AI*……23**

N. BUSHUYEVA, YE. LOBOK
***ENHANCING CREATIVITY IN MULTIMODAL AI SYSTEMS*……..29**

БАРИШЕВСЬКИЙ А.І., ПЕТРЕНКО В.О.
***МЕТОДИ УПРАВЛІННЯ ПРОЄКТАМИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ В УМОВАХ НЕСТАБІЛЬНОСТІ ТА ШВИДКИХ ТЕХНОЛОГІЧНИХ ЗМІН*……....36**

БУЛАВІН Д.О., ПЕТРЕНКО В.О.
***ТРАНСФОРМАЦІЯ ПРОЦЕСІВ РОЗВИТКУ ОРГАНІЗАЦІЙ У ЗМІННОМУ СЕРЕДОВИЩІ*……..43**

ГЛАВАТСЬКИХ В.І., ЛАПКІНА І.О.
***РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ ПРОЄКТІВ МОРСЬКОЇ ТРАНСПОРТНОЇ ГАЛУЗІ*……..50**

ДОБРИЦЬКИЙ Д.О., наук. керівник ФОНАРЬОВА Т.А.
***ОСОБЛИВОСТІ УПРАВЛІННЯ АУТСОРСИНГОВОЮ ІТ-КОМПАНІЄЮ НА СУЧАСНОМУ РИНКУ ІТ-ТЕХНОЛОГІЙ: ВИКЛИКИ, ПІДХОДИ ТА ПЕРСПЕКТИВИ*……..56**

ЖАДАН К.Ю., КОСЕНКО Н.В.
***ВИЗНАЧЕННЯ ВИМОГ ДО ЗМІСТУ ПРОЄКТІВ*…….....64**

КЛИМЕНКО К.А., ГУСЄВА Ю.Ю.
***ПРОЄКТНИЙ ПІДХІД ДО ВПРОВАДЖЕННЯ КОНЦЕПЦІЇ «ВІД ФЕРМИ ДО СТОЛУ» У РЕСТОРАННІЙ ІНДУСТРІЇ*……....71**

КОВТУН Т.А., КРУПСЬКА О.С.
***ВПРОВАДЖЕННЯ ПРИНЦИПІВ ЦИРКУЛЯРНОЇ ЕКОНОМІКИ В ЛОГІСТИЦІ*……77**

КОРХІНА І.А.
***УПРАВЛІННЯ РЕСУРСАМИ ПРОЄКТУ З ТОЧКИ ЗОРУ СТРАТЕГІЇ*…….....83**

ТРОСТЯНСЬКА К.М.
ОСОБЛИВОСТІ БІЗНЕС-МОДЕЛЕЙ ІНТЕЛЕКТУАЛЬНОГО ПІДПРИЄМНИЦТВА ТА ФАКТОРИ, ЩО ВИЗНАЧАЮТЬ ЇХ РОЗВИТОК.....**1100**

ШЕІН О.С., ПЕРЕРВА П.Г.
ВСТАНОВЛЕННЯ РОЗМІРУ РОЯЛТІ НА B2B РИНКАХ.....**1107**

УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЙНИХ СИСТЕМ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ ПРОЄКТНО-ОРІЄНТОВАНИХ ОРГАНІЗАЦІЙ

H.H. SHVACHYCH, V.O. PETRENKO, D.O. MYRONOV, G.V. MYRONOV
AUTOMATED TESTING OF WEB APPLICATIONS: DEVELOPMENT OF A SYSTEM FOR IMPROVING PERFORMANCE AND RELIABILITY.....**1114**

H.H. SHVACHYCH, V.O. PETRENKO, P.O. SHCHERBYNA, O.V. KABACHENKO
INFORMATION SYSTEM FOR SOLVING APPLIED PROBLEMS USING STOCHASTIC PROGRAMMING METHODS.....**1120**

БАРАНЕНКО О.О., ДЯЧЕНКО В.С.
ІМПЛЕМЕНТАЦІЯ SBOM (SOFTWARE BILL OF MATERIALS) ДЛЯ ПРОЄКТНО-ОРІЄНТОВАНИХ ОРГАНІЗАЦІЙ.....**1126**

ТУПКАЛО В.М.
СИСТЕМОТЕХНІКА КІБЕРЗАХИЩЕНИХ ЦИФРОВИХ СИСТЕМ НА ОСНОВІ ВИКОРИСТАННЯ АПАРАТУ СИНТЕЗУ СИГНАТУРНОЇ ЛОГІКО-ПОЛІНОМІЙНОЇ АЛГЕБРИ ПОЛЯ $TSF[2^n, P^m(x)]$.....**1133**

ФОНАРЬОВА Т.А., ПЕТРЕНКО В.О.
ДО ПИТАННЯ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЙНИХ СИСТЕМ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ.....**1144**

УДК 004.056:342

ДО ПИТАННЯ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЙНИХ СИСТЕМ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

Т.А. ФОНАРЬОВА

к.е.н., доцент, доцент кафедри інтелектуальної власності та управління проєктами Українського державного університету науки і технологій, м. Дніпро

ORCID: https://orcid. org/ 0000-0001-7726-6999

В.О. ПЕТРЕНКО

доктор технічних наук, професор, заслужений діяч науки і техніки України, академік Академії наук вищої школи України, завідувач кафедри інтелектуальної власності та управління проєктами Українського державного університету науки і технологій, м. Дніпро

ORCID: https://orcid. org/0000-0001-5017-1674

Український державний університет науки і технологій

м. Дніпро, Україна

TO THE QUESTION OF MANAGING INFORMATION SYSTEMS PROTECTION AND CYBERNETIC SECURITY

T.A. Fonarova

PhD in Economics, assistant professor of the Department of Intellectual Property and Project Management of the Ukrainian State University of Science and Technology, Dnipro

ORCID 0000-0001-7726-6999

V.O. Petrenko

Doctor of Technical Sciences, Professor, Honored Worker of Science and Technology of Ukraine, Academician of the Academy of Sciences of the Higher School of Ukraine, Head of the Department of Intellectual Property and Project Management of the Ukrainian State University of Science and Technology, Dnipro

ORCID: https://orcid. org/0000-0001-5017-1674

Анотація: *Досліджуються сучасні аспекти удосконалення управління захистом інформаційних систем та кібернетичною безпекою підприємств України. Проаналізовано законодавча база та виявлено певні недоліки та суперечності, визначено роль та напрями діяльності наукової спільноти у забезпеченні кібербезпеки. Надано рекомендації з подолання сучасних кіберзагроз. Визначено напрями подальших досліджень.*

Ключові слова*: гібридна війна, кібератаки, кібербезпека, сертифікація систем захисту інформації, штучний інтелект, ризики.*

Abstract: *Modern aspects of improving the management of information systems protection and cyber security of enterprises in Ukraine are studied. The legislative framework is analyzed and certain shortcomings and contradictions are identified, the role and areas of activity of the scientific community in ensuring cybersecurity are determined. Recommendations are given for overcoming modern cyber threats. Directions for further research are determined.*

Keywords: *hybrid warfare, cyber attacks, cybersecurity, certification of information protection systems, artificial intelligence, risks.*

Актуальність дослідження обумовлена наявністю гібридної війни, яку веде агресор проти України. В таких умовах особливого значення набувають питання управління захистом інформаційних систем та кібернетичною безпекою підприємств.

Гібридна війна – це поєднання військових операцій та кібератак. Вона відбувається у кількох вимірах або просторах: військовому, економічному, кібернетичному, інформаційному та культурному. Оцінка цієї комбінації дає розуміння стратегії противника та дозволяє будувати відповідну систему захисту [1].

Здійснення кібератак, нажаль, постійно зростає, під загрозою опинилися важливі об’єкти інфраструктури, інформаційні системи. Запровадження цифровізації у всі галузі діяльності країни, бурхливий розвиток ІТ-технологій,

особливо технологій штучного інтелекту, збільшує ризики протиправних дій щодо порушення безпеки інформаційного та кіберпростору.

Задля готовності забезпечувати кібербезпеку і відбивати відкриту агресію в кіберпросторі Україна реалізувала цілий комплекс заходів для вирішення стратегічних, правових, політичних, технічних та організаційних питань з безпечного функціонування кіберпростору. Основними елементами комплексу є: політика кібербезпеки, яка включає національну стратегію, плани реалізації стратегії, координацію та контроль діяльності кібербезпеки; прийняття відповідного законодавства, яке включає доктрину інформаційної безпеки України, закони, положення та підзаконні акти; глобальне партнерство, яке включає ратифікацію Конвенції про кіберзлочинність, участь у міжнародних центрах та навчання з кібероперацій; просвітницькі програми з кібербезпеки, де головна роль відводиться навчальним програмам у державній вищій освіті [2].

Отже, роль наукової спільноти полягає: в наданні оцінки досконалості законодавчих актів, виявленні проблемних місць з метою їх усунення, що дасть країні більшу правову захищеність; в залученні студентської молоді до вивчення всіх аспектів законодавства, дискусійним обговоренням міжнародного досвіду із захисту інформаційних систем та кіберпростору, особистої безпечної поведінки у мережі Інтеренет; в підготовці кадрів, та вихованні майбутніх фахівців, які розуміють необхідність постійного підвищення обізнаності з питань кібербезпеки; розробка комплаєнс-концепції, яка включає програми контролю за дотриманням безпеки на всіх рівнях діяльності підприємства, підготовка комплаєнс-контролерів; удосконалення менеджменту кризових ситуацій, та розробка практичних рекомендацій й сценаріїв реагування на кібератаки з метою підготовки команди та персоналу; вивчення аспектів захисту інформаційних систем з урахуванням розвитку технологій штучного інтелекту, тощо.

Захист інформаційних систем та кіберпростору починається із вивчення законодавчого підґрунтя. Сьогодні країна має досить потужні правові інструменти боротьби та захисту.

Відповідно до українського законодавства, кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [3].

Слід зазначити, що в Україні законодавча ситуація з кібербезпеки після 2014 року набула значних зрушень: затверджено Доктрину інформаційної безпеки України (введена в дію 25.02.2017 р.), закони України «Про основні засади забезпечення кібербезпеки України» 2163-VIII (набрав чинності 09.05.2018 р.), «Про національну безпеку України» 2469-VIII (набрав чинності 08.07.2018 р.), «Про інформацію» 2657-XII (редакція від 01.01.2017 р.), «Про захист інформації в інформаційно-телекомунікаційних системах» 80/94-ВР (редакція від 19.04.2014 р.), «Про електронні довірчі послуги» 2155-VIII (набрав чинності 07.11.2018 р.), «Про захист персональних даних» 2297-VI (редакція від 30.01.2018 р.) тощо. Низка відповідних положень щодо кібербезпеки закріплена в указах президента, зокрема: «Про Концепцію розвитку сектора безпеки і оборони України» (No 92/2016 від 14.03.2016 р.); «Про стратегічний оборонний бюлетень України» (No 240/2016 від 06.06.2016 р.), «Про Національний координаційний центр кібербезпеки» (No 242/2016 від 07.06.2016 р.) тощо. [2]

Аналіз закону України «Про основні засади забезпечення кібербезпеки України» показує, що в ньому не визначено зміст та заходи кібероборони, саме коли потрібно переходити від заходів кібербезпеки до заходів кібероборони у випадку кібератаки. Недоліком закону також є недосконаліть та невизначеність термінів. [4]

Окрім того, до проблем законодавчих документів слід віднести: відсутність законодавчого визначення такого базового терміна, як «безпека інформації»; брак єдності та неоднозначність тлумачення у термінології, що застосовується у сфері інформаційних технологій (ІТ), зокрема ключових (це стосується і Розділу XVI Кримінального кодексу України, за якими розслідуються кіберзлочини в Україні); неузгодженість терміну «кіберзлочин», який використовується в Законі України «Про основні засади забезпечення кібербезпеки України» з Кримінальним кодексом України (ККУ), який містить окремий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», де використовується термін «комп'ютерний злочин»; відсутнє регламентування системи менеджменту у сфері нормативно-правового забезпечення інформаційних відносин, що повинно забезпечувати динаміку процесів правового забезпечення інформаційної і кібербезпеки в Україні [5].

Сьогодні фахівці та експерти зазначають збільшення кібератак. Так за даними ресурсу [1], фахівці зіткнулися з чотирма основними типами інцидентів під час кібервійни порівняно з мирним періодом: кібершпигунство, руйнівні атаки, зокрема на системи критичної інфраструктури, які часто йшли разом з військовими операціями, інформаційна війна – поширення фейків, пропаганда, психологічний тиск, та опортуністичні напади як зі сторони міжнародних кримінальних угруповань, так і хакерів-початківців. Основними видами загроз для кібербезпеки є malware (шкідливе програмне забезпечення), ransomware (програми-вимагачі), phishing (фішинг), insider threats (внутрішні загрози), distributed denial of service (ddos) attacks (атаки на відмову в обслуговуванні), а також атаки ботнетів, хмарні експлойти тощо [3]

Подолання цих загроз, окрім удосконалення законодавчої бази, можливе в декількох напрямах.

Перший напрям – це достатня кількість відповідних фахівців. І тут велику роль грає Державна служба спеціального зв'язку та захисту інформації України.

Вона відповідає за підготовку фахівців у цих напрямах, що потребує особливої гнучкості, аби нові кадри відповідали мінливим вимогам сьогодення. Для цього існує лише два шляхи: перший – впровадження змін у систему вищої освіти шляхом розширення переліку освітніх можливостей у співпраці з МОНУ; другий – імплементувати міжнародні стандарти та кращі світові практики і розробити кваліфікаційну рамку професій у галузі кібербезпеки, результатом діяльності Держспецзв'язку є збільшення кількості професій галузі кіберзахисту та захисту інформації із 2 до 27. [6]

Другий напрям – це сертифікування систем захисту інформації. Так в Україні діють державні стандарти для сертифікування систем захисту інформації: ДСТУ ISO/IEC 27000:2019 (ISO/ IEC 27000:2018, IDT) - Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів – на заміну ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT); ДСТУ ISO/IEC 27001:2015 (ISO/ IEC 27001:2013; Cor 1:2014, IDT) / Поправка N 2:2019 (ISO/IEC 27001:2013/Cor 2:2015, IDT) - Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги; ДСТУ ISO/IEC 27002:2015 (ISO/ IEC 27002:2013; Cor 1:2014, IDT)/ Поправка N 2:2019 ISO/IEC 27002:2013/Cor 2:2015, IDT) - Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки; ДСТУ ISO/IEC 27005:2019 (ISO/ IEC 27005:2018, IDT) - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки – на заміну ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT); ДСТУ ISO/IEC 27008:2019 (ISO/ IEC TS 27008:2019, IDT) - Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки (Настанова для аудиторів) – на заміну ДСТУ ISO/IEC TR 27008:2018 (ISO/ IEC TR 27008:2011, IDT); ДСТУ ISO/IEC 27011:2018 (ISO/ IEC 27011:2016, IDT) / Поправка N 1:2019 (ISO/IEC 27011:2016/Cor 1:2018, IDT) - Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо керування [5]

Третій напрям – це зміцненні міжнародного співробітництва. Важливою у цьому напрямі є міжнародна співпраця України та світу. Зокрема, у 2023 р. міністерства закордонних справ України, Канади, Данії, Естонії, Франції, Німеччини, Нідерландів, Польщі, Швеції, Великої Британії та Сполучених Штатів Америки оголосили про створення нового механізму співробітництва в сфері кібербезпеки, який отримав назву «Талліннський механізм» [3]. Необхідна подальша імплементації у національне законодавство окремих норм нормативно-правових актів, прийнятих в країнах ЄС та НАТО у сфері захисту інформації, які на державному рівні визнаються усіма країнами [5].

Четвертий напрям – розвиток штучного інтелекту. У 2021 році Європейська комісія оприлюднила пропозицію Регламенту про штучний інтелект (AI Act), що являє собою новаторську правову ініціативу, оскільки вперше в історії встановлює уніфіковані норми для розроблення, розміщення на ринку та використання штучного інтелекту в країнах Європейського Союзу. Попри розбіжності в підходах до регулювання штучного інтелекту в окремих країнах ЄС, цей Регламент прагне забезпечити спільний стандарт та визначити основні принципи, які регулюють цю сферу. За певних умов використання штучного інтелекту в сфері ризикової діяльності може призвести до ситуації, коли користувач або виробник не матиме законних підстав для притягнення до кримінальної або іншого виду юридичної відповідальності. Зазначена ситуація являє собою незвичайний випадок для доктрини кримінального права, тому потребує подальшого вивчення та аналізу. Виникнення таких ситуацій може потребувати розширення поняття суб’єкта кримінально-правових відносин та суб’єкта кримінальної відповідальності, враховуючи специфіку застосування штучного інтелекту в правовій сфер [3].

Найбільш перспективними напрямами розвитку національної системи кіберзахисту є: вдосконалення правової основи кіберзахисту об’єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури; створення галузевих центрів

реагування на кіберінциденти; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки; розвиток системи підготовки кадрів у сфері кібербезпеки; підвищення цифрової грамотності (правил кібергігієни) громадян та культури безпекового поводження в кіберпросторі, впровадження систем інформаційного комплаєнсу та, насамперед, створення довірчих відносин між державою та суспільством, для якого держава повинна грати сервісну роль. [4]

Підводячи підсумок, можливо зазначити, що Україна зробила великий крок вперед у захисті інформаційних систем та у кібернетичній безпеці. Але напрям подальших досліджень повинен бути спрямований на удосконалення законодавчої бази, підсилення інтеграції у міжнародні інститути ЄС щодо захисту кібрпростору, підготовці менеджерів з кібербезпеки, впровадження аудиту інформаційних систем, мінімізації ризиків розвитку штучного інтелекту.

Література:

1. Як бізнес зараз вирішує питання кіберзахисту? За матеріалами офіційного сайту компанії KPMG https://kpmg.com/ua/uk/home/media/press-releases/2023/08/pro-kiberbezpeku-v-ukrayini.html

2. Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. *Захист інформації*, том 21, № 3, 2019. С. 150-157. DOI: 10.18372/24107840/21/13951

3. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка». Серія: "Юридичні науки"*. Том 11, № 1(41), 2024. С. 314-320. https://doi.org/10.23939/law2024.41.314

4. Петренко В. О., Рудченко Д. О., Маймур Є. Ф. Питання правового забзпечення кібербезпеки в Україні. *Причорноморські публічно-правові читання*: Матеріали міжнародної наукової конференції, м. Миколаїв, 10–12 вересня 2021 р. Миколаїв: Видавничий дім «Гельветика», 2021. Ч. 1. 212 с. С. 135-139.

5. Живко З. Б., Рудий Т. В., Сеник В. В., Родченко С. С. Проблеми нормативно-правової бази забезпечення кібербезпеки в Україні: стан і перспективи. *Соціально-правові студії*. Випуск 3 (9), 2020. С. 18-25. DOI 10.32518/2617-4162-2020-3-18-25

6. Кириченко А. Кібербезпека в Україні: шляхи розвитку та можливості. За даними офіційного сайту Укрінформ https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html

Наукове видання

УПРАВЛІННЯ ПРОЄКТАМИ. ПЕРСПЕКТИВИ РОЗВИТКУ ПРОЄКТНОГО ТА НЕЙРОМЕНЕДЖМЕНТУ, ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ УПРАВЛІННЯ, ТЕХНОЛОГІЙ СТВОРЕННЯ ТА ВИКОРИСТАННЯ ОБ'ЄКТІВ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ. ТРАНСФЕР ТЕХНОЛОГІЙ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

VII Міжнародної науково-практичної
інтернет-конференції
(27-28 березня 2025 року)
МІСТ Київ-Дніпро

Електронне видання

Авторська редакція

Головний редактор д.т.н., проф. Петренко В. О.
Науковий редактор д.т.н., проф. Молоканова В. М.
Науковий редактор д.е.н., проф. Перерва П. Г.
Науковий редактор к.т.н., доц. Дорожко Г. К.
Вчений секретар к.е.н., доц. Фонарьова Т. А.

Формат 60х84 1/16. Ум. друк. арк. 67,02. Обл.-вид. арк. 68,54.
Зам. № 58.

Видавець: Український державний університет науки і технологій
вул. Лазаряна, 2, ауд. 2216, ауд. 263 (наукова бібліотека)
м. Дніпро, 49010.
Свідоцтво суб'єкта видавничої справи ДК №7709 від 14.12.2022

Адреса видавця та дільниці оперативної поліграфії:
вул. Лазаряна, 2, Дніпро, 49010