CYBER SECURITY IN CROSS-BORDER COOPERATION

BOOK OF CONFERENCE ABSTRACTS

International academic and practical conference

Berehove, 15–16 October 2024

КІБЕРБЕЗПЕКА
В ТРАНСКОРДОННОМУ СПІВРОБІТНИЦТВІ

Міжнародна науково-практична конференція
Берегове, 15–16 жовтня 2024 року

Збірник тез доповідей

CYBER SECURITY
IN CROSS-BORDER COOPERATION

International academic and practical conference
Berehove, 15–16 October 2024

Book of Conference Abstracts

KIBERBIZTONSÁG
A HATÁROKON ÁTNYÚLÓ EGYÜTTMŰKÖDÉSBEN

Nemzetközi tudományos és szakmai konferencia
Beregszász, 2024. október 15–16.

Absztraktkötet

Міністерство освіти і науки України
Закарпатський угорський інститут імені Ференца Ракоці II
Ужгородський національний університет

КІБЕРБЕЗПЕКА В ТРАНСКОРДОННОМУ СПІВРОБІТНИЦТВІ

Міжнародна науково-практична конференція
Берегове, 15–16 жовтня 2024 року

Збірник тез доповідей

ЗУІ ім. ФЕРЕНЦА РАКОЦІ II
Берегове
2024

УДК 659.2.012.8:004.056(063)
К 38

Збірник містить тези доповідей міжнародної науково-практичної конференції «Кібербезпека в транскордонному співробітництві», яка відбулася 15–16 жовтня 2024 року в місті Берегове. Матеріали конференції охоплюють широке коло питань, пов'язаних із забезпеченням кібербезпеки в умовах посиленої глобальної взаємодії. Зокрема, тези доповідей конференції досліджують сучасні кіберзагрози, інтеграцію штучного інтелекту в системи безпеки, трансформації методів кіберзахисту та обмін закордонним досвідом. Учасниками конференції були обговорені підходи до вирішення актуальних питань інформаційної безпеки на міжнародному рівні та надання практичних знань студентам, фахівцям і дослідникам. Організатори конференції: Закарпатський угорський інститут імені Ференца Ракоці II та Ужгородський національний університет. Співорганізатори: Національний авіаційний університет, IT Степ Університет, Пряшівський університет у Пряшеві та Північний університетський центр у Бая-Маре Технічного університету Клуж-Напока.

Рекомендовано до видання у друкованій та електронній формі (PDF)
рішенням Вченої ради Закарпатського угорського інституту імені Ференца Ракоці II
(протокол №10 від «21» листопада 2024 року)

Підготовлено до видання кафедрами історії та суспільних дисциплін, обліку і аудиту, математики та інформатики Закарпатського угорського інституту імені Ференца Ракоці II і кафедрами програмного забезпечення систем, міжнародних студій та суспільних комунікацій Ужгородського національного університету спільно з Видавничим відділом ЗУІ ім. Ф. Ракоці II

За редакцією:
Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д, Ганна Мелеганич та Оксана Мулеса

Технічне редагування: *Адам Доровці, Олександр Добош та Ігор Лях*
Коректура: *авторська*
Дизайн обкладинки: *Вівієн Товт*
УДК: *Бібліотека ім. Опацої Чере Яноша при ЗУІ ім. Ф.Ракоці II*

Відповідальний за випуск:
Олександр Добош (начальник Видавничого відділу ЗУІ ім. Ф.Ракоці II)

Публікації науково-педагогічних працівників і студентів Ужгородського національного університету виконано в рамках держбюджетної теми ДБ-921М «Захист інформаційної безпеки при управлінні проєктами міжнародного співробітництва на засадах гарантування національної безпеки України» за підтримки Міністерства освіти і науки України.

Проведення конференції та друк видання здійснено за підтримки уряду Угорщини.

Видавництво: Закарпатський угорський інститут імені Ференца Ракоці II (адреса: пл. Кошута 6, м. Берегове, 90202. Електронна пошта: foiskola@kmf.uz.ua; kiado@kmf.uz.ua)
Друк: ТОВ «РІК-У» (адреса: вул. Карпатської України 36, м. Ужгород, 88006. Електронна пошта: print@rik.com.ua)

ISBN 978-617-8143-27-5 (м'яка обкладинка)
ISBN 978-617-8143-28-2 (PDF)

Ministry of Education and Science of Ukraine
Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education
Uzhhorod National University

CYBER SECURITY IN CROSS-BORDER COOPERATION

International academic and practical conference
Berehove, 15–16 October 2024

Book of Conference Abstracts

Transcarpathian Hungarian College
Berehove
2024

UDC 659.2.012.8:004.056(063)
C 89

The book contains abstracts of presentations at the international academic and practical conference "Cybersecurity in Cross-Border Cooperation", which took place on 15-16 October 2024 in Berehove. The conference materials cover a wide range of issues related to cybersecurity in the context of enhanced global interaction. In particular, the conference abstracts explore modern cyber threats, integration of artificial intelligence into security systems, transformation of cyber defence methods and exchange of foreign experience. The conference participants discussed approaches to addressing topical issues of information security at the international level and providing practical knowledge to students, professionals and researchers. Organisers of the conference: Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education and Uzhhorod National University. Co-organisers: National Aviation University, IT Step University, University of Presov and Northern University Center of Baia Mare at Technical University of Cluj-Napoca.

Recommended for publication in printed and electronic form (PDF file format)
by the Academic Council of Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education
(record No.10 of November 21, 2024)

This volume of conference materials has been prepared by the Department of History and Social Sciences, the Department of Accounting and Auditing, the Department of Mathematics and Informatics at the Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education, and the Department of Systems Software, the Department of International Studies and Public Communications at the Uzhhorod National University, and the Division of Publishing at the Transcarpathian Hungarian College.

Edited by:
Stepan Chernychko, Marianna Marusynets, Yelyzaveta Molnar D., Hanna Melehanych and Oksana Mulesa

Technical editing: *Adam Dorovtsi, Sándor Dobos and Ihor Liakh*
Proof-reading: *the authors*
Cover design: *Vivien Tóth*
Universal Decimal Classification (UDC): *Apáczai Csere János Library of Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education*

Responsible for publishing:
Sándor Dobos (head of the Division of Publishing of Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education)

Publications of research and teaching staff and students at the Uzhhorod National University were implemented within the framework of the state budget theme DB-921M "Information Security Protection in the Management of International Cooperation Projects on the Basis of Ensuring the National Security of Ukraine" with the support of the Ministry of Education and Science of Ukraine.

The conference and the publication of the conference abstracts sponsored by the government of Hungary.

Publishing: Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education (Address: Kossuth square 6, 90202 Berehove, Ukraine. E-mail: foiskola@kmf.uz.ua; kiado@kmf.uz.ua)
Printing: "RIK-U" LLC (Address: Carpathian Ukraine Street 36, 88006 Uzhhorod, Ukraine. E-mail: print@rik.com.ua)

ISBN 978-617-8143-27-5 (paperback)
ISBN 978-617-8143-28-2 (PDF)

Ukrajna Oktatási és Tudományos Minisztériuma
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
Ungvári Nemzeti Egyetem

KIBERBIZTONSÁG A HATÁROKON ÁTNYÚLÓ EGYÜTTMŰKÖDÉSBEN

Nemzetközi tudományos és szakmai konferencia
Beregszász, 2024. október 15–16.

Absztraktkötet

II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
Beregszász
2024

ETO 659.2.012.8:004.056(063)
K 38

A kiadvány 2024. október 15–16-án, Beregszászban *Kiberbiztonság a határokon átnyúló együttműködésben* címmel megrendezett nemzetközi tudományos és szakmai konferencián elhangzott előadások absztraktjait tartalmazza. Az előadások szerkesztett anyagai olyan kibervédelemi kérdéseket vizsgálnak a fokozódó globális együttműködés körülményeivel összefüggésben, mint a modern kibertámadások, a mesterséges intelligencia integrálása a biztonsági rendszerekbe, a kiberbiztonsági módszerek átalakulása és a nemzetközi kibervédelmi tapasztalatcsere. A konferencia résztvevői továbbá megvitatták az információbiztonság aktuális kérdéseinek lehetséges megoldásait nemzetközi szinten, valamint a tudás, ismeretanyag hallgatóknak, szakembereknek és kutatóknak történő átadásának módjait. A konferencia szervezői: a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola és az Ungvári Nemzeti Egyetem. Társszervezők: Nemzeti Repülőmérnöki Egyetem, IT-STEP University, Eperjesi Egyetem, a Kolozsvári Műszaki Egyetem Nagybányai Északi Egyetemi Központja.

Nyomtatott és elektronikus formában (PDF-fájlformátumban) történő kiadásra javasolta
a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Tudományos Tanácsa
(2024. november 21., 10. számú jegyzőkönyv).

Kiadásra előkészítette a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Történelem- és Társadalomtudományi Tanszéke, Számvitel és Auditálás Tanszéke, Matematika és Informatika Tanszéke, Kiadói Részlege, valamint az Ungvári Nemzeti Egyetem Szoftverrendszerek Tanszéke, Nemzetközi Tanulmányok és Közszolgálati Kommunikáció Tanszéke együttműköve
a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Kiadói Részlegével.

Szerkesztette:
Csernicskó István, Maruszinec Marianna, Molnár D. Erzsébet,
Melehánics Anna és Mulesza Okszána

Műszaki szerkesztés: *Daróci Ádám, Dobos Sándor és Ljáh Ihor*
Korrektúra: *a szerzők*
Borítóterv: *Tóth Vivien*
ETO-besorolás: *a II. RF KMF Apáczai Csere János Könyvtára*

A kiadásért felel:
Dobos Sándor (a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Kiadói Részlegének vezetője)

Az Ungvári Nemzeti Egyetem kutatói és oktatói munkatársainak és hallgatóinak publikációi Ukrajna Oktatási és Tudományos Minisztériumának támogatásával, a DB-921M „Az információbiztonság védelme a nemzetközi együttműködési projektek irányításában Ukrajna nemzetbiztonságának biztosítása alapján” című állami költségvetési projekt teljesítésének részeként készültek.

A konferenciát és a kiadvány megjelentetését
Magyarország Kormánya támogatta.

Kiadó: II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola (cím: 90 202, Beregszász, Kossuth tér 6. E-mail: foiskola@kmf.uz.ua; kiado@kmf.uz.ua)
Nyomdai munkálatok: „RIK-U” Kft. (cím: 88 006 Ungvár, Kárpáti Ukrajna u. 36. E-mail: print@rik.com.ua)

ISBN 978-617-8143-27-5 (puhatáblás)
ISBN 978-617-8143-28-2 (PDF)

ЗМІСТ / CONTENT / TARTALOM

Летісія СВЕДКУ
студентка 2 курсу
спеціальності Міжнародні відносини, суспільні комунікації та регіональні студії
кафедри історії та суспільних дисциплін
Закарпатського угорського інституту імені Ференца Ракоці II
***Науковий керівник* – Маріанна МАРУСИНЕЦЬ**
кандидат філологічних наук, доцент,
доцент кафедри історії та суспільних дисциплін,
старший дослідник Науково-дослідного центру імені Тіводора Легоцькі
Закарпатського угорського інституту імені Ференца Ракоці II

КІБЕРБЕЗПЕКА: ДОСВІД ОАЕ

Дослідження присвячено аналізу кібербезпеки в Об'єднаних Арабських Еміратах (ОАЕ), зосереджуючись на основних ініціативах, стратегіях та законодавчих заходах, спрямованих на захист національної кіберінфраструктури. В роботі розглянуто Національну стратегію кібербезпеки ОАЕ, заходи, вжиті для підвищення обізнаності громадян, а також роль aeCERT у реагуванні на кіберзагрози. Особливу увагу приділено впровадженню новітніх технологій, таких як блокчейн, для підвищення захисту інформаційних даних у різних секторах. ОАЕ посідають п'яте місце у світі за рівнем кібербезпеки завдяки комплексному підходу та міжнародній співпраці.

Ключові слова: *кібербезпека, ОАЕ, Національна стратегія кібербезпеки, блокчейн, кібершантаж, кіберзагрози, захист даних.*

У сучасному світі питання кібербезпеки набувають все більшого значення, особливо у регіонах, які швидко розвиваються з точки зору технологій та інновацій. На Близькому Сході кібербезпека стає центральним викликом через зростання цифрових технологій та широке впровадження робототехніки і машинного навчання, що активно розвиваються. Проте, попри ці інноваційні досягнення, безпека, конфіденційність і кіберобізнаність значно відстають від рівня розвинутих економік. ОАЕ, як одна з провідних економік регіону, стикається з викликом зростання кіберзагроз. Зокрема, спостерігається 183-відсоткове збільшення кіберзагроз лише в ОАЕ, що стимулює значні інвестиції в сферу кібербезпеки. Очікується, що до 2025 року ринок кібербезпеки на Близькому Сході досягне понад 8 мільярдів дирхамів ОАЕ, демонструючи зростання на 14% порівняно з 2020 роком.

Актуальність дослідження кібербезпеки в ОАЕ зумовлена швидким розвитком цифрових технологій і збільшенням залежності сучасних економік від інформаційної інфраструктури. На тлі глобальної цифровізації і зростання кіберзагроз, ОАЕ опинилися серед країн, які стикаються зі значним збільшенням кіберінцидентів. Таким чином, необхідність у поглибленому вивченні досвіду ОАЕ в контексті розвитку та зміцнення систем кібербезпеки є надзвичайно важливою як для регіональних, так і для міжнародних дослідників.

Наукова новизна дослідження полягає в тому, що в порівнянні з іншими існуючими роботами у вільному доступі практично відсутні ґрунтовні аналізи кібербезпеки ОАЕ. Водночас, це дослідження спрямоване на всебічне вивчення досвіду країни, зокрема шляхів адаптації до нових кіберзагроз, а також інвестиційних ініціатив для забезпечення надійного кіберзахисту. Дослідження є інноваційним у своєму підході, оскільки виявляє тенденції розвитку кібербезпеки на Близькому Сході через призму одного з провідних економічних і технологічних центрів регіону – ОАЕ. Тому його результати можуть стати важливим внеском у подальші дослідження в цій галузі.

Метою дослідження є всебічний аналіз досвіду Об'єднаних Арабських Еміратів у сфері кібербезпеки, оцінка ефективності впроваджених заходів захисту інформаційної інфраструктури, а також виявлення інноваційних підходів і стратегій, що використовуються для протидії кіберзагрозам в умовах глобальної цифровізації. Дослідження також

спрямоване на вивчення тенденцій розвитку кібербезпеки в ОАЕ та їх впливу на регіональний і міжнародний рівень кіберзахисту.

Важливим аспектом забезпечення кібербезпеки є правове регулювання захисту даних і конфіденційності. Наразі у Раді співробітництва Перської затоки (GCC) немає єдиного національного законодавства, яке б комплексно регулювало ці питання. Відсутність єдиного набору законів ускладнює розробку загальних стандартів захисту даних на регіональному рівні. Проте національні та федеральні конституції країн регіону визнають право на конфіденційність, що закріплюється у галузевих законах, зокрема у сфері банківської справи, охорони здоров'я та телекомунікацій.

Комплексні режими захисту даних все ж існують у певних вільних економічних зонах, таких як Дубайський міжнародний фінансовий центр (DIFC), Катарський фінансовий центр (QFC) та Dubai Healthcare City. Ці режими базуються на європейській моделі захисту даних, зокрема на Директиві ЄС щодо захисту даних. Вони передбачають більш жорсткі правила та контроль за обробкою й зберіганням особистих даних.

Крім того, закони шаріату, які мають велике значення в країнах Перської затоки, забороняють втручання в приватне життя особи та розголошення її секретів без згоди. Втручання допускається лише тоді, коли це відповідає суспільним інтересам. Проте міра покарання за порушення конфіденційності часто залежить від рішення судді і може варіюватися в залежності від обставин конкретної справи.

Вищезгаданий підхід до захисту даних створює певні правові прогалини, що впливає на безпеку кіберпростору в регіоні. Відсутність гармонізованого законодавства ставить під загрозу ефективність боротьби з кіберзлочинністю, що особливо актуально в умовах зростання кіберзагроз на тлі цифровізації економік країн Близького Сходу.

Уряди країн Близького Сходу усвідомлюють зростаючі загрози, пов'язані з оцифруванням, і приділяють дедалі більше уваги розвитку кібербезпеки. Розуміючи необхідність захисту критично важливих інформаційних інфраструктур, держави регіону активізують свої зусилля для підвищення національних можливостей у сфері кіберзахисту. Особливо виділяються в цьому контексті Об'єднані Арабські Емірати, які стали одним із провідних центрів інновацій у сфері кібербезпеки на Близькому Сході.

Згідно зі звітом Global Cybersecurity Index 2020, опублікованим Міжнародним союзом електрозв'язку (ITU), Об'єднані Арабські Емірати досягли значних успіхів у зміцненні своєї кібербезпекової інфраструктури. ОАЕ посіли п'яте місце у світі серед 193 країн за рівнем розвитку кібербезпеки, що демонструє їхню відданість захисту цифрового середовища та здатність ефективно протистояти кіберзагрозам.

Загальний бал ОАЕ становив 98,06 зі 100 можливих, що підкреслює високий рівень кібербезпеки в країні. У порівнянні з попереднім звітом 2019 року, де ОАЕ посіли 33-є місце, цей стрибок до п'ятої позиції у 2020 році демонструє значний прогрес країни у розбудові своєї кіберстійкості [5]. У цьому рейтингу ОАЕ розділили п'яте місце з Росією та Малайзією, що свідчить про їхнє лідерство серед країн із потужною кіберінфраструктурою.

Окреслений результат є прямим наслідком цілеспрямованих зусиль уряду ОАЕ щодо розробки стратегій кібербезпеки, впровадження передових технологій та співпраці на міжнародному рівні. ОАЕ продовжують вдосконалювати свою кібербезпекову систему, що є важливим фактором для підтримки стабільності цифрового середовища та сприяння інноваціям в умовах глобалізованого світу.

ОАЕ виступають маяком стійкості в умовах невпинного технологічного прогресу, активно зміцнюючи свою цифрову інфраструктуру для протидії кіберзагрозам, що постійно еволюціонують. Бачення кібербезпеки країни охоплює не лише поточні виклики, але й спрямоване на створення основи для безпечного цифрового майбутнього на наступні 50 років. Ця проактивна стратегія включає захист від цифрової злочинності та побудову довготривалої кіберстійкості.

Стратегія кібербезпеки ОАЕ підтримується на високому державному рівні, а також ґрунтується на сучасному законодавстві, що відповідає викликам сучасності. Держава активно

впроваджує передові технології та створює регуляторні механізми, які дозволяють оперативно реагувати на нові загрози в цифровому середовищі. Пильний нагляд за дотриманням кібербезпеки та чіткі вказівки на рівні уряду дозволяють ОАЕ не лише вирішувати поточні проблеми, але й забезпечити стійкість та безпеку цифрової економіки в довгостроковій перспективі.

Подорож ОАЕ до цифрової стійкості значною мірою підтримується однозначною підтримкою уряду, що є ключовим фактором у розвитку національної кібербезпеки. Вирішальним етапом стало створення в 2020 році Ради з кібербезпеки ОАЕ, яка отримала мандат на розробку комплексної стратегії для побудови надійної та безпечної кіберінфраструктури в країні. Ця ініціатива стала основою для консолідації зусиль у сфері кіберзахисту на державному рівні та забезпечення координації між різними секторами.

Рада з кібербезпеки відіграє ключову роль у забезпеченні стійкості національної кіберінфраструктури, виступаючи центром організації спільної відповіді на кіберзагрози. До її складу входять експерти з різних галузей, що дозволяє ефективно координувати зусилля держави та приватного сектору у боротьбі з цифровими ризиками. Особливий акцент робиться на захисті бізнесу, який часто стає головною мішенню для кіберзлочинців.

Для посилення кібербезпеки компаній Рада активно співпрацює з низкою провідних світових компаній у рамках моделі державно-приватного партнерства. Наприклад, у 2020 році були підписані попередні угоди з такими гігантами, як Huawei, Amazon Web Services і Deloitte, для спільної роботи у сфері кіберзахисту. Ця співпраця дозволяє ОАЕ скористатися найновітнішими технологіями та експертизою у сфері кібербезпеки, зміцнюючи національну кіберінфраструктуру і забезпечуючи ефективну протидію цифровим загрозам.

За перші три квартали 2023 року в ОАЕ було успішно припинено понад 71 мільйон спроб кібератак [8], що свідчить про високу ефективність комплексних механізмів кіберзахисту, впроваджених у країні. Це є показником того, що стратегічні заходи, ухвалені урядом та приватним сектором, здатні забезпечити стійкість національної кіберінфраструктури перед зростаючими кіберзагрозами.

Загалом шлях ОАЕ до безпечного цифрового майбутнього базується на кількох ключових елементах. По-перше, це проактивні урядові ініціативи, які створюють надійну основу для захисту кіберпростору. По-друге, перспективне законодавство, що адаптується до швидко змінюваного цифрового середовища та впливає на корпоративні практики, допомагає забезпечити відповідність нормам кібербезпеки. По-третє, це відданість держави боротьбі з новими кіберзагрозами та прагнення забезпечити довготривалу стійкість у цифровій сфері.

Важливою частиною забезпечення кібербезпеки в Об'єднаних Арабських Еміратах є реалізація комплексних стратегій, спрямованих на захист цифрової інфраструктури та підтримку розвитку бізнесу і суспільства в умовах швидкої цифровізації. ОАЕ запустили кілька національних і регіональних стратегій, які забезпечують системний підхід до захисту кіберпростору.

Однією з ключових ініціатив є Національна стратегія кібербезпеки ОАЕ [6], спрямована на створення безпечної та потужної кіберінфраструктури в країні. Ця стратегія дозволяє громадянам і підприємствам реалізовувати свої амбіції в цифровому світі, забезпечуючи при цьому високий рівень кіберзахисту. Оновлена версія стратегії була запущена у 2019 році Органом регулювання телекомунікацій і цифрових технологій (TDRA), який відповідає за розвиток сектору ІКТ та цифрову трансформацію ОАЕ.

На додаток до загальнонаціональної стратегії, емірат Дубай реалізує власну Стратегію кібербезпеки Дубая [3], яка була розроблена для зміцнення позицій Дубая як світового лідера в інноваціях, безпеці та кіберзахисті. Ця стратегія спрямована на забезпечення безпечного кіберпростору через впровадження засобів контролю, що гарантують конфіденційність, достовірність, доступність і захист приватності даних.

Стратегія кібербезпеки Дубая охоплює п’ять ключових напрямків:

1. Підвищення кіберстійкості шляхом побудови сильної та захищеної інфраструктури.

2. Забезпечення безпеки інформаційних систем на всіх рівнях, від урядових установ до бізнесу.

3. Розвиток кіберграмотності населення через освіту та навчальні програми.

4. Інновації у сфері кібербезпеки, що сприяють впровадженню нових технологій і методів захисту.

5. Міжнародна співпраця для обміну передовими практиками в галузі кібербезпеки.

В Об'єднаних Арабських Еміратах питання кібербезпеки активно інтегрується в усі сфери, включаючи правову та правоохоронну діяльність. ОАЕ приділяють особливу увагу безпеці даних у кримінальних розслідуваннях, впроваджуючи новітні технології для забезпечення захисту інформації. Яскравим прикладом є впровадження блокчейн-технології Cardano у кримінальні розслідування, що демонструє прагнення країни до використання інновацій для зміцнення кібербезпеки.

Під час Всесвітнього поліцейського саміту в Дубаї місцеві правоохоронні органи презентували пілотний проєкт на базі Cardano, який спрямований на безпечне управління даними, пов'язаними з кримінальними справами. Цей проєкт дозволяє правоохоронцям обмінюватися криміналістичними даними, включаючи специфічні докази, такі як скани куль у бетоні, з міжнародними організаціями, зокрема Інтерполом, що забезпечує високий рівень захисту та конфіденційності.

Система розподіленого реєстру (DLT), розроблена Cardano Foundation, дозволяє правоохоронним органам зберігати докази та інші дані, пов'язані з кримінальними справами, у повній безпеці. Це забезпечує не лише захист від несанкціонованого доступу, але й гарантує цілісність і достовірність інформації, що є важливим фактором у розслідуваннях.

Таким чином, кібербезпека в ОАЕ охоплює всі сектори, включаючи правоохоронні органи, де новітні технології, такі як блокчейн, відіграють ключову роль у забезпеченні захисту даних. Це ще раз підкреслює комплексний підхід ОАЕ до захисту своєї цифрової інфраструктури та створення безпечного середовища в усіх аспектах життєдіяльності [1].

Регулювання кібербезпеки в Об'єднаних Арабських Еміратах відбувається на основі сучасного та всебічного законодавства, яке спрямоване на захист державних і приватних інтересів у цифровій сфері. Одним із ключових документів у цій сфері є Федеральний указ-закон № 34 від 2021 року про боротьбу з чутками та кіберзлочинністю, який набув чинності 2 січня 2022 року [4]. Цей закон забезпечує комплексну правову базу для вирішення проблем, пов'язаних із зловживанням онлайн-технологіями та протидією кіберзлочинам.

Основною метою цього закону є підвищення рівня захисту від кіберзлочинів, що здійснюються за допомогою інформаційних технологій, мереж та онлайн-платформ. Він також спрямований на захист державних вебсайтів і баз даних ОАЕ, боротьбу з поширенням чуток та фейкових новин, захист від електронного шахрайства та забезпечення конфіденційності особистих даних громадян. Закон охоплює широкий спектр кіберзлочинів і встановлює покарання для осіб, які створюють або використовують електронні засоби для злому, атак або підробки державних інформаційних систем та даних.

Серед основних злочинів, зазначених у законі, можна виділити:

- Створення або модифікація роботів для поширення неправдивої інформації.
- Фальсифікація електронних документів.
- Вторгнення в приватне життя інших осіб.
- Підробка медичних даних, банківських рахунків і конфіденційних кодів.
- eBegging (електронне жебрацтво) та інші форми онлайн-шахрайства.
- Публікація контенту, що не відповідає стандартам медіаконтенту.
- Створення або керування вебсайтами для сприяння торгівлі людьми.
- Передача, володіння та використання незаконних фінансових коштів.
- Шантаж, вимагання та образа інших осіб.

Закон також забороняє такі дії, як образа іншої країни чи релігії, реклама вогнепальної зброї та вибухових речовин, введення споживачів в оману шляхом публікації неправдивої рекламної

інформації, а також проведення статистичних досліджень або сприяння демонстраціям без належної ліцензії.

Завдяки цьому закону, ОАЕ створює високі стандарти кібербезпеки, захищаючи як державні інтереси, так і права громадян у цифровій сфері. Така комплексна правова база дозволяє ефективно протидіяти кіберзлочинності та забезпечити безпеку в інформаційному просторі країни.

Об'єднані Арабські Емірати запровадили комплексний підхід до регулювання інформаційної безпеки. Регуляторний орган телекомунікацій та цифрового уряду (TDRA) розробив «Регламент забезпечення інформації ОАЕ» [9], метою якого є підвищення мінімального рівня захисту інформаційних активів та допоміжних систем для всіх організацій у країні. Цей регламент спрямований на створення надійного цифрового середовища в ОАЕ та забезпечення національної кіберстійкості.

Регламент ІА встановлює управлінські та технічні засоби контролю інформаційної безпеки, які організації повинні впроваджувати для створення, підтримки та постійного вдосконалення своєї інформаційної безпеки. TDRA визначає критично важливі суб’єкти, які зобов’язані виконувати вимоги цього регламенту у відповідності до Політики захисту критичної інформаційної інфраструктури ОАЕ (CIIP). Регламент охоплює всі аспекти обробки, зберігання, передачі та використання інформації, будь то у фізичній чи електронній формі, і стосується інформації, яка перебуває у власності, оренді або контролі суб’єктів.

Ключові положення Регламенту ІА включають:

- Опис того, як забезпечується інформаційна безпека на національному, галузевому та організаційному рівнях.
- Використання ризик-орієнтованого підходу до впровадження заходів інформаційної безпеки.
- Чітке окреслення ролей і обов'язків ключових зацікавлених сторін щодо планування, розробки, реалізації та постійного моніторингу і вдосконалення заходів інформаційної безпеки.
- Довідковий каталог загальних засобів контролю інформаційної безпеки, які спрямовані на захист від типових загроз, що використовують відомі вразливості.
- Реалізацію галузевих вимог шляхом надання спеціалізованих засобів контролю для вирішення конкретних загроз у різних галузях.
- Підхід до поетапного впровадження, який допомагає усунути найпоширеніші загрози та сприяє поступовому впровадженню заходів інформаційної безпеки.
- Оцінку відповідності щодо інформаційної безпеки та підхід TDRA до оцінки ефективності цих заходів.
- Створення засобів для комунікації між організаціями та секторами, що сприятиме обміну інформацією та формуванню національної обізнаності про ситуацію у сфері кібербезпеки.

Цей регламент є важливим кроком у підвищенні національної кіберстійкості та ефективної протидії зростаючим кіберзагрозам. Він дозволяє забезпечити захист як державних, так і приватних інформаційних активів, впроваджуючи найсучасніші засоби контролю і технології для захисту національної кіберінфраструктури.

Важливим елементом національної стратегії кібербезпеки Об'єднаних Арабських Еміратів є діяльність групи реагування на надзвичайні ситуації з комп'ютерами (aeCERT). Ця група була створена з метою покращення стандартів інформаційної безпеки в ОАЕ та захисту IT-інфраструктури країни від потенційних кіберзагроз і порушень. aeCERT відіграє ключову роль у зміцненні національної кіберстійкості, забезпечуючи координацію дій між державними органами та приватними компаніями для запобігання кіберінцидентам і мінімізації їхніх наслідків.

Основною місією aeCERT є забезпечення більш безпечного кіберпростору для громадян та жителів ОАЕ шляхом моніторингу, виявлення та реагування на кіберзагрози. Група також займається розповсюдженням інформації про нові загрози, уразливості в системах і

кіберінциденти, що дозволяє підвищити рівень обізнаності серед громадян і бізнесу про поточні ризики та способи їхньої мінімізації.

Одним із важливих аспектів діяльності aeCERT є оперативне реагування на кібератаки та їхнє усунення, що дозволяє запобігати серйозним наслідкам для національної безпеки та економіки. Група також сприяє підвищенню стандартів безпеки в державних і приватних установах через розробку рекомендацій та надання технічної підтримки щодо захисту інформаційних систем.

Отже, aeCERT є важливим інструментом у боротьбі з кіберзагрозами, оскільки сприяє створенню захищеного цифрового середовища в ОАЕ та підвищенню кіберстійкості на всіх рівнях – від приватних користувачів до національних інституцій [7].

У рамках підвищення рівня кібербезпеки та залучення громадськості до боротьби з кіберзагрозами, Об'єднані Арабські Емірати ініціювали низку проектів, спрямованих на забезпечення цифрової стійкості та підвищення обізнаності населення щодо загроз у кіберпросторі.

Однією з ключових ініціатив є «Кіберпульс» (Cyber Pulse). Ця програма націлена на залучення широких верств населення до участі у заходах із забезпечення кібербезпеки, зокрема шляхом інформування про підозрілу онлайн-активність і кроки, необхідні для запобігання електронному шахрайству, особливо фішингу. У рамках цієї ініціативи організовуються навчальні курси, семінари та лекції з кібербезпеки, під час яких учасники дізнаються, як захистити себе в цифровому світі. Перший етап ініціативи був орієнтований на жінок і сім'ї, тоді як другий – на студентів, які є однією з найбільш вразливих категорій у кіберпросторі.

Ще однією важливою ініціативою є Salim – онлайн-консультант з кібербезпеки, яку було розроблено Командою реагування на надзвичайні ситуації в області комп'ютерів ОАЕ (aeCERT) у співпраці з Aqdar. Під гаслом «На шляху до безпечної кіберкультури» цей проект націлений на поширення знань про кібербезпеку серед усіх верств суспільства та формування покоління, яке володіє інтегрованими знаннями з інформаційної безпеки та здатне діяти уважно і обережно в Інтернеті.

Також важливою є програма «Посли ОАЕ електронної безпеки», яку реалізує TRA. Ця ініціатива спрямована на підготовку найкращих студентів ОАЕ для виконання ролі послів у просуванні обізнаності про кібербезпеку. Студенти, які беруть участь у програмі, допомагають поширювати знання серед своїх однолітків, а також в інших спільнотах, підвищуючи загальний рівень кіберграмотності в країні.

У 2016 році поліція Дубая у співпраці з Управлінням з регулювання телекомунікацій і цифрових технологій (TDRA) запустила ще одну важливу ініціативу – кампанію з підвищення обізнаності про кібершантаж. Ініціатива під назвою Al Ameen націлена на захист жертв від кібершантажу та притягнення злочинців до відповідальності незалежно від їхнього місцезнаходження. Кампанія також передбачає співпрацю з Інтерполом для міжнародного переслідування осіб, які займаються шантажем в Інтернеті [2].

Завдяки цим ініціативам, ОАЕ демонструють проактивний підхід до кібербезпеки, залучаючи не тільки державні установи, а й широкі верстви населення до боротьби з кіберзагрозами.

ОАЕ є прикладом держави, яка активно розвиває свої можливості у кіберзахисті, втілюючи проактивні урядові ініціативи, сучасне законодавство, інноваційні технології та співпрацю на міжнародному рівні. По-перше, країна розробила Національну стратегію кібербезпеки, що охоплює широкий спектр ініціатив, спрямованих на підвищення кіберстійкості держави та забезпечення захисту від кіберзагроз на всіх рівнях – від урядових установ до приватного сектору. Важливим елементом цієї стратегії є спільна робота з міжнародними партнерами, що дозволяє ОАЕ впроваджувати передові рішення та адаптуватися до нових викликів у кіберпросторі.

По-друге, ОАЕ приділяють значну увагу захисту даних через створення правової бази для боротьби з кіберзлочинністю, включаючи Федеральний указ-закон № 34 від 2021 року, який

охоплює різноманітні форми кіберзлочинів, від фальсифікації електронних документів до кібершантажу.

По-третє, важливим кроком стало створення aeCERT – групи реагування на надзвичайні ситуації з комп'ютерами, яка координує роботу з протидії кіберзагрозам і підвищує рівень безпеки цифрового середовища в ОАЕ. Вони працюють не тільки з державними структурами, але й з приватним сектором, сприяючи підвищенню обізнаності та реагуванню на інциденти.

Додатково, ініціативи, такі як Cyber Pulse та Salim, демонструють націленість на залучення громадян до кібербезпеки через освіту та підвищення обізнаності. Ці програми сприяють формуванню кіберкультури в суспільстві, що є критично важливим для підтримки національної кіберстійкості.

Загалом, ОАЕ посідають лідерські позиції у світових рейтингах кібербезпеки, завдяки стратегічному підходу, законодавчим ініціативам та технічним рішенням, що забезпечують надійний захист національних інтересів у цифровому світі. ОАЕ продовжують демонструвати проактивну позицію у створенні безпечного кіберпростору, готуючи підґрунтя для успішного розвитку своєї цифрової економіки на найближчі десятиліття.

Список використаних джерел

1. ОАЕ використають блокчейн Cardano для підвищення безпеки кримінальних розслідувань. URL: https://fintechinsider.com.ua/oae-vykorystayut-blokchejn-cardano-dlya-pidvyshhennya-bezpeky-kryminalnyh-rozsliduvan/ (дата звернення: 21.09.2024).
2. Cyber safety and digital security. URL: https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security (last access: 21.09.2024).
3. Dubai Cyber Security Strategy. URL: https://u.ae/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-cyber-security-strategy (last access: 21.09.2024).
4. Federal Decree-Law No. (34) of 2021 On Countering Rumors and Cybercrimes. URL: https://uaelegislation.gov.ae/en/legislations/1526 (last access: 21.09.2024).
5. Global Cybersecurity Index 2020. URL: https://www.itu.int/hub/pubs/ (last access: 21.09.2024).
6. The UAE’s National Cybersecurity strategy. URL: https://www.wam.ae/en/details/1395302769739 (last access: 21.09.2024).
7. TRA. URL: https://tdra.gov.ae/en/aecert (last access: 21.09.2024).
8. UAE has thwarted 71 million cyber attacks this year, authorities say. URL:https://www.thenationalnews.com/uae/2023/11/03/uae-has-thwarted-71-million-cyber-attacks-this-year-authorities-say/ (last access: 21.09.2024).
9. UAE Information Assurance Regulation. URL: file:///C:/Users/%D0%98%D0%B2%D0%B0%D0%BD%D0%BA%D0%B0/Downloads/UAE%20IA%20Regulation%20v11%201.pdf (last access: 21.09.2024).

УДК 659.2.012.8:004.056(063)
К 38

Кібербезпека в транскордонному співробітництві. Наукове видання (Збірник тез доповідей) Закарпатського угорського інституту імені Ференца Ракоці II / Редактори: Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д, Ганна Мелеганич та Оксана Мулеса. Берегове: ЗУІ ім. Ференца Ракоці II, 2024. – 166 с. (українською, англійською та угорською мовами)

ISBN 978-617-8143-27-5 (м'яка обкладинка)
ISBN 978-617-8143-28-2 (PDF)

Збірник містить тези доповідей міжнародної науково-практичної конференції «Кібербезпека в транскордонному співробітництві», яка відбулася 15–16 жовтня 2024 року в місті Берегове. Матеріали конференції охоплюють широке коло питань, пов'язаних із забезпеченням кібербезпеки в умовах посиленої глобальної взаємодії. Зокрема, тези доповідей конференції досліджують сучасні кіберзагрози, інтеграцію штучного інтелекту в системи безпеки, трансформації методів кіберзахисту та обмін закордонним досвідом. Учасниками конференції були обговорені підходи до вирішення актуальних питань інформаційної безпеки на міжнародному рівні та надання практичних знань студентам, фахівцям і дослідникам. Організатори конференції: Закарпатський угорський інститут імені Ференца Ракоці II та Ужгородський національний університет. Співорганізатори: Національний авіаційний університет, ІТ Степ Університет, Пряшівський університет у Пряшеві та Північний університетський центр у Бая-Маре Технічного університету Клуж-Напока.

Наукове видання

КІБЕРБЕЗПЕКА В ТРАНСКОРДОННОМУ СПІВРОБІТНИЦТВІ

Міжнародна науково-практична конференція
Берегове, 15–16 жовтня 2024 року

Збірник тез доповідей

2024 р.

Рекомендовано до видання у друкованій та електронній формі (PDF)
рішенням Вченої ради Закарпатського угорського інституту імені Ференца Ракоці II
(протокол №10 від «21» листопада 2024 року)

Підготовлено до видання кафедрами історії та суспільних дисциплін, обліку і аудиту, математики та інформатики Закарпатського угорського інституту імені Ференца Ракоці II і кафедрами програмного забезпечення систем, міжнародних студій та суспільних комунікацій Ужгородського національного університету спільно з Видавничим відділом ЗУІ ім. Ф. Ракоці II

За редакцією:
Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д,
Ганна Мелеганич та Оксана Мулеса

Технічне редагування: *Адам Доровці, Олександр Добош та Ігор Лях*
Коректура: *авторська*
Дизайн обкладинки: *Вівієн Товт*
УДК: *Бібліотека ім. Опацої Чере Яноша при ЗУІ ім. Ф.Ракоці II*

Відповідальний за випуск:
Олександр Добош (начальник Видавничого відділу ЗУІ ім. Ф.Ракоці II)

Публікації науково-педагогічних працівників і студентів Ужгородського національного університету виконано в рамках держбюджетної теми ДБ-921М «Захист інформаційної безпеки при управлінні проєктами міжнародного співробітництва на засадах гарантування національної безпеки України» за підтримки Міністерства освіти і науки України.

Проведення конференції та друк видання здійснено за підтримки уряду Угорщини.

Видавництво: Закарпатський угорський інститут імені Ференца Ракоці II (адреса: пл. Кошута 6, м. Берегове, 90202. Електронна пошта: foiskola@kmf.uz.ua; kiado@kmf.uz.ua) *Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції Серія ДК 7637 від 19 липня 2022 року*
Друк: ТОВ «РІК-У» (адреса: вул. Карпатської України 36, м. Ужгород, 88006. Електронна пошта: print@rik.com.ua) *Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції Серія ДК 5040 від 21 січня 2016 року*

Шрифт «Times New Roman».
Папір офсетний, щільністю 80 г/м². Друк цифровий. Ум. друк. арк. 13,49.
Формат 70x100/16.

ISBN 978-617-8143-27-5