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

КІБЕРБЕЗПЕКА У СФЕРІ КУЛЬТУРИ КІБЕРСТІЙКОСТІ

CYBER SECURITY IN THE FIELD OF CYBER RESILIENCE CULTURE

KIBERBIZTONSÁG A KIBERREZILIENCIA TERÜLETÉN

Віталій АНДРЕЙКО
кандидат історичних наук, доцент
доцент кафедри міжнародних студій та суспільних комунікацій,
Леонід ДЕРБАК
магістр 2-го року навчання спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
ДВНЗ «Ужгородський національний університет»

ОСОБЛИВОСТІ ДІЯЛЬНОСТІ США У СФЕРІ КІБЕРБЕЗПЕКИ

У сучасному цифровому світі кібербезпека стала важливим національним питанням для урядів різних країн світу. Цифрова трансформація, зростаюча залежність від інформаційно-комунікаційних технологій, інтенсифікація кіберзагроз стали руйнівним потенціалом для багатьох національних урядів. Сполучені Штати, сьогодні, є однією з перших країн світу в якій політична еліта здійснює практику захисту свого національного інформаційного поля від несанкціонованого втручання.

Стимулом для розвитку політики кібербезпеки став терористичний акт від 11 вересня 2001 р. Наступні терористичні атаки на інформаційні ресурси, які були розташовані на території США, завдавали значних фінансових збитків економіці країни. Адміністрація президента Джорджа Буша-мол. почала роботу над концептуальними засадами американської політики кібербезпеки. Так, у 2003 р. було прийнято «Національну стратегію захисту кіберпростору». Стратегія містила наступні положення: запобігання кібератакам на критично важливі об'єкти; зниження вразливості США перед кіберзагрозою; мінімізація збитків від кібератак.[1]

Новий етап стратегії боротьби із кіберзагрозою пов'язаний із приходом до влади Барака Обами (2009-2017). У травні 2009 р. Б. Обама виступив із промовою «Міжнародна стратегія США для кіберпростору». Ключовим завданням стратегії стало формування механізму глобального управління (global governance) у світовому кіберпросторі.

Для реалізації нового проекту було створено нову структуру на чолі з координатором з кібербезпеки, а посаду координатора зайняв Крістофер М. Пейнтер. Особливе місце у практиці реалізації цього проекту відводилося партнерським відносинам США із союзниками. За Барака Обами, були відзначені ініціативи, що висувалися Сполученими Штатами в «Групі двадцяти партнерів». У рамках співпраці із партнерами проводилися операції американської команди з політики кібербезпеки. Її результати направлялися до держав-союзників США для вивчення намірів і діяльності в кіберпросторі потенційних американських противників (насамперед росії та Китаю) та подальшої нейтралізації кіберзагроз. У 2018 р., США разом із партнерами провели 24 операції в 14 країнах світу. В ході проведених спільних операцій було виявлено 30 небезпечних шкідливих програм.[2]

Б.Обама продовжив практику концептуального оформлення політики стримування у кіберпросторі. Так, було прийнято «Міжнародну стратегію щодо дій у кіберпросторі» (2011), «Доповідь Міністерства оборони США з питань політики кіберпростору» (2011). Було закріплено право США при реагуванні на кібератаки використовувати будь-який інтелектуальний інструментарій для захисту національного інформаційного поля США.

Приход до влади Дональда Трампа відкрив нову амбіційну сторінку в інформаційній сфері США. Була прийнята стратегія «America first». Вже у травні 2017 р. президент видає указ «Про зміцнення кібербезпеки федеральних мереж та критичної інфраструктури». Документ було покладено до основи внутрішньої національної кіберстратегії США, а пізніше трансформовано до змісту зовнішньополітичних амбіцій США. Адміністрація Трампа спрямовувала інтелектуальний потенціал на захист кіберпростору задля сприяння економічному розвитку та процвітанню країни. У кіберстратегії було визначено наступні напрями: просування американського впливу на кіберпростір що забезпечить американське процвітання; збереження миру через зміцнення сили; захист американського народу та американського способу життя.

У стратегії Д.Трампа зазначалося, головним викликом США є відродження глобальної стратегічної конкуренції між великими державами, насамперед із Китаєм. Принципово новим у документі Трампа став акцент на оборонному та наступальному характері політики США у сфері кібербезпеки. Так, радник з національної безпеки США, Джон Болтон у травні 2018 р. заявив, що американське керівництво має стійкій намір брати участь у наступальних операціях» у кіберпросторі. Метою такої активності було «стримування неприпустимої поведінки традиційних ворогів США» у кіберсфері: Ірану, Китаю, росії та Північної Кореї.[3]

Від моменту обранням президента США Джо Байдена розпочався новий етап американської політики у сфері кібербезпеки. У своєму виступі Байден констатував, що кіберзагрози стають ключовим викликом для світової стабільності та національної безпеки.

Першими документами у сфері кібербезпеки став указ Байдена «Про кібербезпеку федеральних органів влади США» та «Меморандум з національної безпеки». У документах було закріплено мету США у сфері кібербезпеки. Пріоритетним завданням було відзначено захист громадян та операторів – об'єктів критично важливої інфраструктури. Особлива увага приділялася проблемам кібербезпеки у контексті нових гібридних загроз.

Особлива увага приділялася взаємодії з приватним сектором. Відповідно у серпні 2021 р. було ініційовано проведення зустрічі з керівниками найбільших технологічних компаній (Google, Amazon, Microsoft, Apple), страхових організацій, банків та освітніх установ. За підсумками зустрічей були висунуто низку ініціатив. Ініціативи були орієнтовані на зміцнення державно-приватного партнерства у сфері кібербезпеки. Було висунуто наступні напрямі координації зусиль: нарощування потенціалу в кіберпросторі; підвищення якості критичної інфраструктури; розвиток сектору кібербезпеки, як окремої національної галузі; забезпечення галузі кваліфікованою робочою силою.[4]

До того ж, при державному департаменті США було створено Бюро з питань кіберпростору та цифрової політики. На нове Бюро було покладено відповідальність за узгодження прийнятих політичних рішень у галузі кібербезпеки, та додана функція просування цифрової політики.

Таким чином, за чверть століття Сполучені Штати здійснили помітний крок від визнання кіберпроблеми до практики організації процесу захисту свого національного інтересу у світовому кіберпросторі. Важливим компонентом американської кіберполітики незмінно залишалася стратегія стримування конкурентів (КНР, рф, Іран КНДР) та допомога партнерам. США прагнуть сформувати порядок, якій буде заснований на правилах. Такій підхід передбачає вироблення і прийняття принципів для певного кола держав-партнерів і наступна їх імплементація у світову практику.

Список використаних джерел:

1. The National Strategy to Secure Cyberspace // The White House, February 2003. Електронний ресурс. – URL: https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.
2. International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World // The White House. Електронний ресурс.
   URL: http://www.pircenter.org/media/content/files/9/13480895180.pdf.
3. National Cyber Strategy 2018. USA. September 2018. Електронний ресурс. –URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
4. The United States of America Cyberspace Solarium Commission // U.S. Cyberspace Solarium Commission. Washington, DC, 2021. - Електронний ресурс.
   URL: https://www.solarium.gov/report.

Інна ЧЕРВІНСЬКА
доктор педагогічних наук, професор,
професор кафедри початкової освіти
та освітніх інновацій,
завідувач творчою навчально-науковою лабораторією
«Гірська школа Українських Карпат»
Прикарпатського національного університету
імені Василя Стефаника

КІБЕРБУЛІНГ В ОСВІТНЬОМУ СЕРЕДОВИЩІ: МЕХАНІЗМИ РЕАГУВАННЯ ТА ПРОФІЛАКТИКИ

Актуальність проблеми булінгу та його різновидів у сучасному освітньому середовищі закладів загальної середньої освіти засвідчує її затребуваність в освітянської спільноти, батьків, представників громадськості. Однак, незважаючи на таку популярність, ця проблема задля її успішного вирішення вимагає поєднання наукових розвідок учених та напрацювань й досвіду педагогів-практиків.

Адже згідно результатів статистичних даних про кібербулінг в освітньому середовищі, його показники зростають. Особливе зростання помічено в період воєнного стану в якому ось уже третій рік перебуває Україна.

Впродовж останніх років явище насильства в шкільному середовищі викликає певний інтерес дослідників з багатьох освітніх галузей. Відносно недавно кібербулінг став предметом вивчення і в Україні, зокрема у працях вчених Т. Миронюк, Л. Найдьонова, О. Лапа, О. Момот, І. Лубенець та інших. Посилює цей інтерес прийняття Закону України «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)» (2019) [1].

Ідею розгортання кампанії протидії булінгу, розпочату державними й громадськими організаціями, підтримали засоби масової інформації, освітянські спільноти.

Проте, варто зазначити, що для світового наукового простору ця проблема не є новою. Вперше її дослідженням почали займатися на початку 70-х років минулого століття вчені П.-П. Хайнеманн (1972), Д. Ольвеус (1973) та А. Пікас (1975) зі Скандинавії [1]. Що й започаткувало процес вивчення різних видів цькування серед школярів.

Згодом зазначені локальні дослідження переросли у міжнародні та уможливили започаткування співпраці між науковими товариствами різних країн. Це привернуло увагу освітян, політиків, батьків. З інтенсивним розвитком інтернету, поширенням спілкування учнів у соцмережах проблема булінгу в шкільному середовищі перейшла в цькування особистості в соціальних мережах та інтернеті й отримала назву – *кібербулінг.*

Реалії сьогодення підтверджують, що проблема кібербулінгу як прояву агресії в освітньому середовищі стає все більш значущою. Умови сучасного суспільства сприяють поширенню жорстокості та насильства, які все частіше проявляються у відносинах між молодими людьми.

У цьому контексті варто наголосити, що шкільне цькування певним чином різниться від понять «конфлікт», «примус», «приниження», оскільки характеризується як об'єктивно існуючі впродовж певного періоду, регулярні приниження гідності та знущання над учнями з метою шантажу, залякування школярів через соціальні мережі. Адже у віртуальному світі, як і в реальному житті, на молодих людей чатує багато небезпек. І однією з них є «віртуальне цькування» або «кібербулінг».

Кібербулінг (з англ. bull – бик; *агресивно нападати, чіплятися, провокувати, тероризувати*). Це – розсилка повідомлень образливого й загрозливого змісту, поширення в інтернеті неправдивої і принизливої інформації, а також фото та відео за участю об’єктів цькування.

Таким чином, під кібербулінгом розуміємо способи публічного приниження жертви за допомогою цифрових технологій. До проявів кібербулінгу в шкільному середовищі відносимо й сучасні інтернет-ігри «Синій кит», «Червона сова», «Розбуди мене о…», «Голуба принцеса»

та інші. Через відеоконтент соціальних мереж так звані «куратори» намагаються вплинути на ще не зовсім стійку дитячу психіку, надсилають учням різні завдання, організовують пошукові квести, а в комплексі – можуть й довести до самогубства. Роблять це злочинці шляхом погроз вбити когось із близьких із застосуванням сильного психологічного тиску.

Аналіз соціальних мереж підлітків та опрацювання статистичних даних у відкритих джерелах дає підстави стверджувати, що кібербулінг присутній в усіх сферах діяльності учнівської молоді, тому маємо досить велику кількість форм кіберцькування.

Кібербулінг – це активна дія, яка спрямована на завдання психологічної травми зростаючій особистості, шляхом приниження, образ, відкритого шантажу за допомогою соціальних мереж, телефону, знімання на відео принижень, погроз, бійок та поширення без дозволу цього контенту в соціальних мережах.

Кібербулінг має структуру умовного трикутника, яка містить три компоненти: кібербулер, жертва та спостерігачі. Ініціаторами цькування – кібербулерами зазвичай є учні, які мають певні проблеми з психічним розвитком, страдають так званим «нарцисизмом», прагнуть влади, намагаються самоствердитися за рахунок інших школярів.

Кібербулінг – це новітня форма дитячої агресії, що відображає жорстоку поведінку інших осіб з метою нашкодити, принизити, образити молоду людину й не тільки, шляхом використання різноманітних інформаційно-комунікативних засобів, електронної пошти та розсилки в соціальних мережах. Зазвичай терміном «кібербулінг» позначають різні форми агресивної поведінки в мережах та спілкування за допомогою сучасних медіаресурсів.

До типових характеристик кібербулінгу відносимо:

- *систематичність* (повторюваність) дій кібербулера;
- *наявність сторін протидії* – кривдник (булер), потерпілий (обрана жертва), спостерігачі (за наявності);
- *дії або бездіяльність кривдника*, наслідком яких є нанесення або заподіяння психічної або фізичної травми, приниження, страх, тривога, підпорядкування потерпілого інтересам кривдника;
- *соціальна ізоляція потерпілого*;
- *дія кібербулінгу може бути персоніфікованою та анонімною* (жертва не здогадується, хто є кривдником);
- *швидке поширення у віртуальному просторі;*
- *від проявів кібербулінгу неможливо сховатися* (на відміну від булінгу в класному колективі);
- *спрямування на завдання психологічної* або ж фізичної шкоди молодій людині;
- *фінансова зацікавленість,* шахрайські наміри та дії.

За сучасних реалій воєнного стану найпоширенішими видами кібербулінгу в освітньому середовищі виступають: публічне розголошення особистої інформації, ошуканство, відчуження (ізоляція), перепалка (флеймінг), самозванство, наклепи, нападки (домагання), фішинг, хепіслепінг, кіберпереслідування, онлайн-грумінг, тролінг тощо.

Чек-лист порад, які допоможуть запобігти кібербулінгу в освітньому середовищі.

1. *Кіберпес.* Для боротьби з кібербулінгом створено чат-бот проти кібербулінгу. Кіберпес допоможе дізнатись більше про кібербулінг і його прояви, видалити образливі коментарі з соціальних мереж, підкаже контакти служб допомоги. Здобувачі освіти можуть спілкуватися Кіберпсом у Viber. У чат-боті можна довідатися про те, як діяти учням студентам, батькам, педагогам, якщо вони стали жертвою кібербулінгу.

Інформація у чат-боті допоможе визначити вид кібербулінгу, як самостійно видалити образливі матеріали з соціальних мереж, а також куди звертатись за допомогою.

У чат-боті «Кіберпес» міститься детальна інформацію про кібербулінг, як він проявляється в соцмережах, як швидко визначити загрозливий контент, що містить кібербулінг. Надаються дієві поради про те, що робити, якщо ви стали жертвою кібербулінгу, як правильно видалити матеріали, що містять прояви різних видів цькування.

2. З метою запобігання проявам булінгу та кібербулінгу в освітньому середовищі створено спеціальний проєкти з протидії булінгу в школі *«Стоп, шкільний терор» або («Безпечна школа»).* Концепція *«Школа, безпечна і дружня до дитини». «Коли вашу дитину цькують»* – посібник для батьків школярів.

3. Міністерство цифрової трансформації України за підтримки ЮНІСЕФ запустило новий освітній серіал *«Про кібербулінг для підлітків*». Щоб переглянути всі серії та отримати сертифікат, необхідно авторизуватися в системі.

Цькування в освітньому середовищі є більш прихованим, ніж в інших молодіжних спільнотах. Воно стає більш жорстокішим, продуманим, добре спланованим.

Зазвичай це цілеспрямоване та усвідомлене приниження людини і педагогічній спільноті необхідно докласти всіх зусиль для організації ефективної роботи щодо профілактиці кібербулінгу в освітньому середовищі.

Діяльність із запобігання кібербулінгу серед здобувачів освіти має бути орієнтована на виховання ціннісного ставлення школярів до свого життя та здоров'я, створення позитивної атмосфери з метою сприяння успішній соціалізації кожного учасника освітнього процесу.

Список використаних джерел:

1. Алексєєнко Т.Ф. Булінг і мобінг: причини розвитку і шляхи профілактики. Особистість у просторі виховних інновацій : матеріали Всеукраїнської науково-практичної конференції, м. Івано-Франківськ, 19 жовтня 2018 р. Івано-Франківськ : НАІР, 2018.
2. Закон України «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)» (2019) [ ]. URL https://zakon.rada.gov.ua/laws/show/2657-viii#Text
3. Кіричевська Є.В. Насильство в загальноосвітніх навчальних закладах: стратегії подолання. Практична психологія та соціальна робота. 2010. Вип. 8. С. 4–10.

Олександр БАТЮКОВ
завідувач відділу сталого розвитку громад та організації роботи освітніх хабів, провідний юрисконсульт Донецького обласного інституту післядипломної педагогічної освіти
Світлана ЛУЦЕНКО
керівник апарату Маріупольської районної державної адміністрації

ПСИХОЛОГО-ПРАВОВІ НАСЛІДКИ КІБЕРБУЛІНГУ: ВПЛИВ ТА МЕХАНІЗМИ ЗАХИСТУ

Слід погодитися, що перехід від особистого спілкування до онлайн-комунікації створює нові виклики для соціальних взаємодій, що, як наслідок, призводить до появи таких явищ, як кібербулінг, які все більше стають об'єктом досліджень у науковій літературі.

Л. Найдьонова характеризує кібербулінг як використання інформаційно-комунікаційних технологій для заподіяння нападів на однолітків – не тільки в шкільному середовищі, але і в його онлайн аналогах відкритого інформаційного простору, в соціальних мережах, опосередкованому технологіями між особовому спілкуванню [1].

До основних психологічних особливостей кібербулінгу варто віднести високу проникність, швидкість поширення інформації, широту аудиторії, використання технічних засобів зв'язку, відсутність безпосереднього міжособистісного контакту, анонімність агресора тощо. Серед наслідків – проява у жертв фізичних, емоційних та психосоціальних аспектів.

За даними дослідження UNICEF, в Україні близько 50% підлітків визнали, що були жертвами кібербулінгу, а кожна третя дитина прогулювала школу через кібербулінг [2].

Захист від кібербулінгу в освітньому, зокрема, середовищі включає кілька ключових механізмів. Перш за все, важливим є підвищення рівня обізнаності через тренінги та освітні програми для всіх категорій учасників освітнього процесу. Превентивні заходи передбачають впровадження певної «політики» щодо кібербулінгу та формування культури поваги. Психологічна підтримка жертв кібербулінгу є важливим аспектом, як і можливість оперативного реагування через анонімні повідомлення про інциденти. Співпраця з батьками, проведення тренінгів та заходи з юридичною складовою також сприяють створенню безпечного освітнього середовища.

На законодавчому рівні ці питання здебільшого передбачені ратифікованою Конвенцією ООН про права дитини (далі – Конвенція), Кодексом України про адміністративні правопорушення (далі – КУпАП), Законами України «Про освіту», «Про охорону дитинства» (далі – Закони), іншими підзаконними актами. Конвенція закріплює право дитини на захист від будь-яких форм насильства, зокрема, забезпечувати захист прав дітей у цифровому просторі. КУпАП передбачає адміністративну відповідальність за дії, пов'язані з кібербулінгом. Закони, разом з тим, визначають обов'язки закладів освіти та учасників освітнього процесу щодо створення безпечного освітнього середовища, здійснення та проведення заходів з метою попередження правопорушень тощо.

Таке явище як кібербулінг є доволі серйозним викликом освітньої складової в Україні, що має на меті як психологічні, так і правові наслідки для його жертв та правопорушників. Ефективний захист від нього вимагає комплексного підходу: психологічну реабілітацію, правове регулювання, притягнення до відповідальності, підвищення обізнаності суспільства та посилення правового контролю в цьому напрямку.

Список використаних джерел:

1. Найдьонова Л.А. Кібербулінг у підлітковому рейтингу інтернет-небезпек. Психологічні науки: проблеми і здобутки. 2018. Вип. 1. С. 141–159.
2. Дослідження UNICEF «Які вони, українські підлітки: про соцмережі, секс, алкоголь, спорт, довіру до батьків та друзів. Дослідження». URL: https://life.pravda.com.ua/society/2019/05/22/236974/

Євгенія ГАЙОВИЧ
аспірант кафедри загальної педагогіки
та педагогіки вищої школи,
начальник відділу електронного навчання центру
інформаційних технологій
ДВНЗ «Ужгородський національний університет»

КЕЙС-СТАДІ: БЕЗПЕКА МЕСЕНДЖЕРІВ В ОСВІТІ

Ключові слова: освітній процес, освітні платформи, месенджери, ІТ-інструменти, кібербезпека.

Сучасний освітній процес дедалі більше характеризується використанням інформаційних технологій та систем, а освітньо-наукова комунікація здійснюється через різні месенджери і платформи. З огляду на питання онлайн-присутності в інформаційному, науковому, освітньому цифровому просторах виникає потреба дослідити безпеку каналів комунікації та ефективність у забезпеченні конфіденційності, захисту персональних даних і збереження інформації. Месенджери широко застосовуються для організації навчального процесу, але недостатня увага до питань кібербезпеки може створювати серйозні загрози для учасників освітнього середовища.

Наукова проблема полягає в дослідженні рівня безпеки найбільш популярних месенджерів, які використовуються в освітніх установах, на основі аналізу їхніх функціональних можливостей і систем захисту даних та окресленні основних кіберзагроз, пов'язаних з використанням месенджерів в освітньому процесі. Мета – оцінка безпеки популярних месенджерів в освітньому середовищі та надання рекомендацій щодо їх використання.

Станом на 2024 рік існує чимала кількість месенджерів. Німецька компанія зі збору та візуалізації даних Statista проаналізувала ринок використання месенджерів та визначила, що у 2024 році перші 5 сходинок рейтингу серед застосунків у світі посідають: WhatsApp (2 млрд користувачів), Facebook Messenger (1,3 млрд користувачів), WeChat (1,2 млрд користувачів), QQ (648 млн користувачів), Telegram (500 млн користувачів). Для порівняння, згідно з даними компанії InMind, в Україні у 2024 році найпопулярнішими месенджерами є Viber (73,6%), Facebook Messenger (42,7%), Telegram (31,6%), WhatsApp (25,3%), Skype (19,2%).

За аналізом вибірок можна зробити висновок, що ці месенджери спрямовані на особисте використання, де рівень безпеки має не менш важливе значення, ніж для установ, і зокрема освітніх. На жаль, часто месенджери особистого використання стають інструментами комунікації в робочому середовищі, у тому числі і в рамках освітнього процесу, що є не зовсім коректним. Українські дослідники та науковці, до прикладу С.Л. Лебедєва та М.К. Лебедєв [1], аналізують месенджери з точки зору зручності використання та функціоналу, але не з точки зору безпеки.

Найбільшу прихильність освітян отримали Viber та Telegram. У період карантину використання цих месенджерів серед освітян Закарпатської області складало понад 90%. Щодо безпеки, то ці застосунки не входять у топ найбезпечніших. За даними Cyber Division, Інститут дослідження кібервійни ICWR, Telegram не є безпечним месенджером і не рекомендується у використанні як для приватного спілкування, так і корпоративного, через наскрізне шифрування повідомлень не відбувається за замовчуванням, як у Signal, Threema чи WhatsApp. Це окрема функція у вигляді секретних чатів. До 99% спілкування в цьому месенджері відбувається поза «секретними» чатами. Весь контент, який продукується в Telegram за відсутності наскрізного шифрування за замовчуванням (метадані, чати, фото, відео, аудіо), зберігається на серверах назавжди, навіть якщо користувач видалить дані з телефону. Частина серверів Telegram знаходяться у росії, за даними OSINT, а також використовує для передачі мережевого трафіку лише російські компанії – RETN і LLC GLOBALNET. У цьому випадку так само адміністратори мережі можуть легко моніторити трафік, який є незашифрованим [2].

Платформи для комунікації в закладах освіти з акцентом на безпеку мають відповідати високим стандартам захисту даних та конфіденційності. Для цього потрібне комплексне рішення, а саме розгортання відповідних воркспейсів, які включатимуть додатки та застосунки для швидкої комунікації, зберігання даних та багаторівневе управління ними, а також забезпечуватимуть надійний рівень безпеки. Такі ресурси використовуються більше в закладах вищої освіти і менше в закладах загальної середньої та професійної.

Google Workspace – це пакет спеціалізованого хмарного програмного забезпечення й інструментів для спільної роботи від компанії Google. Продукти доступні широкому загалу безкоштовно, однак у версіях Google Workspace передбачені корпоративні функції – спеціальні адреси електронної пошти в домені компанії. Доменні облікові записи мають ряд переваг та надають ширший спектр можливостей. Google використовує наскрізне шифрування для всіх даних, що передаються між користувачами. Google Chat забезпечує шифрований прямий обмін повідомленнями, групові розмови та простори, які дозволяють користувачам створювати, призначати завдання та ділитися файлами в межах робочого середовища на додаток до спілкування в чаті. Платформа відповідає вимогам GDPR та стандартам захисту конфіденційності даних. До особливостей можна віднести адміністрування прав доступу, можливість контролю з боку IT-адміністраторів закладу.

Microsoft Teams – центр для командної роботи в Office 365 від Microsoft, який інтегрує користувачів, вміст і засоби, необхідні команді для ефективнішої роботи. Платформа забезпечує високий рівень захисту через наскрізне шифрування, двофакторну автентифікацію та інтеграцію з Microsoft 365, яка відповідає стандартам GDPR та інших регуляцій. Дані зберігаються в зашифрованому вигляді, що унеможливлює несанкціонований доступ. Створення приватних каналів, захищений обмін файлами, адміністрування доступу до ресурсів – основні переваги ресурсу.

Slack – корпоративний месенджер, який пропонує розширені функції безпеки, такі як наскрізне шифрування даних під час передачі, а також управління доступом до робочих каналів. Платформа відповідає вимогам HIPAA, GDPR та інших стандартів. Відзначається контролем доступу через адміністрування, інтеграцією з системами безпеки, моніторингом активності.

Різноманіття ресурсів для комунікації буде і надалі збільшуватися через вимоги часу та глобалізаційні процеси. Тож вибір месенджерів повинен відбуватися з урахуванням безпекових критеріїв: наскрізне шифрування, двофакторна автентифікація, управління даними. Безсумнівно потрібне навчання учасників освітнього процесу основам кібербезпеки для роботи з платформами (створення надійних паролів, уникнення фішингових атак). І найголовнішим є розробка внутрішніх політик щодо використання месенджерів для навчальних цілей, правил комунікації з урахуванням відповідальності за дані.

Отже, месенджери є зручним та ефективним інструментом для навчальної комунікації, але потребують ретельної уваги та підходу до питань безпеки та вибору правильних платформ, а впровадження правил безпечного використання можуть суттєво знизити ризики для конфіденційності та захисту інформації в освіті.

Список використаних джерел:

1. Лебедєва С. Л. Месенджер Telegram як основний і додатковий канал комунікації в освітньому процесі / С. Л. Лебедєва, М. К. Лебедєв // Інноваційна педагогіка. – 2022. – Вип. 54, Т. 2. – С. 193-196. DOI https://doi.org/10.32782/2663-6085/2022/54.2.38
2. Ризики telegram. Чи безпечно користуватися месенджером та чи пов’язаний він з ФСБ і ГРУ РФ? Розповідають фахівці Cyber Division та Інституту дослідження кібервійни ICWR. Електронний ресурс: https://forbes.ua/innovations/riziki-telegram-chi-bezpechno-koristuvatisya-mesendzherom-ta-chi-povyazaniy-vin-z-fsb-ta-gru-rf-rozpovidayut-fakhivtsi-cyber-division-ta-institutu-doslidzhennya-kiberviyni-icwr-19022024-19311

Роман КЕЛЕМЕН
кандидат педагогічних наук,
адвокат, керівник ТОВ
"Закарпатський центр
правової допомоги"

КІБЕРБЕЗПЕКА , СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХОЛОГІЇ ТА ЇХ ВПЛИВ НА МАЙБУТНІХ ФАХІВЦІВ ПРАВОЗНАВСТВА У ПРОЦЕСІ НАВЧАННЯ В КОЛЕДЖІ

Анотація. *Процес модернізації юридичної освіти в сучасній Україні акцентує увагу на розвитку практичної підготовки майбутніх фахівців правознавства, в якій значну роль відіграє використання новітніх технологій та штучного інтелекту в процесі навчання. Підкреслюється комплексний характер забезпечення інформаційної та кібербезпеки, необхідність постійного вдосконалення методів і способів захисту даних, підвищення рівня знань у цій сфері.*

Ключові слова: *новітні технології, професійна підготовка, фахівці правознавства, кібербезпека .*

Сучасний рівень розвитку інформаційних технологій суттєво впливає на юридичну практику в Україні. Професійна діяльність правознавця надзвичайно складна і багатогранна, оскільки пов'язана з роботою державних установ і посадових осіб різних рівнів ієрархії, спрямована на охорону інтересів держави, законних інтересів і прав громадян. Важко уявити діяльність сучасного юриста без використання комп'ютерної техніки та сучасних мобільних пристроїв: планшетів, смартфонів і ноутбуків. Враховуючи високе призначення юридичної діяльності в суспільстві, вона повинна здійснюватися на засадах єдності загальнолюдського, національного, особистісно-орієнтованого і гуманістичного підходів.

Актуальним є визначення Н. Кожем'яко, яка розглядає професійну юридичну діяльність як діяльність, яку фахівці виконують у межах своєї професії на індивідуальному рівні (як окремі професіонали), а також на рівні країни і суспільства [2, с. 97]. Поняття «фахівець правознавства» використовується як загальне найменування для людей, які займаються юридичною діяльністю і отримали професійну юридичну освіту, яка контролюється державою і зміст якої визначено нормативно-правовими актами. Специфічною для юридичної професії, для професійної юридичної діяльності є реалізація фахівцем правознавства наявних спеціальних знань у процесі вирішення правових завдань. Ця специфіка визначає зміст роботи майбутніх фахівців правознавства, всю їхню професійну кар'єру.

Основою професіоналізму майбутніх фахівців правознавства є хороша освіта. Для того, щоб стати фахівцем в юриспруденції, необхідно глибоко вивчити право і закон. Окрім бази юридичних знань, майбутні фахівці правознавства повинні володіти комплексом певних навичок, тобто вміти застосовувати свої знання на практиці.

У своїй роботі юристи постійно збирають, обробляють, використовують, зберігають та поширюють інформацію, яка потребує комплексного захисту організаційно-технічними та правовими засобами. Без забезпечення безпеки цієї інформації повноцінна робота юриста (адвоката) з інформацією неможлива.

Інформаційна безпека діяльності юриста – стан захищеності інформації, що становить предмет таємниці, забезпечуються її конфіденційність, цілісність і доступність [2, с. 159].

Конфіденційність інформації – це забезпечення доступу до інформації тільки суб'єктів, які мають на це право. Цілісність інформації – стан, за якого її зміна здійснюється тільки навмисно і тільки суб'єктами (авторизованими користувачами), що мають на це право. Доступність інформації – стан, за якого суб'єкти, які мають право доступу до інформації, можуть реалізувати його безперешкодно, тобто безперешкодне забезпечення доступу до інформації авторизованих користувачів [2, с. 53].

Загалом діяльність майбутніх фахівців правознавства спрямована на реалізацію правових норм і забезпечення правопорядку в різних сферах життя суспільства. Для її здійснення фахівці правознавства повинні вміти: тлумачити і застосовувати закони й інші нормативно-

правові акти; забезпечувати дотримання законодавства в діяльності державних органів, фізичних та юридичних осіб; юридично правильно кваліфікувати факти й обставини; розробляти документи правового характеру, здійснювати правову експертизу нормативних актів, давати кваліфіковані юридичні висновки і консультації; приймати правові рішення і здійснювати інші юридичні дії в точній відповідності з законом; систематично підвищувати власну професійну компетентність, вивчати законодавство і практику його застосування, орієнтуватися в спеціальній літературі та ін. Саме ці вміння повинні бути сформовані в студентів в процесі навчання в коледжі та є основою професійної компетентності майбутніх фахівців правознавства.

Юридична діяльність тісно пов'язана з конфіденційними інформаційними даними клієнтів. Саме конфіденційність є головним принципом для надання належної правової допомоги, повному та беззаперечному захисту прав та інтересів клієнтів. Задля повного збереження та недопущення витоку даних, юристи мають бути впевненими в безпеці електронних даних, засобів телекомунікації та документів.

Окрім комп'ютерних пристроїв значний витік інформації може відбуватися через Месенджери - програми швидкого обміну повідомленнями через мережу Internet. До найвідоміших слід віднести WhatsApp, Viber, Telegram, Skype. Саме через ці інтернет-ресурси передається чимало важливої інформації, яка також може містити таємницю. Кожен з них позиціонується як захищений та надійний ресурс із повним захистом персональних даних. Проте, кожен з месенджерів піддавався кібератакам, які призводили до витоку конфіденційних інформацій.

У разі вчинення кібератаки юридична компанія може не лише втратити особисті дані клієнтів та продукти своєї інтелектуальної праці, а й навіть не зуміти вчасно зреагувати на те, що трапилось. І наслідки такої інформаційної недбалості можуть бути глобальні. Порушення конфіденційності даних юридичної фірми та її клієнтів часто призводить до вимагання та шантажу, інсайдерської торгівлі та недобросовісної конкуренції. І це може не лише завдати шкоди репутації — юридична фірма понесе відповідальність, починаючи від фінансової та закінчуючи кримінальною.

Таким чином, одним з важливих підходів формування професійної компетентності майбутніх фахівців правознавства є інтегрований підхід до навчання, тобто системність, комплексність, синтез дисциплін міжнародно-правового і цивільно-правового циклів.

Список використаних джерел:

1. Бовдир О. С. Роль комунікативної культури у професіях юристів. *Педагогічний альманах*. 2010. Вип. 5. С. 104–110.
2. Кожем'яко Н. В. Особливості діяльності фахівця юридичного профілю. Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка. Сер.: Педагогіка. 2011. № 4. С. 95–101.
3. Питання кібербезпеки у світі юриспруденції . Судово-юридична газета. 2019. Вип. 3. С. 19-22.
4. Завадський А.А. Інформаційна та кібербезпека адвокатської діяльності. Порівняльно - аналітичне право. 2021. №5. С.321-323.

Андріана КЕЛЕМЕН
кандидат педагогічних наук,
начальник відділу освіти, культури,
молоді та спорту Хустської РДА-РВА

ШТУЧНИЙ ІНТЕЛЕКТ У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ МАЙБУТНІХ СОЦІАЛЬНИХ ПРАЦІВНИКІВ: ОЧІКУВАНІ ПЕРСПЕКТИВИ ВІД ВПРОВАДЖЕННЯ

Анотація. *Взаємодія новітніх технологій і освітніх систем є нині доволі актуальною проблемою, яка вирішується завдяки різним способам трансляції знань, культурних навичок і патернів поведінки, тому ми погоджуємося з думкою, що сучасну освіту необхідно розглядати з позицій культурно-історичного аспекту.*

Ключові слова: *інформаційно-комунікативні технології, професійна підготовка, соціальні послуги, цифровізація, штучний інтелкт, роботизація.*

В українському суспільстві зросла кількість соціальних проблем, а тому відчувається гостра потреба у вдосконаленні соціальної політики та покращенні якості надання соціальних послуг населенню. Як незаперечний факт розглядаємо необхідність вдосконалення системи соціальної роботи, що реалізовується, головним чином, через надання соціальних послуг, а також на порядок денний поставлено вдосконалення кадрового забезпечення. З огляду на цей факт, відчувається ріст попиту на покращення професійної підготовки майбутніх фахівців, які будуть надавати населенню соціальні послуги.

Соціальна робота є досить складним видом професійної діяльності, а тому майбутній соціальний працівник повинен під час професійної підготовки у закладах вищої освіти оволодіти ґрунтовними знаннями, що виступатимуть головною запорукою високої професійної кваліфікації, та конкурентоспроможності фахівців на ринку праці. Наголосимо на тому, що мета соціальної діяльності конкретизується в змісті та визначає коло основних професійних обов'язків. Головним чином зміст професійної діяльності соціального працівника передбачає різноманітний спектр практичної діяльності, що передбачає цілеспрямований вплив на формування і реалізацію соціальної політики на всіх рівнях (від загальнодержавних до місцевих) через надання допомоги окремій людині чи групі людей, які опинилися у складній життєвій ситуації, шляхом підтримки, консультування, реабілітації, патронажу та інших видів соціальних послуг.

Інформаційно-комунікативні технології, цифровізація і роботизація сформували нову реальність сучасного світу, ведуть до соціокультурних змін соціуму, створюють широкий спектр впливу на життя людини.

Технології штучного інтелекту, впливають на біологічну, соціальну, ментальну й духовну сутність людини, відкривають для людей нові адаптаційні можливості та особистісні перспективи, а з іншого боку, – призводять до формування низки деструктивних соціальних феноменів, ускладнюють процес комунікації та взаємовідносин з іншими суб'єктами, адаптації до мінливого соціотехнологічного середовища, втручання в приватне життя, виключення окремих осіб і груп населення зі звичних для них соціальних зв'язків, практик та способу життя і, як наслідок, породжують соціальне відторгнення.

Нині йдеться про архіважливість глобального розвитку світу, який має дати відповідь на техногенні виклики сьогодення, забезпечивши розвиток науки й технологій штучного інтелекту у гармонії з інтересами кожного індивіда.

Отже, у зв'язку з сучасними вимогами майбутній фахівець, який надаватиме соціальні послуги населенню, має бути людиною високої загальної культури та володіти на належному рівні сучасними інноваційними технологіями.

Список використаних джерел

1. Калаур С.М., Олексюк Н.С. Доцільність використання акмеологічного підходу для самореалізації майбутнього фахівця. *Наукові записки. Серія «Психолого-педагогічні науки» Ніжинський державний університет імені Миколи Гоголя*. Ніжин: НДУ ім. М. Гоголя, 2012. №4. С. 83–86.
2. Пальчевський С. С. Акмеологія – поклик майбутнього. *Акмеологія в Україні: теорія і практика*. К. : КУ ім. Б. Грінченка, 2010. № 1. С. 7–13.
3. Баранов О. А. Визначення терміна «штучний інтелект». Інформація і право. 2023. № 1(44). С.32-49.

Світлана РОМАНЮК
завідувач кафедри педагогіки та методики початкової освіти, професор, доктор педагогічних наук
Чернівецький національний університет імені Юрія Федьковича

КІБЕРБЕЗПЕКА ДЛЯ МОЛОДШИХ ШКОЛЯРІВ: ВИКЛИКИ ТА МОЖЛИВОСТІ

В умовах швидкого розвитку інформаційних технологій, коли Інтернет входить в усі сфери суспільного життя, знання про кебербезпеку стають надзвичайно важливими, особливо для молодших школярів. Адже з раннього віку діти починають користуватися різними гаджетами, соціальними мережами, ігровими платформами, що створюють для них безліч можливостей у навчанні і спілкуванні. Однак дані технології приховують низку загроз, таких як кібербулінг, фішинг, шахрайство, небезпечні сайти, тому вкрай необхідним на сучасному етапі формувати обізнаність молодших школярів у роботі з цифровими технологіями, розвивати навички їх інформаційної грамотності. На важливості окресленої проблеми вказують Закон України «Про освіту» (2017), «Про основні засади забезпечення кібербезпеки України» (2017), Концепція «Нова українська школа» (2016), Концепція впровадження медіаосвіти в Україні (2016), в яких акцентується увага на інформаційно-цифровій компетентності, а, отже, необхідності формування цифрової грамотності та захисту учасників освітнього процесу у контексті використання інформаційних технологій.

Актуальність даного феномена зумовлена ще й тим, що сучасний світ постійно змінюється, більшу частину свого часу діти проводять у ЗМІ, які мають всебічний, потужний і водночас неоднозначний вплив на духовний світ особистості, виховання підростаючого покоління, часто стаючи провідним чинником її соціалізації, соціального навчання. Тому дуже важливо, щоб вони могли адекватно сприймати, аналізувати та оцінювати інформацію, що передається, і розумно використовувати її у своєму житті, були кіберзахищеними. Метою дослідження є обгрунтування важливості знань у сфері кібербезпеки.

Аналіз наукових розвідок засвідчує, що дослідженням даної проблеми займалися Л. Мастерман, Д. Маккуейл, Е. Томан, Капітон А., Капля О., Мальцева І., Ткач Ю. Проте в останніх зосередженно фокус на нормативно-правовому регулюванні та формуванні системи інформаційної безпеки України.

Сучасна шкільна освіта повинна підготувати учнів до життя в освітньому просторі та реаліях неоднозначного соціуму, виробити в них практичні навички, які допоможуть вирішувати нагальні проблеми. Варто пам’ятати, що доступ до інформації сьогодні має кожен, яка здебільшого є маніпулятивною і вимагає критичного мислення та адекватної реакції. Впровадження основ кібербезпеки в освітній процес може допомогти дітям не лише захистити себе, а й стати відповідальними та свідомими користувачами інформаційних технологій. В контексті зазначеного провідна роль належить учителю, який має допомогти школяру зрозуміти усі ризики, повязані із ЗМІ, навчити його виявляти фейкову інформацію, маніпуляції й приймати обгрунтовані рішення. З цією метою варто використовувати з молодшими школярами ігрові технології/ мультфільми, відео, конкурси, які демонструватимуть учням правила безпечної поведінки, етичного спілкування з друзями та незнайомцями у соціальних мережах, навчатимуть основам кібербезпеки. Отже, знання з кібербезпеки, сприятиме вмілому користауванню інтернет-ресурсами, попередженню інформаційних загроз, підготовці здобувачів освіти до викликів цифрового суспільства.

Список використаних джерел:

1. Romaniuk S., Vasylyk M. Funkcje kształtowania kompetencji medialnych uczniów w procesie edukacyjnym współczesnej szkoły. Studia Gdańskie. Wizje i rzeczywistość. 2022. Tom XIX. p. 78

Марія ОЛІЯР
доктор педагогічних наук,
професор кафедри початкової освіти
та освітніх інновацій
Прикарпатський національний
університет імені Василя Стефаника

ПРОБЛЕМА КІБЕРБЕЗПЕКИ В ОСВІТНЬОМУ ПРОСТОРІ ЗВО

Мета статті – висвітлити проблему протидії кіберзагрозам, що супроводять інформаційно-освітній простір ЗВО. Інформаційна безпека стала глобальною проблемою через зростаючу залежність суспільства від глобальної мережі Інтернет, а кіберзагрози – одним із найсерйозніших викликів у різних сферах життя суспільства, в тому числі в освітній. Кіберпростір є сьогодні постійним компонентом системи вищої професійної освіти, а викладачі і студенти знаходяться в групі ризику у зв'язку з високою інформаційною активністю.

Проблему кібербезпеки, кібергігієни та кіберзахисту в закладах освіти розглядали чимало вітчизняних і зарубіжних учених (В. Бурячок, І. Гончарова, А. Горбенко, С. Євсеєв, Г. Король, Ю. Лісовська, С. Остапов, В. Савченко, О. Маклюк, В. Толубко, В. Хорошко, D. Geer, E. Jardine, E. Leverett та ін.). Водночас проблемі формування готовності викладачів та студентів до протидії кібератакам приділяється недостатньо уваги.

Кібератака є ненавмисним або несанкціонованим доступом, використанням, маніпулюванням, перериванням або знищенням інформації, електронних пристроїв, процесів, що використовуються для її обробки. Вона може завдати серйозної шкоди в інформаційному просторі ЗВО. Щоб успішно протистояти кібератакам, викладачі та студенти мають оволодіти відповідним рівнем культури кібербезпеки і бути готовими до боротьби за чистоту інформаційно-комунікаційних технологій. Кібербезпека в освіті полягає в поінформованості користувачів про потенційні ризики при використанні таких засобів комунікації, як Інтернет, соціальні мережі, чати, онлайн-ігри, електронна пошта, миттєві повідомлення та ін.

Викладач ЗВО повинен стати моделлю, що допомагає покращити поведінку студентів при використанні інформаційних технологій, інформувати їх про можливі ризики та збитки і впливати на студентів своїми діями. Тому немає жодних сумнівів, що викладач потребує знань в галузі цифрової безпеки та способів її досягнення. Вважаємо, що для формування готовності викладачів і студентів до протидії кібератакам необхідне додаткове навчання за програмою інформаційної безпеки, яка включає низку актуальних тем (різні види загроз інформаційній безпеці, ідентифікація, автентифікація, авторизація, основи криптографічного захисту інформації; програмно-апаратні засоби забезпечення інформаційної безпеки та методи захисту персональних даних; основи цифрової гігієни (кібергігієни), цифрової етики (культури мережевого етикету, цифрового іміджу); права користувача у цифровому середовищі; безпека персонального комп'ютера та робочого місця; безпека соціальних мереж і месенджерів; безпечна робота в браузері; безпека переговорів, листування; безпека мобільного пристрою; безпека паролів; дії у випадку інциденту тощо).

Ефективним є застосування електронного навчання кібербезпеки, зокрема технологій доповненої та віртуальної реальності. За допомогою цих сучасних технологій можна виявляти чинники небезпеки в реальному інформаційному середовищі (слабкі паролі, оприлюднення інформації, яка може бути використана для здійснення кібератак, фішинг, відсутність антивірусного програмного забезпечення, шкідливі веб-сайти тощо). Ефективним у роботі зі студнетами є електронне навчання кібербезпеки за допомогою технології гейміфікації, що сприяє підвищенню інтересу до навчання, можливості глибоко проникнути в суть проблеми, залученню аудиторії до активної роботи з реагування на кібератаки.

Отже, закладам вищої освіти належить реалізувати комплексний підхід до оволодіння викладачами та студентами основами кібербезпеки, який полягає в розробленні програм, використанні сучасних методів і технологій навчання, що допомагають користувачам отримувати необхідний досвід та підвищувати свою компетенцію.

Mykola PROTSENKO
PhD in Technical Sciences, Associate Professor,
Computer Systems and Networks Department,
National Aviation University

CYBERSECURITY: DEFENDING NETWORKS FROM EVOLVING THREATS

Cybersecurity has become critical in the modern age of rapidly digitizing information and global interconnected networks. Cyberattacks threaten the confidentiality, integrity, and availability of networks, systems, and sensitive data. These threats range from malware to ransomware, each posing a serious risk to information security.

The aim of this study is to provide a comprehensive analysis of cybersecurity, focusing on the tactics, innovations, and challenges involved in safeguarding networks and data from evolving cyber threats. It also examines vulnerabilities, the role of human error, and the importance of proactive measures to protect against future cyber risks.

Among many threats, malware including viruses, worms, Trojan horses, and ransomware remains a major concern. Viruses spread by attaching to legitimate applications, while worms exploit network vulnerabilities to replicate and spread autonomously. Trojans disguise themselves as legitimate software, allowing unauthorized access, and ransomware encrypts user data, demanding ransom for its release. These threats compromise the integrity and confidentiality of sensitive information.

Social engineering, which manipulates human psychology to trick individuals into divulging private information or installing malware, is another significant danger. Phishing, one of the most common social engineering techniques, involves sending fraudulent emails designed to steal sensitive information. Variations like spear-phishing target specific individuals or organizations, while pretexting involves creating fake scenarios to extract information. Identity theft is another tactic cybercriminals use to commit fraud. A robust defense against social engineering requires a mix of technology, education, and policy enforcement.

Cybersecurity is an evolving field due to new vulnerabilities emerging in networks, systems, and data storage. Software vulnerabilities like buffer overflows and injection attacks are common, as is the rise of insecure Internet of Things (IoT) devices. Weak encryption, default passwords, and unsafe configurations in IoT devices provide entry points for attackers. As a result, proactive cybersecurity measures, including strong defenses, regular system updates, and advanced threat detection tools, are necessary to combat future threats.

Technological solutions are integral to cybersecurity. Firewalls, intrusion detection and prevention systems (IDS/IPS), and encryption technologies protect networks and data. Virtual Private Networks (VPNs) secure data transmission over less secure networks, and endpoint protection tools like antivirus software safeguard individual devices. Security Information and Event Management (SIEM) systems further enhance security by monitoring and analyzing log data in real-time to detect and respond to security incidents.

The results of the article indicate that cybersecurity threats are increasingly complex, with significant risks posed by malware and social engineering tactics. It highlights the need for comprehensive defenses, including the adoption of advanced technologies and proactive measures to address vulnerabilities.

Looking ahead, machine learning (ML) and artificial intelligence (AI) are reshaping cybersecurity. AI-driven systems can detect patterns, predict threats, and adapt in real-time, offering faster and more flexible responses to cyberattacks. Future cybersecurity efforts will likely focus on establishing standardized security protocols for IoT devices and integrating blockchain technology to secure data transmission and enhance transparency.

In conclusion, cybersecurity is essential for protecting networks, systems, and data from cyberattacks in an increasingly digital world. The increasing frequency and sophistication of cyber threats necessitate a proactive and flexible approach to security, highlighting the shared responsibility to build a secure digital ecosystem.

Ігор ТОДОРОВ
доктор історичних наук,
професор кафедри міжнародних студій
та суспільних комунікацій
ДВНЗ «Ужгородський національний університет»

КІБЕРБЕЗПЕКА В НОВІТНІХ БЕЗПЕКОВИХ УГОДАХ УКРАЇНИ

З початку 2024 року, Україна уклала 27 угод щодо співпраці у сфері безпеки з різними державами та Європейською унією. Російське вторгнення в Україну зруйнувало стабільність у Європі та значно вплинуло на глобальну безпеку.

Постановка наукової проблеми. Висвітлюються сучасні виклики, пов'язані з кібербезпекою та гібридними загрозами, з якими стикається Україна в умовах російської агресії. Проблема полягає в необхідності формування стратегії кібербезпеки та розробки ефективних механізмів співпраці України з міжнародними партнерами для протидії загрозам у кіберпросторі. Зроблений аналіз ефективності новітніх безпекових угод України, спрямованих на підвищення її стійкості перед гібридними та кіберзагрозами, а також на вдосконалення механізмів координації між Україною та міжнародними партнерами, такими як ЄС і НАТО.

Завдання дослідження: проаналізувати укладені угоди України у сфері кібербезпеки з ЄС, НАТО та іншими міжнародними партнерами з початку 2024 року; вивчити досвід країн НАТО та ЄС щодо підтримки України в кіберпросторі до та після російського вторгнення; оцінити ефективність міжнародного співробітництва через такі механізми, як Талліннський механізм і Європейський центр передового досвіду з протидії гібридним загрозам; дослідити заходи ЄС та НАТО щодо зміцнення стійкості України перед гібридними загрозами та кіберзлочинністю; визначити перспективи подальшої політичної та технічної співпраці України з ЄС і НАТО у сфері кібербезпеки; сформулювати рекомендації щодо підвищення ефективності кібербезпеки України в умовах зовнішніх загроз.

Актуальність дослідження. Актуальність проблеми обумовлена суттєвим зростанням кіберзагроз та гібридних атак, зокрема з боку Російської Федерації, що ставить під загрозу не лише національну безпеку України, але й стабільність у Європейському Союзі та НАТО. На тлі широкомасштабної агресії Росії Україна стає ключовим фронтом кібербезпеки у Європі, що вимагає посилення її спроможностей протидіяти загрозам у кіберпросторі та інтеграції в міжнародні механізми захисту. Укладання нових угод з ЄС, НАТО та іншими міжнародними партнерами, а також розвиток кіберстійкості та захист критичної інфраструктури є ключовими аспектами для забезпечення безпеки та стабільності в регіоні.

Наукова новизна дослідження. Новизна дослідження полягає в системному аналізі новітніх міжнародних безпекових угод України у сфері кібербезпеки, укладених після 2024 року. На відміну від попередніх робіт, які здебільшого фокусувалися на військових або інформаційних аспектах гібридних загроз, це дослідження акцентує увагу на інтеграції кібербезпеки в міжнародні механізми та розвиток стійкості на національному рівні.

Висновки. Досліджено роль України як ключового партнера у міжнародній кібербезпеці та обґрунтовано переваги її досвіду для міжнародних ініціатив.

СУЧАСНІ ПРАКТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ

MODERN PRACTICES IN THE FIELD OF CYBER SECURITY

MODERN GYAKORLATOK A KIBERBIZTONSÁG TERÜLETÉN

Anastasiya YEVTUSHENKO
Second year Bachelor student,
"Cybersecurity and information Protection" major
National Aviation University
***Scientific supervisor* - Larysa TEREMINKO**
Associate professor,
Department of foreign languages for professional communication
National Aviation University

CYBERSECURITY IN THE CONTEXT OF CYBER RESILIENCE: UKRAINIAN EXPERIENCE

With the development of digital technologies, the issue of cybersecurity is becoming increasingly relevant in various sectors of society. In the context of national security, cyber resilience plays a crucial role in the ability of systems and organizations to withstand cyberattacks and quickly recover from them. Ukraine's experience in this area is unique due to the constant cyber threat from a neighboring state, which began long before the full-scale invasion in 2022. However, the stated problem has not been properly analyzed which is the *purpose* of our report.

After the annexation of Crimea in 2014, Ukraine faced numerous cyberattacks targeting critical infrastructure, government institutions, media, and private businesses. One of the most high-profile incidents was the Petya virus attack in 2017, which affected thousands of computers worldwide but was primarily directed at Ukrainian targets. This incident revealed weaknesses in the country's cybersecurity systems and spurred efforts to strengthen protective measures.

A key aspect of Ukraine's development in cyber resilience was the creation of specialized organizations such as the State Service of Special Communications and Information Protection (SSSCIP), responsible for coordinating national cybersecurity efforts. Additionally, the Cyber Emergency Response Team (CERT-UA) plays an essential role by responding to incidents and cooperating with international partners, including NATO and the EU.

Another important element of cyber resilience is raising awareness among citizens and the private sector about cyber threats. Ukraine has actively implemented educational programs, training sessions, and cybersecurity courses for professionals at various levels. These initiatives contribute to the enhancement of cybersecurity culture among the population and businesses, which face daily risks in the digital environment.

Ukraine's experience in building cyber resilience has become an important example for other countries facing cyber threats. The constant exchange of information and cooperation with international partners allows Ukraine not only to protect its critical systems but also to develop new methods of combating cybercrime.

In *conclusion*, it is worth noting that cyber resilience is not just a technical issue but also a social one. It requires a comprehensive approach, encompassing legal, organizational, and educational measures. Having gone through numerous cyber challenges, Ukraine continues to strengthen its position in this field, demonstrating to the world the importance of a systematic approach to cybersecurity in the modern era. Ukraine's experience shows that building cyber resilience requires not only technical solutions but also broad societal support. Modern cybersecurity demands continuous updating of knowledge and skills among both professionals and ordinary citizens. Close cooperation with international organizations such as NATO and the EU helps Ukraine adopt best practices and exchange experiences.

References:

1. State Service of Special Communications and Information Protection of Ukraine (SSSCIP). Official website. https://www.dsszzi.gov.ua
2. CERT-UA Cyber Incident Response Center. Official website. https://cert.gov.ua
3. Ukraine Cybersecurity Report 2023 published by the National Cybersecurity Coordination Center (NCCC)

Валентина БІЛАН
аспірантка Інституту держави і
права імені В.М. Корецького НАН України
за спеціальність «Міжнародне право»

КІБЕРЗАГРОЗИ ТА ЇХ ПРАВОВЕ РЕГУЛЮВАННЯ В УМОВАХ МІЖНАРОДНИХ ЗБРОЙНИХ КОНФЛІКТІВ

Кіберзагрози у сучасних міжнародних збройних конфліктах становлять одну з найбільших загроз для національної безпеки держав та стабільності міжнародної системи. Вони охоплюють широкий спектр шкідливих дій, спрямованих на ураження важливих інфраструктур, порушення інформаційної цілісності та поширення дезінформації, які мають як економічні, так і політичні наслідки для міжнародного співтовариства [1]. В умовах активізації гібридних конфліктів відсутність чітких механізмів регулювання кіберпростору лише підсилює вразливість держав, що вказує на нагальну потребу в міжнародно-правових стандартах і узгоджених заходах з кібербезпеки [2].

Сутність кіберзагроз у збройних конфліктах:

Сучасні кіберзагрози у конфліктах виходять за рамки звичайних кібератак, перетворюючись на комплексну систему заходів, спрямованих на послаблення супротивника у військовій, економічній та соціальній сферах. Види кіберзагроз включають:

1. Атаки на критичну інфраструктуру — порушення енергетичних, транспортних і фінансових систем може мати катастрофічні наслідки для економіки та національної безпеки [3].

2. Кіберрозвідка та шпигунство — застосування шкідливого програмного забезпечення для збору чутливої інформації та шпигунства стає поширеним засобом отримання даних [4].

3. Дезінформація та психологічна війна— маніпулювання громадською думкою через поширення фейкових новин та пропаганди задля послаблення морального духу населення, підриву довіри до державних інститутів та провокування соціальної нестабільності.

Такі дії є складовими гібридної війни, де кіберпростір відіграє важливу роль у комплексному застосуванні засобів впливу на державу-супротивника. Використання кіберзагроз у збройних конфліктах відкриває можливості для нанесення значної шкоди без прямого використання традиційних збройних сил.

Правове регулювання кіберзагроз на міжнародному рівні:Ефективне протидія кіберзагрозам під час міжнародних конфліктів вимагає чіткої координації зусиль між державами та розробки правових механізмів для регулювання кіберпростору. Існуючі міжнародні документи націлені на зниження рівня кіберзлочинності, проте їх правове регулювання у період збройних конфліктів потребує удосконалення.

1. Будапештська конвенція про кіберзлочинність— цей документ визначає кіберзлочини як глобальну загрозу, що потребує міжнародного співробітництва для їх запобігання і розслідування, однак у межах цієї конвенції не передбачено правових заходів щодо кіберзагроз у збройних конфліктах [5].

2. Резолюції ООН — Генеральна Асамблея ООН неодноразово вказувала на важливість кібербезпеки у своїх резолюціях, закликаючи держави розробити заходи щодо захисту критичної інфраструктури і гарантувати дотримання норм міжнародного права у кіберпросторі [6].

3. Група урядових експертів ООН з розвитку норм поведінки у кіберпросторі — ці експерти активно працюють над створенням норм поведінки в кіберпросторі, що сприятимуть міжнародному регулюванню кіберзагроз та можуть використовуватись як основа для нових стандартів у випадках збройних конфліктів [7].

4. Європейські директиви з кібербезпеки (NIS2) — ЄС ухвалив низку документів, спрямованих на зміцнення захисту критичної інфраструктури від кіберзагроз, що є важливим кроком для підвищення рівня кібербезпеки у державах-членах [8].

Проблеми та перспективи:Ключовими проблемами у правовому врегулюванні кіберзагроз залишаються відсутність єдиного розуміння кібернападів та кібероборони, а також нестача узгоджених механізмів реагування на них у межах міжнародного права. Важливою перешкодою є різниця у поглядах держав на суверенітет у кіберпросторі та труднощі у забезпеченні відповідальності за дії в кіберсфері під час конфліктів. Більшість міжнародних акторів визнають необхідність узгоджених підходів, однак повне врегулювання кіберзагроз потребує багатосторонніх переговорів та взаємних компромісів.

Висновки: З огляду на розвиток кіберзагроз під час міжнародних збройних конфліктів, міжнародне право стоїть перед новими викликами у сфері безпеки, що вимагають адаптації існуючих норм або створення нових стандартів. ООН, ЄС та інші організації здійснюють вагомі кроки до забезпечення кібербезпеки, однак для досягнення ефективного регулювання необхідно узгодження зусиль на міжнародному рівні, створення нових норм та зміцнення співробітництва між національними й міжнародними інституціями. Ці заходи мають сприяти захисту критичної інформаційної інфраструктури та прав людини у кіберпросторі під час збройних конфліктів.

Список використаних джерел:

1. Jones, C. “Cyber Warfare in International Conflicts.” Journal of Security Studies, 2020.
2. European Union Agency for Cybersecurity (ENISA). “Threat Landscape Report 2021”.
4. Smith, L. “The Role of Malware in Cyber Conflicts”. Journal of Computer Security, 2022.
5. United Nations. “Resolution 70/237 on Developments in the Field of Information and Telecommunications in the Context of International Security”.
6. Council of Europe. "Budapest Convention on Cybercrime," 2001.
7. United Nations Group of Governmental Experts. "Report on Norms in Cyberspace," 2021.

Марія МЕНДЖУЛ
докторка юридичних наук, професорка,
професорка кафедри цивільного права та процесу
Оксана МУЛЕСА
докторка технічних наук, професорка,
професорка кафедри програмного забезпечення систем
ДВНЗ «Ужгородський національний університет»

ПРОБЛЕМИ ГАРАНТУВАННЯ КІБЕРБЕЗПЕКИ У ПРОЦЕСІ ТРАНСКОРДОННОГО СПІВРОБІТНИЦТВА ПІД ЧАС ВОЄННОГО СТАНУ

Повномасштабна війна у нашій державі показала яким чином інформація у сучасному світі може бути використана як інструменти боротьби і є невід'ємною складовою так званих «гібридних воєн». За таких умов вкрай важливим є дослідження як поняття кібербезпеки, так і тих інструментів захисного механізму, які б з одного боку сприяли захисту персональних даних, а з іншого боку були основою для регіональної, національної та міжнародної безпеки. У рамках цих тез висвітлено окремі проблеми гарантування кібербезпеки у процесах транскордонного співробітництва із врахуванням тих ризиків, які зумовлені гібридною війною.

Шинкаренко І. Р. та Шинкаренко І. І. вважають, що формування інформаційної безпеки під час війни є «такою системою політичних, правових та технічних дій уповноважених органів, які мають на меті захистити громадян, суспільство і державу», а розвиток нормативно-правових засад по управлінню національною безпекою має відбуватися через розробку відповідних нормативно-правових актів, концепцій, стратегій та програм тощо [1, С. 140]. Водночас вказане визначення не передбачило особливостей дії захисного механізму по гарантуванню інформаційної безпеки в умовах воєнного стану. Крім того, автори не розглядають поняття кібербезпека та як воно співвідноситься із терміном інформаційної безпеки.

На думку Тайєр Амро, в умовах війни важливими є насамперед методи забезпечення інформаційної безпеки, зокрема: інструменти гарантування кібербезпеки (охорона комп'ютерних систем від несанкціонованих доступів, атаки вірусів тощо); забезпечення фізичної безпеки інформації; гарантування в управлінському механізмі дієвого громадського контролю; гарантування безпеки інформаційного простору, управління тією інформацією, яка є конфіденційною, належна взаємодія між різними структурами держави, військовими підрозділами і громадськістю, розвиток системи публічної інформації, масової комунікації; належний моніторинг та аналіз інформації [2, С. 86-87]. Всі вказані складові забезпечення інформаційної безпеки під час війни важливі, водночас не вистачає використання інструментів штучного інтелекту для боротьби із дезінформацією, створеною за допомогою ШІ.

Науковці при детальному дослідженні інформаційної безпеки виділяють такі групи інформаційно-технологічних загроз: 1) інформаційна зброя, що може як впливати на психіку людини, так і на державну інформаційно-технологічну інфраструктуру; 2) використання сучасних інформаційних технологій із метою завдання шкоди (фінансові махінації, незаконне копіювання технологій тощо); 3) через комп'ютерні системи впровадження тотального контролю як за життям людини, так і за роботою публічних структур, державних установ; 4) використання інформаційних технологій у політичній боротьбі [3]. Вказані загрози варто на нашу думку доповнити п'ятим – використання штучного інтелекту для продукування дезінформації та її максимального поширення через мережу Інтернет.

На нашу думку, поняття «інформаційної безпеки» ширше аніж поняття «кібербезпека». Визначення поняття «кібербезпека» закріплено у ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» під якою прийнято розуміти: «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація

реальних і потенційних загроз національній безпеці України у кіберпросторі». Відповідно кібербезпека обмежується на відміну від інформаційної безпеки виключно мережею Інтернет чи іншими глобальними мережами передачі даних.

В контексті гарантування кібербезпеки у транскордонному співробітництві слід згадати про Стратегію кібербезпеки України, яка взагалі не згадує жодного разу громади та органи місцевого самоврядування [4]. Вочевидь вказаний акт потребує перегляду і оновлення, адже питання кібербезпеки є ключовим для національної безпеки і його гарантування не можливе без впровадження заходів протидії на місцях.

В умовах реалізації проєктів по транскордонному співробітництву вкрай важливим є гарантування кібербезпеки, особливо коли учасниками таких проєктів є територіальні громади. Закарпатська, Львівська, Чернівецька, Івано-Франківська області доволі активно долучаються через різних суб'єктів до реалізації проєктів по транскордонному співробітництву. Ми проаналізували проєкти у рамках двох програм «Hungary-Slovakia-Romania-Ukraine ENPI Cross-border Cooperation Programme 2007-2013» та «Hungary-Slovakia-Romania-Ukraine ENI CBC Programme 2014-2020». Проведене дослідження показало, що у рамках програми «Hungary-Slovakia-Romania-Ukraine ENPI Cross-border Cooperation Programme 2007-2013» було підтримано 31 проект за участі різних громад із Закарпатської області. Програма «Hungary-Slovakia-Romania-Ukraine ENI CBC Programme 2014-2020» передбачала три кола конкурсів, проекти в останньому колі завершували реалізацію проектів не пізніше осені 2023 року. Проведений аналіз показав, що у першому колі програми «Hungary-Slovakia-Romania-Ukraine ENI CBC Programme 2014-2020» було відібрано тільки чотири проекти, у другому колі – 46 проєктів, у третьому конкурсі програми – 30 підтриманих проєктів [5].При змістовному аналізі проєктів транскордонного співробітництва було виявлено, що на разі питанням гарантування кбербезпеки на рівні прикордонних територій не займалися жоден із залучених проєктів. Водночас процеси цифровізації, розвиток інформаційних технологій створюють умови для належної організаційної та технічної підтримки реалізації проєктів транскордонного співробітництва.

Таким чином, кібербезпека у транскордонному співробітництві є важливим елементом гарантування як національної, так і міжнародної безпеки. Проблеми із дезінформацією, використанням неправдивих повідомлень, невірний чи викривлений переклад новин не тільки є порушенням права на інформацію, а можуть стати підґрунтям для ворожнечі та зростання напруги на прикордонних територіях. З огляду на це у питаннях транскордонної співпраці важливе значення відіграє саме гарантування кібербезпеки.

Список використаних джерел:

1. Шинкаренко І. Р., Шинкаренко І. І. Інформаційна безпека України в умовах воєнного стану / Сучасні проблеми правового, економічного та соціального розвитку держави: тези доп. XI Міжнар. наук.-практ. конф.(м. Вінниця, 9 груд. 2022 р.). Вінниця, 2022. С. 139-140.
2. Амро Т. Взаємозв'язок систем забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану: методи та можливості. Публічне урядування. 2022. № 5 (33). С. 83-88.
3. Свердлов Д.В., Борисенко Т.В. Забезпечення інформаційної безпеки держави в умовах дії правового режиму воєнного стану / Актуальні проблеми превентивної діяльності Національної поліції в умовах воєнного стану : матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 27 квіт. 2022 р.). Дніпро: ДДУВС, 2022. С. 78-80.
4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12
5. The 3rd Call for Proposals of the Hungary-Slovakia-Romania-Ukraine ENI CBC Programme 2014-2020. URL: https://huskroua-cbc.eu/calls/3rd-call-for-proposals

Валерія ЧОБАЛЬ
студентка 3 курсу спеціальності
035.10 «Філологія. Прикладна лінгвістика»
***Науковий керівник* – Ігор ЛЯХ**
доктор технічних наук, доцент,
професор кафедри інформатики
та фізико-математичних дисциплін
Ужгородський національний університет

РОЛЬ ЛІНГВІСТИЧНОЇ ЕКСПЕРТИЗИ ТА ШТУЧНОГО ІНТЕЛЕКТУ В ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасному світі, де кіберзагрози стають все більш витонченими, інформаційна безпека виходить на новий рівень важливості. Захист інформаційних систем вже не обмежується лише технічними аспектами, такими як захист мереж і шифрування даних. Текстова інформація, що поширюється через повідомлення, соціальні мережі, електронну пошту та інші канали, стає основним об'єктом кіберзагроз, як-от фішингові атаки, дезінформація, мова ненависті. У цьому контексті лінгвістичний аналіз та штучний інтелект (ШІ) відіграють важливу роль у забезпеченні інформаційної безпеки.

Кібербезпека (або інформаційна безпека) — це сукупність заходів, процесів і технологій, спрямованих на захист інформаційних систем, мереж, програм і даних від несанкціонованого доступу, атак, пошкоджень або крадіжок. Вона охоплює всі аспекти безпеки в інформаційному середовищі, включаючи захист від кіберзагроз, таких як: хакерські атаки, віруси, шкідливі програми, фішинг та інші види кіберзлочинів [1].

Кіберзлочинність має безпрецедентний вплив на бізнес у різних секторах, її збитки у 2023 році сягнули близько 8 трильйонів доларів США.

У сучасну цифрову епоху надійна кібербезпека стає критично важливою, оскільки керівники компаній прагнуть випереджати постійно змінювані загрози. Подібно до інших галузей, роль штучного інтелекту (ШІ) в сфері кібербезпеки ставатиме дедалі вагомішою.

Прогнозується, що до 2027 року ринок штучного інтелекту в кібербезпеці досягне 46,3 мільярда доларів США [2].

Лінгвістичний аналіз в інформаційній безпеці полягає у вивченні структури мови та її використання для виявлення потенційних загроз. За допомогою лінгвістичного аналізу можна виявити потенційні фішингові атаки на основі характерних мовних ознак, таких як неграмотність, використання термінології або інтонація, що не відповідає офіційному стилю. Також цей підхід дозволяє ідентифікувати прояви кібербулінгу, мови ненависті та інших шкідливих дій у текстових повідомленнях [3].

Проблемами лінгвістичної експертизи займалися такі лінгвісти як Дж. Олссон, Р. Шай , Дж. Макменамін , Дж. Гіббонс та інші.

ШІ має значний потенціал у сфері кібербезпеки, особливо в аналізі великих обсягів текстових даних. Використання алгоритмів машинного навчання та нейронних мереж дозволяє автоматизувати процеси аналізу, підвищуючи їх ефективність і точність. Ключові напрямки, де ШІ грає важливу роль:

- обробка природної мови (NLP - Natural language processing). Технології ШІ дозволяють автоматично аналізувати текст, виявляючи підозрілі або небезпечні патерни. Це дає змогу швидше реагувати на загрози, як-от фішингові атаки, дезінформаційні кампанії або зловмисний контент;

- аналіз стилю та авторства. Алгоритми машинного навчання здатні порівнювати тексти за низкою параметрів (лексика, синтаксис, частота використання певних слів, ритм) і на основі цього робити висновки про стиль автора або підтверджувати авторство. Такі системи корисні в судових розслідуваннях, коли потрібно встановити, чи належить конкретний текст певній особі.

- порівняння текстових матеріалів. Штучний інтелект значно пришвидшує процес порівняння текстів для виявлення подібностей або відмінностей. Це може бути використано для аналізу плагіату, виявлення змін у документах або текстах різних версій. Системи можуть швидко знаходити співпадіння на різних рівнях: від лексичного до синтаксичного.

- аналіз змісту та контексту. ШІ допомагає виявляти глибинні змісти текстів, аналізуючи контекст і структуру повідомлень. Лінгвістичні алгоритми здатні ідентифікувати приховані сенси, натяки або навіть сарказм у тексті. Це значно пришвидшує і полегшує роботу експертам, які досліджують юридичні документи або проводять судову експертизу для виявлення маніпуляцій чи прихованих погроз.

- розпізнавання аномалій: за допомогою алгоритмів ШІ можна відстежувати незвичайні патерни в текстовій комунікації, які можуть свідчити про шахрайські дії або кібератаки.

Поєднання лінгвістичного аналізу та технологій штучного інтелекту створює потужний інструмент для кібербезпеки. Лінгвістичний аналіз дозволяє глибше зрозуміти специфіку мови загроз, тоді як ШІ автоматизує та прискорює цей процес, забезпечуючи виявлення загроз у режимі реального часу [4].

Наприклад, у випадку дезінформаційних кампаній, лінгвістичний аналіз може ідентифікувати специфічні риторичні стратегії, що використовуються для маніпуляцій громадською думкою. Штучний інтелект, у свою чергу, здатен аналізувати тисячі повідомлень одночасно, виділяючи ті, які містять ці патерни. Це дає можливість оперативно реагувати на дезінформацію та обмежувати її вплив.

Незважаючи на значний потенціал, використання штучного інтелекту та лінгвістики в кібербезпеці стикається з низкою викликів. Наприклад, кіберзлочинці постійно вдосконалюють свої методи, використовуючи все більш складні мовні структури та уникаючи стандартних патернів, що ускладнює роботу алгоритмів ШІ. Крім того, аналіз контексту повідомлень залишається складним завданням для автоматизованих систем, оскільки для точного тлумачення інформації іноді потрібен людський фактор.

Однак, з розвитком технологій та поглибленням знань у галузі лінгвістичного аналізу, ці труднощі поступово вирішуються. У майбутньому можна очікувати інтеграцію ще більш складних моделей штучного інтелекту, здатних адаптуватися до нових форм загроз та забезпечувати ефективний захист від кіберзлочинів.

Отже, лінгвістичний аналіз та штучний інтелект є невід'ємною частиною сучасної системи кібербезпеки. Вони допомагають швидко ідентифікувати текстові загрози, аналізувати величезні обсяги даних та забезпечувати гнучкий і ефективний захист від кіберзагроз. Завдяки їхній синергії інформаційна безпека стає більш стійкою до нових викликів, які з'являються в епоху цифрових технологій.

Список використаних джерел:

1. Комп’ютерна безпека – [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0.
2. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам – [Електронний ресурс] – Режим доступу: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/.
3. Лінгвістична експертиза : підручник / Л. І. Шевченко, Д. Ю. Сизонов ; за ред. Л. І. Шевченко. Київ : ВПЦ "Київський університет", 2021. 244 с.
4. Strategic Communications Basic Concepts: NATO-Based Standards (English-Ukrainian and Ukrainian-English Dictionary) [Bazovi poniattia stratehichnykh komunikatsii: standarty na osnovi dokumentiv NATO (anhliisko-ukrainskyi ta ukrainsko-anhliiskyi slovnyk] (2019). Kyiv : Natsionalna akademiia SBU, 336

Марта ШЕЛЕМБА
кандидат політичних наук,
доцент кафедри міжнародних
студій та суспільних комунікацій,
ДВНЗ «Ужгородський національний університет»

ІНТЕГРАЦІЯ СУЧАСНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ У НАВЧАЛЬНИЙ ПРОЦЕС: ДОСВІД ДВНЗ «УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»

Концепція цифрової трансформації враховується в удосконаленні підготовки фахівців з міжнародних відносин в УжНУ через ряд ініціатив та практичних заходів, спрямованих на інтеграцію сучасних цифрових технологій у навчальний процес. Ось кілька способів, як це реалізується:

1.Інтеграція технологій в навчальні програми:

Інтеграція технологій в навчальні програми в Ужгородському національному університеті (УжНУ) відображає сучасні тенденції у вищій освіті, спрямовані на підготовку студентів до ефективної роботи в умовах цифрової трансформації. УжНУ впроваджує різноманітні технології в навчальний процес з метою покращення якості освіти та розвитку цифрових навичок студентів. Ось кілька прикладів інтеграції технологій в навчальні програми УжНУ:

- Електронні навчальні платформи: УжНУ використовує сучасні електронні навчальні платформи, такі як Moodle або Google Classroom, для організації дистанційного навчання та спільної роботи студентів із викладачами. Це дозволяє забезпечити доступ до навчальних матеріалів, завдань та інтерактивних занять у будь-який час і з будь-якого місця.
- Використання відео та вебінарів: УжНУ активно використовує відео матеріали та вебінари для навчання студентів. Відеоуроки дозволяють ефективно демонструвати складні концепції, а також надають можливість вивчати матеріал у форматі, доступному для самостійного опрацювання.
- Цифрові інструменти для колаборації: УжНУ сприяє використанню цифрових інструментів для спільної роботи студентів у групах. Застосунки для спільної роботи над проектами (наприклад, Google Docs, Slack) дозволяють студентам ефективно обмінюватися ідеями та співпрацювати над завданнями в онлайн-режимі.
- Онлайн-тестування та оцінювання: УжНУ використовує спеціальні платформи для проведення онлайн-тестування та оцінювання знань студентів. Це дозволяє здійснювати ефективний моніторинг успішності та оцінювати рівень засвоєння навчального матеріалу.

2.Електронні бібліотеки та бази даних: УжНУ надає студентам доступ до електронних бібліотек та баз даних з міжнародних відносин, що дозволяє здійснювати пошук та аналіз актуальної інформації онлайн. Це сприяє розвитку навичок роботи з інформаційними ресурсами та дослідницької діяльності.

3.Використання відеоконференцій та онлайн-комунікацій: Факультети та кафедри проводять відеоконференції та онлайн-семінари з використанням платформ, таких як Zoom або Microsoft Teams. Це дозволяє студентам брати участь у дистанційних заняттях та взаємодіяти з викладачами та колегами, незалежно від місця перебування.

4.Проекти та курси з цифрової грамотності: впровадження спеціальних курсів з цифрової грамотності для студентів з міжнародних відносин. Ці курси допомагають розвивати навички роботи зі збором, аналізом та використанням даних, оволодівати основами цифрового маркетингу та комунікацій у міжнародному контексті.

5.Участь у міжнародних проектах та програмах**:** УжНУ може сприяти участі студентів у міжнародних проектах та програмах з використанням цифрових технологій. Це може

включати співпрацю з міжнародними організаціями або університетами за допомогою віртуальних засобів комунікації.

6.Стимулювання інновацій та досліджень в галузі цифрової трансформації: УжНУ може створювати сприятливі умови для розвитку інноваційних проектів та досліджень в галузі цифрової трансформації, що сприяє активному впровадженню сучасних цифрових рішень у навчальну діяльність.

Ці ініціативи спрямовані на підвищення якості освіти та підготовку фахівців з міжнародних відносин до успішної роботи у сучасному цифровому світі. Вони дозволяють студентам здобувати не лише традиційні знання, але й цифрові компетенції, які стають все більш важливими у професійній діяльності у глобальному масштабі.

Список використаних джерел

1. Концепція розвитку інформаційного суспільства в Україні: URL: https://www.kmu.gov.ua/npas/246420577
2. Концепція розвитку дистанційного та електронного навчання в Україні. URL: https://bzl.cprpp.org.ua/koncepciya-rozvitku-distancijnoi-osviti-v-ukraini-10-38-36-24-01-2022
3. Концепція інноваційного розвитку ДВНЗ «Ужгородський національний університет» на 2015-2025 рр. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/50325

Kira SHVED
Second year Bachelor students,
"Cybersecurity and information Protection" major
National Aviation University
***Scientific supervisor* – Natalia BILOUS**
Associate professor, Department of foreign languages for professional communication
National Aviation University

MODELS AND TOOLS FOR EFFECTIVE RESPONSE TO CYBER INCIDENTS IN THE CONTEXT OF CERT: CHALLENGES AND PROSPECTS

CERT-UA is a governmental team that responds to computer emergencies in Ukraine, operating under the leadership of the State Service for Special Communications and Information Protection of Ukraine.

CERT uses several models and methodologies to respond quickly to cyber incidents:

NIST Incident Response Framework – a model consisting of 4 main stages (preparation, detection and analysis, containment and elimination, post – incident activity). This model aimed at countering cyber threats by developing policies, procedures and response plans.

Kill Chain Model – it is used to analyze the sequence of attack actions in order to detect and stop them at different stages, in particular: intelligence, armament, delivery, operation, installation, command and control.

MITRE ATT&CK FRAMEWORK – contains a detailed catalog of TTPs practices used by hackers. CERT uses this framework to analyze the behavioral characteristics of cyberattacks and facilities their detection.

SIEM – systems – the systems combine data from different networks and systems to quickly identify different threats and automate the incident detection process.

SOAR – automated response and incident coordination platforms. The COAR integrates various security systems and enables rapid detection and remediation of threats through automated processes.

CIS (Critical Security Controls) – a set of basis cybersecurity measures that help protect against the most common threats. CERT uses these controls to ensure effective protection.

The main advantages of CERT:

- Collect and analyze data on cyber incidents and maintain a state register of such cases.
- Provide practical assistance to owners of cyber defense facilities in preventing, detecting and eliminating the consequences of cyber incidents.
- To organize and conduct practical seminars on cyber defense for participants of the national cybersecurity system and owners of cyber defense facilities.
- Prepare and publish on its official website recommendations for countering modern cyber threats and cyberattacks.

Challenges that CERT may encounter:

- Lack of resources
- Outdated technologies
- Increase of amount and complexity of attacks
- Insufficient of information and cooperation
- Human factor

Natalia TODOROVA
PhD, Associate Professor
Department of multicultural education and translation
Uzhhorod National University

INTEGRATING CYBERSECURITY AND ARTIFICIAL INTELLIGENCE INTO TERTIARY EDUCATION PEDAGOGY

In today's interconnected digital world, cybersecurity threats continue to evolve, posing serious risks to personal privacy, organizational integrity, and national security. AI technologies are being employed across industries, not only to drive innovation but also to combat these cybersecurity challenges. However, there is a significant gap in how tertiary education prepares students to tackle these issues. Most academic programs still treat cybersecurity and AI as niche technical subjects rather than as integral components of a broader educational framework. This separation restricts students' ability to develop their digital literacy, critical thinking, and ethical reasoning necessary to face real-world challenges.

For universities and colleges, it becomes crucial to incorporate these fields into the core of tertiary education pedagogy. However, the challenge remains: How can higher education institutions effectively integrate cybersecurity and AI into their teaching practices and curricula to ensure students are adequately prepared?

The purpose of this research is to investigate how tertiary education can more effectively incorporate cybersecurity and AI into its pedagogical practices. This includes exploring the development of a curriculum framework that not only teaches students the technical skills required in these fields but also fosters a deeper understanding of the ethical, societal, and professional implications of AI and cybersecurity. The goal is to create a holistic educational approach that prepares students to be competent, responsible digital citizens and professionals.

The research aims to identify strategies that educators can employ to better integrate practical applications of AI and cybersecurity challenges into the learning environment. Additionally, the research will examine how these teaching practices can encourage critical thinking, problem-solving, and ethical decision-making in students — skills that are vital in an increasingly digital and AI-driven world.

With these objectives in mind, several key tasks are addressed:

- to study *existing curricula* to identify gaps where AI and cybersecurity education can be integrated and explore interdisciplinary approaches that combine technical skills with ethical, legal, and societal perspectives;
- to develop a *pedagogical framework* that equips educators with the tools and resources needed to teach these subjects effectively, combining both theory and practical applications, such as case studies, simulations, and real-world problem-solving scenarios.
- to analyze *the role of AI in cybersecurity*, specifically how AI technologies can be used to detect and counter cyber threats, exploring the limitations and ethical concerns associated with AI in this domain;
- to investigate how to foster *ethical reasoning* and *critical thinking* skills in students through the integration of AI and cybersecurity in the curriculum, balancing technological innovation with the protection of privacy and human rights;
- to identify effective teaching strategies that engage students in hands-on learning experiences, bridging the gap between academic theory and real-world application.

Thus, the integration of AI and cybersecurity into tertiary education is not just a technical challenge but a pedagogical imperative. As the digital landscape continues to evolve, educational institutions must adapt to ensure their graduates are not only proficient in these fields but also capable of making informed, ethical decisions. By developing a robust pedagogical framework that incorporates cybersecurity and AI into the curriculum, universities and colleges can equip students with the knowledge and skills needed to navigate the complexities of the modern digital world.

Ольга ГРИЩУК
старший науковий співробітник
Національний університет оборони України
Олександр КОРЧЕНКО
перший проректор, Державний університет інформаційно-комунікаційних технологій

ВЕРИФІКАЦІЯ МАТЕМАТИЧНОЇ МОДЕЛІ СИМТЕРИЧНОЇ КРИПТОГРАФІЧНОЇ СИСТЕМИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ДИФЕРЕНЦІАЛЬНИХ ПЕРЕТВОРЕНЬ

Постановка проблеми в загальному вигляді. У сучасних умовах питання кібербезпеки, безпеки інформації та інформаційної безпеки перебувають у фокусі національної безпеки України. Від їх якісного вирішення суттєво залежить рівень кібероборони держави. Разом з тим в Україні щодня фіксуються та відбиваються сотні кібератак на критичні застосунки, особливо ті з них, які використовуються в державних органах управління. На сьогодні непоодинокими є випадки здійснення спроб несанкціонованого доступу до мовної інформації, яка циркулює в системах спеціального зв'язку та в мережах VoIP-телефонії. Тому питання забезпечення безпеки мовної інформації в рамках проблеми забезпечення кібероборони держави на сьогодні й надалі залишається актуальним та потребує свого вирішення.

Аналіз останніх досліджень і результатів. У системах та мережах в яких циркулює мовна інформація на сьогодні найчастіше застосовують методи криптографічного захисту. Відомі методи криптографічного захисту мовної інформації реалізовано у симетричних або асиметричних криптографічних системах захисту відповідно. Зважаючи на більшу швидкодію симетричних криптографічних систем, порівняно з асиметричними системами захисту мовної інформації, їх застосування на практиці залишається в пріоритеті. Але внаслідок швидкого розвитку тактик криптоаналізу, вони також підвладні зламу. Саме тому дуже важливо верифікувати новітні математичні моделі симетричних криптографічних систем захисту мовної інформації, зокрема й на основі диференціальних перетворень.

Викладення основного матеріалу дослідження. У відомих публікаціях було запропоновано математичну модель симетричної криптографічної системи захисту мовної інформації. Верифікуючи згадану модель, дослідимо її основні особливості. Перша особливість – в моделі в якості криптографічного алгоритму використовується інтегральне рівняння Фредгольма першого роду. Друга особливість – ключем шифрування виступає ядро інтегрального рівняння. Третьою особливістю є те, що шифруванню в такій криптосистемі підлягає мовна інформація у вигляді аналогового сигналу ще до її оцифрування аналогово-цифровими перетворювачами. Четверта особливість – це використання в процесі шифрування та розшифрування мовної інформації диференціальних перетворень академіка НАН України Г. Пухова. П’ята особливість досліджуваної моделі – це використання методу регуляризації А. Тихонова для реалізації процедури розшифрування шифротексту з вихідної мовної інформації у вигляді диференціального спектру. Зважаючи на такі особливості математична модель симетричної картографічної системи захисту мовної інформації на основі диференціальних перетворень володіє доведеними теоретичною та практичною стійкістю.

Висновки та перспективи подальших досліджень. Таким чином, зважаючи на зазначене можна стверджувати: по-перше, теоретична та практична нерозв’язність зворотної некоректної задачі Фредгольма першого роду гарантує теоретичну та практичну криптостійкість досліджуваної системи. Цей висновок випливає з гіпотези Н. Фергюсона про залежність безпеки шифру від складності вирішення певного типу рівнянь; по-друге, досліджувана модель побудована за класичною моделлю симетричної криптосистеми. Відмінність між відомими моделями та досліджуваною моделлю проявляється лише на рівні застосовуваних процедур шифрування та дешифрування. Отже, додержання класичного принципу побудови криптосистеми дозволяє стверджувати, що розроблені та покладені в основу узагальненої моделі концепти є повністю доведеними, а сама модель є адекватною, тобто верифікованою.

Юрій МАТЕЛЕШКО
кандидат історичних наук, доцент
доцент кафедри міжнародних студій
та суспільних комунікацій
ДВНЗ «Ужгородський національний університет»

ЦИФРОВА ДИПЛОМАТІЯ: ПЕРЕВАГИ ТА РИЗИКИ

Цифрову (електронну) дипломатію (далі – ЦД) прийнято вважати однією з форм публічної (громадської) дипломатії, яка використовує Інтернет, нові інформаційно-комунікаційні технології та соціальні мережі як засоби здійснення дипломатичних відносин. Від класичної публічної дипломатії ЦД відрізняється тим, що вона забезпечує ширший та прозоріший доступ до інформації та надає можливості для більшої взаємодії між окремими особами та організаціями. Крім державних акторів, в електронній дипломатії беруть участь також різні неурядові суб'єкти (політичні партії, громадські організації, інфлюенсери тощо).

Перевагами ЦД є:

1. Вона робить діяльність держави в міжнародних відносинах більш ефективною. Так, обмін інформацією в режимі реального часу заначно прискорює зовнішньополітичну діяльність. Пряма взаємодія з громадськістю та залучення недержавних акторів допомагають підтримувати легітимність і розвивати чи зміцнювати відносини в мінливому світі.

2. За допомогою використання вебсайтів, блогів, соціальних мереж тощо ЦД дає можливість залучати широку аудиторію політиків, дипломатів та громадян з усіх куточків земної кулі. Зокрема, вона, на відміну від традиційної дипломатії, може впливати на людей, які ніколи не відвідували ту чи іншу країну або її представництва.

3. ЦД дає змогу здійснювати швидкі та ефективні комунікації. Цифрові технології значно пришвидшують збір та обробку інформації, а також зв’язок, необхідний в умовах екстрених ситуацій.

4. Порівняно із традиційними видами дипломатії, ЦД, що базується на використанні передових технологій, потребує менших фінансових витрат, а іноді її застосування взагалі не вимагає якихось грошових ресурсів (наприклад, дописи у соцмережах).

5. ЦД допомагає малим державам, які обмежені в людських та фінансово-економічних ресурсах, більш ефективно реалізовувати їхню зовнішню політику та міжнародні відносини.

Водночас використання ЦД може призводити до таких ризиків:

1. Свобода Інтернету та соціальних мереж веде до поширення неправдивої інформації, а також небезпечних ідеологій, зокрема екстремістських. Крім того, світова мережа збільшує кількість суб’єктів та інтересів, залучених до розробки політики, ускладнюючи тим самим процес ухвалення рішень і зменшуючи контроль цього процесу.

2. ЦД може бути вразливою щодо хакерських атак, які здійснюють різні державі та недержавні суб’єкти, зокрема члени служб безпеки, організованих злочинних і терористичних груп тощо.

3. Брак знань про використання цифрових комунікаційних технологій може призвести до негативних наслідків, зокрема у вигляді «витоку» важливої інформації та навіть небезпечних політичних конфліктів.

4. Культура анонімності, за якої будь-хто може видати себе за когось іншого, може спричинити серйозні кризи в результаті публікації суперечливої чи неправдивої інформації.

Загалом ЦД має більше переваг, ніж ризиків. Міжнародні актори, зокрема держави та міжнародні організації, можуть вагатися щодо використання ЦД лише через відсутність готовності та спроможності боротися з її ризиками. Таким чином, ЦД як елемент м’якої сили XXI ст. повинна супроводжуватися політикою захисту від різних загроз, які несуть інформаційно-комунікаційні технології.

Ганна МЕЛЕГАНИЧ
кандидат політичних наук, доцент
доцент кафедри міжнародних
студій та суспільних комунікацій
Каріна ТОВТИН
магістр 2-го року навчання спеціальності
«Міжнародні відносини,
суспільні комунікації та регіональні студії»
ДВНЗ «Ужгородський національний університет»

ОСОБЛИВОСТІ ФОРМУВАННЯ КІБЕРДИПЛОМАТІЇ УКРАЇНИ

На сьогоднішній день кібербезпека є одним із найважливіших аспектів національної безпеки України. Це пов'язано з активними гібридними загрозами, зокрема кібератаками з боку різних держав і організацій, а особливо з боку російської федерації, які намагаються впливати на критичні інфраструктури, державні органи та приватний сектор нашої країни.

Впродовж останніх десятиліть сфера інформаційних технологій продовжує стрімко в Україні розвиватися, перетворившись на певний феномен. Активна участь України в розробці та впровадженні новітніх підходів у сфері цифрових та інформаційних технологій, зокрема інтеграція їх у мобільний застосунок, вебпортал і бренд цифрової держави в Україні під назвою ДІЯ, водночас вимагає розробку та застосування заходів з кібербезпеки, що охоплює широкий спектр рішень, розроблених відповідно до різноманітних потреб державного та приватного секторів України для забезпечення надійного захисту від усіх видів кіберзагроз. Крім того, багато українських компаній та стартапів спеціалізуються на кібербезпеці, що зміцнює позиції країни як джерела інновацій у цій сфері і безумовно позитивно впливає на імідж країни як центру технологічних інновацій. Але так як кібербезпека вже давно стала на порядок денний для більшості держав, то це вимагає спільних узгоджених дій між країнами. На жаль, немає ще єдиного регуляторного інституту чи механізму, але певні спроби на управління а цій галузі роблять ЄС, ООН та ОБСЄ. Україна, переживаючи складні кібератаки та протидіючи їм, активно долучається до обговорення міжнародних правових норм щодо кіберпростору та бере участь у ініціативах з протидії кіберзлочинності, що сприяє налагодженню зв'язків з іншими державами. Так, як кіберпростір не обмежений державними кордонами, то це стає і сферою міжнародних та міждержавних відносин. В умовах війни Україна активно розвиває напрямок кібердипломатії, що передбачає використання кібербезпеки як інструменту для зміцнення міжнародних відносин та для підтримки стабільності в кіберпросторі. В Україні Мністерство закордонних справ має відділ кібердипломатії і ведеться активна робота над розробкою Стратегії кібердипломатії України. Варто також зазначити, що широке розуміння поняття кібердипломатія трактує як мистецтво, науку і засоби, за допомогою яких нації, групи або окремі особи ведуть свої справи в кіберпросторі, захищаючи свої інтереси і просуваючи свої політичні, економічні, культурні або наукові зв'язки, зберігаючи при цьому мирні відносини. Таким чином кібердипломатія передбачає використання дипломатичних інструментів та ініціатив для досягнення цілей як державами так і іншими суб'єктами і найкраще якщо це робиться на спільних для країн правилах чи домовленостях.

Отже, Україна останніми роками стала важливим гравцем у сфері кібербезпеки на міжнародній арені та активно розвиває кібердипломатію, що сприяє формуванню нових підходів до міжнародних відносин у цифрову епоху. Ця ситуація підвищила репутацію України як країни, здатної протистояти складним та масштабним кібератакам. Вона стає не лише жертвою, але й ефективним захисником кіберпростору, що дозволяє іншим державам вивчати її досвід.

Оксана РЕЗВАН
завідувач кафедри психології, педагогіки та мовної підготовки, доктор педагогічних наук, професор Харківського національного університету міського господарства імені О.М.Бекетова
Лідія ТКАЧЕНКО
доктор педагогічних наук, професор, завідувач кафедри теорії і методики викладання філологічних дисциплін у дошкільній, початковій і спеціальній освіті, Харківський національний педагогічний університет імені Г. С. Сковороди

ПСИХОЛОГІЯ БЕЗПЕЧНОГО ПРОСТОРУ МЕШКАНЦІВ ПРИКОРДОННОГО ВОЄННОГО ХАРКОВА

Початок повномасштабної війни в Україні актуалізував багато проблему особистої небезпеки українців, які опинились в умовах проживання на прифронтових територіях. Особливо актуальною означена проблема є для мешканців м. Харкова, що в силу своїх територіальних особливостей знаходиться під постійними ворожими обстрілами. Будь-який особистий простір – фізичний, інформаційний, психологічний – харків'яни сприймають з огляду на суб'єктивно усвідомлюваний рівень його безпеки, що частіш за все обумовлений динамікою ситуації.

Чинниками безпеки стають елементи повсякденного життя містян, які до війни не усвідомлювались як актуальні. Так, наприклад, елементом безпеки в кризово езистенційній ситуації «життя або смерть» у переважно російськомовному на початку війни місті стало «мовне питання». У сюжеті журналістки Аліни Доротюк (https://www.youtube.com/watch?v=4UAjV_-UMDc&ab_channel=%D0%90%D0%BB%D1%96%D0%BD%D0%B0%D0%94%D0%BE%D1%80%D0%BE%D1%82%D1%8E%D0%BA) представлено історію харківських волонтерів Олександра і Світлани, які на початку війни вивозили людей, заблокованих обстрілами у підвалах. Із усього трагізму тих подій особливого сенсу набула історія про мовний аспект безпекової ситуації. Олександр розповів, що коли волонтери у періоди затишшя йшли між будинками і кричали російською мовою, щоб люди виходили із укриттів, ніхто не реагував, але коли із уст одного волонтера прозвучало: «Хто є живий – виходьте!», - із підвалів повалили люди.

Найбільш популярним простором у прифронтовому Харкові, що вимушено знаходиться в умовах ізоляції (онлайн навчання, тривалі повітряні тривоги і комендантські години тощо), є інформаційний, джерела якого обираються містянами з огляду на оперативність і найбільш якісну повноту висвітлювання подій. Саме тому актуалізується проблема кібербезпеки інформаційного простору мешканців прифронтового міста.

Харків'яни досить свідомо сприймають рівень небезпеки простору, у якому перебувають повсякчас. Вони навчились розпізнавати реальну і потенційну загрози, бути готовими до миттєвих реакцій, а також фільтрувати інформацію, яка надходить з різних джерел. Варто зазначити, що найбільш стресовим для харків'ян є не стільки аварії тепло та електромереж, як нестабільність Інтернету у період і після обстрілів, коли зникає можливість отримати оперативну інформацію, яка дуже часто є запорукою збереження життя. Найбільш популярним інформаційним джерелом для харків'ян є телеграм-канали Лачен пише (https://t.me/s/lachentyt), TLk News (https://t.me/s/tlknewsua) та інші, що дозволяють отримувати саме оперативну інформацію про траєкторію рухів (та її оперативні зміни) ворожих ракет та дронів у повітряному просторі. Саме тому мешканці міст, які актуально постійно потерпають від війни не підтримують ідею закриття телеграм каналів загалом – радше модернізацію їхньої діяльності в аспекті урахування результатів розслідування діяльності тих із них, які мають відношення до використання особистих даних підписників. І саме тут актуальності набуває

зміст Конвенції Ради Європи про кіберзлочинність (Будапешт, листопад 2001 р.), в якій увага звертається на потребі досягнення паритету правоохоронних інтересів і пошани до фундаментальних прав людини таких, як право кожного безперешкодно дотримуватись поглядів, право на свободу слова, включаючи право на пошук, отримання і передачу будь-якої інформації та ідей, незважаючи на кордони, права на повагу до приватного життя, а також права на захист особистої інформації. Отже, право на отримання і використання інформації – як важливого фактору життя мешканців прифронтового міста – має бути врегульованим засобами кібербезпеки, що дозволяють городянам бути частиною інформаційного поля у найбільш безпечний спосіб.

Кібербезпека людини як користувача інформаційного простору корелює із безпекою реального фізичного простору, про який користувачам надається інформація. В аспекті означеного особливої уваги потребує урегулювання потоку коментарів на дописи підписників у повідомленнях про «прильоти» ворожих ракет та вибухи у міській інфраструктурі. Підписники, які звичайно, знаходяться під стресом після таких подій, намагаються у будь-який спосіб повідомити про локацію трагедій, при цьому ті, хто усвідомлює відповідальність за наслідки розміщення інформації, шифрують і узагальнюють інформацію так, щоб вона стала зрозумілою лише для місцевої аудиторії, наприклад, вказують лише район – без конкретизації локації, використовують сленгові назви об’єктів тощо. Варто зауважити, що адміністратори каналів використовують право блокування підписників, які в коментарях не дотримуються правил інформаційної безпеки або розпалюють ворожнечу між певними суспільними групами.

Отже, кібербезпека інформаційного простору прифронтового Харкова наразі має бути у центрі уваги відповідних органів, а у післявоєнний період може стати майданчиком для наукових досліджень у означеній галузі.

Лариса ТЕРЕМІНКО
кандидат педагогічних наук, доцент кафедри іноземних мов професійного спрямування,
Анастасія ЯРОШ
2 курс, 125 «Кібербезпека та захист інформації»
Національний авіаційний університет
Анастасія ЄВТУШЕНКО
студентка 2 курсу спеціальності «Кібербезпека та захист інформації»,
Національний авіаційний університет

СУЧАСНІ ПРАКТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ

Сучасні технології та інтенсивний розвиток цифрових інфраструктур створюють нові виклики у сфері кібербезпеки. Основною проблемою є зростання кількості кібератак та постійне удосконалення методів, які використовують зловмисники. Традиційні підходи до захисту інформації вже не забезпечують необхідного рівня безпеки, тому існує потреба у впровадженні інноваційних практик, здатних адаптуватися до нових загроз і забезпечити комплексний захист.

Метою дослідження є аналіз та оцінка сучасних практик у сфері кібербезпеки, таких як Zero Trust, використання штучного інтелекту (ШІ) для моніторингу та аналізу загроз, а також впровадження багатофакторної автентифікації (MFA). *Актуальність* дослідження полягає в необхідності розробки ефективних механізмів захисту даних в умовах збільшення складності та частоти атак, а також зростання кіберзагроз, таких як фішинг, шкідливе програмне забезпечення та соціальна інженерія.

У порівнянні з існуючими дослідженнями, дана робота зосереджена на комбінованому аналізі кількох інноваційних підходів, що вже показали свою ефективність у протидії сучасним загрозам. Зокрема, концепція Zero Trust розглядається як фундаментальний зсув у моделі довіри, що відрізняється від традиційних perimeter-based систем безпеки. Використання ШІ для аналізу великих обсягів даних дозволяє автоматично виявляти складні атаки, тоді як MFA додає додатковий рівень захисту, що значно ускладнює несанкціонований доступ.

Для досягнення мети дослідження було проведено аналіз ефективності зазначених практик на основі їх впровадження в корпоративних середовищах та в державних установах. Концепція Zero Trust продемонструвала високу ефективність у запобіганні атакам за рахунок контролю доступу на кожному рівні мережі. Використання ШІ дозволило значно скоротити час реакції на загрози й підвищити точність виявлення кібератак. Багатофакторна автентифікація забезпечила підвищення стійкості до фішингових атак та інших методів соціальної інженерії.

Основними *результатами* дослідження є виявлення ефективності сучасних підходів до кібербезпеки. Впровадження Zero Trust забезпечує більш високий рівень захисту, завдяки постійній перевірці всіх запитів і користувачів. Однак його реалізація може бути складною й вимагати суттєвих змін у існуючих системах. Впровадження ШІ у системи кібербезпеки дозволяє значно підвищити їх ефективність, зокрема, у виявленні нових типів загроз і реагуванні на них. Проте необхідно враховувати потребу в постійному навчанні моделей і можливі етичні та конфіденційні питання. Автоматизація процесів реагування на інциденти дозволяє зменшити час на виявлення і нейтралізацію загроз, що критично важливо в умовах швидко змінюваного кіберсередовища.

Таким чином, сучасні практики кібербезпеки демонструють значний потенціал у покращенні захисту інформаційних систем, проте їх ефективність залежить від правильного впровадження та інтеграції з існуючими технологіями. Подальші дослідження мають бути спрямовані на інтеграцію цих підходів у загальні архітектури безпеки й розробку нових стратегій боротьби з кібератаками.

Михайло ШЕЛЕМБА
кандидат політичних наук, доцент кафедри
міжнародних студій та суспільних комунікацій,
ДВНЗ «Ужгородський національний університет»

ЦИФРОВА ТРАНСФОРМАЦІЯ ОСВІТИ У СФЕРІ МІЖНАРОДНИХ ВІДНОСИН: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Під час дослідження підготовки фахівців з міжнародних відносин щодо цифрової трансформації в Україні були виявлені різні прогалини. Деякі з найбільш поширених проблем у цій галузі включають:

1. **Обмежена освіта з цифрових технологій:** Багато програм підготовки фахівців з міжнародних відносин можуть недооцінювати важливість цифрових технологій у сучасному світі. Внаслідок цього студенти можуть не мати достатньої підготовки у галузі цифрової грамотності, аналізу даних та використання цифрових інструментів для розв'язання проблем міжнародного масштабу.
2. **Відсутність спеціалізованих курсів з цифрової трансформації:** У багатьох навчальних програмах з міжнародних відносин може бути недостатньо спеціалізованих курсів з цифрової трансформації. Це може призводити до того, що студенти не мають можливості отримати практичний досвід з використання сучасних цифрових інструментів у своїй професійній діяльності.
3. **Недостатня увага до кібербезпеки та приватності:** У підготовці фахівців з міжнародних відносин може бути недостатньою адекватна увага до питань кібербезпеки та захисту особистих даних. Оскільки це стає все більш важливим у глобальному контексті, важливо, щоб майбутні фахівці були готові до викликів і загроз у цій сфері.
4. **Недостатня інтеграція цифрових тем у навчальні плани:** У деяких випадках цифрова трансформація може бути розглянута як додатковий елемент, а не невід'ємна частина основної програми. Це може призводити до недостатньої інтеграції цифрових тем у навчальні плани та зменшувати ефективність підготовки студентів до сучасних викликів.

Усунення цих прогалин вимагає комплексного підходу до оновлення навчальних програм, включення практичних аспектів цифрової трансформації у навчальні плани, створення можливостей для отримання практичного досвіду та розвитку цифрових компетенцій серед студентів.

Diana BOBCHYNETS
Mariia IVANOVA
***Second year Bachelor students,* "Cybersecurity and information Protection" major**
***Scientific supervisor* – Ann DYSHLEVA**
Senior Lecturer, Department of foreign languages for professional communication,
National Aviation University

THE IMPACT OF CROSS-BORDER CYBERCRIME ON GLOBAL SECURITY

The development of digital technologies has transformed the world, making cyberspace a key element of the global infrastructure. It ensures the smooth operation of businesses, government agencies, communication networks and critical systems. However, this progress has also created a serious threat in the form of cybercrime, which is increasingly crossing national borders. Cross-border cybercrime poses a serious challenge to global security, as its effects extend from the economy and governments to the personal lives of citizens.

One of the most significant aspects of cross-border cybercrime is its devastating economic impact. Experts estimate that global economic losses from cybercrime run into billions of dollars each year. Crimes related to financial fraud, phishing and data theft are becoming commonplace, affecting both individual companies and entire government agencies. One example is the attack on Equifax in 2017, when the personal data of more than 147 million people was stolen. This resulted in significant financial losses and had serious international implications. This incident illustrates the vulnerability of even the largest corporations to cyber threats.

In addition, cybercriminals often use the international nature of the Internet to avoid responsibility. The existence of different legal systems makes it difficult for law enforcement agencies in different countries to cooperate, allowing criminals to operate with relative impunity. They can launch attacks from one country while their victims are in another, making it much more difficult to bring them to justice.

In addition to economic damage, cross-border cybercrime poses a serious threat to national security. In today's world, critical infrastructures such as energy, transport, water and healthcare facilities are increasingly dependent on digital technologies. This dependence makes them attractive targets for cybercriminals who can cause significant damage to states and their citizens. Hackers or organised groups of cybercriminals often target government agencies to steal sensitive data or commit sabotage. One of the most high-profile examples was the attack on the Ukrainian energy system in 2015, which left more than 230,000 people without electricity.

Cybercrime can also be used to interfere in the political processes of countries. For example, during the 2016 US presidential election, cyberattacks on political organisations and the spread of disinformation demonstrated a new type of threat to democratic processes. Such actions can destabilise the political situation and influence the election results.

Cross-border cybercrime is often used as a tool of cyberwarfare. Governments or organised groups of hackers use cyberattacks as part of complex operations aimed at destabilising the infrastructure or political processes in hostile countries. Cyberattacks are difficult to trace and link to specific states or organisations, making them difficult to investigate. However, it is known that some states are actively developing their cyber forces to protect national interests or attack opponents in cyberspace. For example, cyberattacks during the conflicts in Syria and Ukraine have demonstrated how cybercriminals can become a tool of hybrid warfare, combining traditional military operations with cyberattacks.

These attacks can be directed not only at military targets, but also at civilian targets such as medical facilities or transport systems. Such actions can lead to serious humanitarian consequences and even loss of life.

Cross-border cybercrime poses a serious threat to global security. They affect the economy, national infrastructure, political processes and personal security. Given the growing scale and complexity of these crimes, the international community must step up efforts to improve mechanisms for combating cybercrime. This includes the creation of international standards and norms for regulating cyberspace and the development of protective measures.

The effective fight against cross-border cybercrime is only possible through close cooperation between states, information exchange and the introduction of innovative technological solutions that can counter new threats.

Illia YEVPAK
Second year Bachelor students "Cybersecurity and information Protection" major
National Aviation University
Scientific supervisor – **Natalia BILOUS**
Associate professor, Department of foreign languages for professional communication
National Aviation University

CYBER THREATS IN CROSS-BORDER FINANCIAL TRANSACTIONS

Cyber threats in cross-border financial transactions are one of the most pressing issues in today's digital world. With the growth of globalization and integration of financial markets, more and more transactions take place between different countries, which makes it difficult to control and protect such transactions. Financial institutions, companies and governments face a number of threats that can lead to financial losses and reputational damage.

One of the main cyber threats is fraud in financial transactions. Cross-border payments are often targeted by attackers due to the complexity and multi-step nature of these transactions, which increases opportunities for covert interference. Fraudsters use phishing, social engineering and compromised payment systems to steal funds or gain unauthorized access to financial data. Phishing attacks are especially dangerous because they can target company employees who unknowingly share sensitive information.

Another serious problem is money laundering through cross-border financial transactions. Cybercriminals use international banks, cryptocurrencies and payment platforms to hide the origin of illicit funds. The difficulty of tracking financial flows between different countries creates "loopholes" in the security system that criminals use to move money across borders with minimal risk of detection. Criminal groups often take advantage of loopholes in the law or different levels of security in different countries to remain undetected.

Hacker attacks on payment systems and financial institutions also pose a significant threat. Hackers are constantly improving their methods of gaining access to banking systems, intercepting transactions or stealing customer data. Attacks on payment gateways and processing centers, through which thousands of transactions pass every day, are particularly dangerous. Denial-of-service (DDoS) attacks or system breaches can paralyze banking institutions and lead to large financial losses for both the institutions and their customers.

Protecting cross-border financial transactions requires financial institutions and governments to implement advanced cybersecurity measures. This includes multi-factor authentication, data encryption, real-time transaction monitoring and the development of effective systems to share cyber threat information between countries. Additionally, increasing employee and customer awareness of cybercriminal tactics is critical to minimizing the risks of human error. In today's world of global financial transactions, cyber security has become a key element of the success and stability of the international economic system.

Victoria KARPENKO
Evgenia LICHENKO
Second year Bachelor students,
"Cybersecurity and information Protection" major
National Aviation University
***Scientific supervisor* – Ann DYSHLEVA**
Senior Lecturer,
Department of foreign languages for professional communication
National Aviation University

INTERNATIONAL RESPONSE MECHANISMS TO CROSS-BORDER CYBER INCIDENTS

International mechanisms for responding to cross-border cyber incidents are becoming increasingly important as cybercrime grows in both scale and complexity, as well as in its impact. These mechanisms largely depend on cooperation between governments, private companies, and international law enforcement agencies. Given the global nature of cyber threats, effective responses require international coordination, public-private partnerships, and well-established information-sharing frameworks.

One of the leading efforts in this field is the World Economic Forum's Partnership Against Cybercrime. This partnership emphasizes the necessity of close collaboration between the public and private sectors, law enforcement agencies, and cybersecurity experts. The goal of this initiative is to create information-sharing networks that allow for the rapid identification and response to new threats, such as malware and supply chain attacks. By combining the resources of various sectors, this partnership aims to increase the costs for cybercriminals and limit their ability to operate effectively. Additionally, the initiative promotes the development of standardized protocols to ensure the integrity and resilience of interconnected supply chains in the face of complex attacks like ransomware.

Another important mechanism is INTERPOL's Gateway initiative, which facilitates cooperation between international law enforcement agencies and private companies to enhance their ability to track and respond to cyber incidents. INTERPOL's partnerships with the private sector enable law enforcement to tap into technical expertise and private sector data, accelerating and improving the accuracy of cybercrime investigations. Moreover, global public awareness campaigns coordinated by INTERPOL play a crucial role in preventing cyber incidents by raising public understanding of cyber risks.

Additionally, the Cybercrime Atlas initiative, supported by global companies like Microsoft, Fortinet, and PayPal, provides tools for mapping the cybercriminal ecosystem. This platform helps improve the understanding of how cybercriminal networks operate, facilitating operational collaboration between the public and private sectors to identify and disrupt cybercriminal structures. By increasing the visibility of cybercriminal activities, this platform fosters global cooperation among stakeholders in the fight against cybercrime.

Effectively combating cybercrime requires international cooperation and well-established information-sharing mechanisms. Cybercrime does not respect national borders, making it essential to respond through joint efforts. Collective actions, including public-private partnerships and multilateral frameworks, help reduce the risks of cyber incidents, support law enforcement efforts, and strengthen global cybersecurity resilience.

Another critical aspect is collaboration to enhance the security of industrial control systems (ICS) and operational technology (OT), which are increasingly becoming targets for cybercriminals. As manufacturing systems become more digital, they also become more vulnerable to cyber threats. International cooperation and information-sharing are critical to ensuring the protection of such systems from increasingly sophisticated threats. For example, efforts to protect critical infrastructure from attacks on industrial control systems are a vital part of national and global security strategies.

Moreover, international efforts are essential for the rapid response to large-scale cyber incidents. According to Secure Futures, global collaboration allows for more effective coordination during crisis situations in cyberspace. For instance, global information-sharing initiatives enable the swift exchange of data about attacks and vulnerabilities, leading to a faster and more coordinated response.

In the future, as cyber threats continue to evolve, international cooperation mechanisms will become even more critical. Joint efforts by governments, the private sector, and international organizations to develop shared tools, platforms, and protocols will be key to strengthening global resilience against cyber threats. Specifically, creating joint tools for analyzing cybercriminal activity and standardizing response methods will help reduce risks and improve security in the digital world.

Only through active international cooperation and the sharing of best practices can the global community effectively combat the growing threat of cybercrime and ensure the resilience of the digital infrastructure that modern society relies on.

Olena KOVALCHUK
Maria MOGYLEVETS
Second year Bachelor students,
"Cybersecurity and information Protection" major
National Aviation University
***Scientific supervisor* – Ann DYSHLEVA**
Senior Lecturer,
Department of foreign languages for professional communication,
National Aviation University

CROSS-BORDER COOPERATION IN CYBERSPACE: THE KEY TO SHAPING GLOBAL SECURITY STANDARDS

The thesis is aimed at studying the role of transboundary cooperation in cyberspace as a tool for shaping global security standards. The study examines the main mechanisms of international cooperation in the field of cybersecurity, assesses the effectiveness of existing international agreements and initiatives, and identifies prospects for further development of cross-border cooperation to strengthen cybersecurity. The relevance of the topic is driven by the growing number of cyber threats that do not recognize state borders, making cross-border cooperation particularly important. In today's world, where digital technologies are a key element of the functioning of the economy, public administration and society, cybersecurity issues are becoming extremely important. The development of universal security standards and rules through international cooperation is a critical step towards creating a safer cyberspace.

The development of technology and globalisation are creating new challenges for cybersecurity, especially in the wake of a pandemic. Social networks, with their growing influence on society, require special prote

An analysis of Ukrainian legislation shows that it needs to be adapted to European standards, despite the ratification of the Council of Europe Convention on Cybercrime, which covers a number of important issues such as fraud, counterfeiting and copyright infringement. Ukraine's legal framework needs to be updated to respond more effectively to cyber threats. As noted by O. Polyakov, international cooperation is key to overcoming the legal vacuum created by the rapid development of information technology and the lagging behind of legislative mechanisms for responding to modern cyber threats. International cooperation is aimed at building trust between countries, developing common approaches to countering cyber threats, consolidating efforts in investigating cybercrime and preventing the use of cyberspace for illegal activities.

The most advanced system of cyber defence of critical infrastructure exists in the United States. NIST standards developed in the US are actively used around the world to help identify and prevent cyber threats. The 2003 US National Cyber Security Strategy has become an important element of the country's national security strategy. This strategy defines three main goals: protecting critical infrastructure from cyber attacks, reducing vulnerability to such attacks, and minimising damage and recovery time after incidents. In France, the 2015 Digital Security Strategy, which complements the 2013 White Paper on Defence, focuses on protecting national sovereignty, fighting cybercrime, increasing digital literacy, ensuring economic security and strengthening the country's international role. Given the EU's progress in establishing cybersecurity mechanisms, Ukraine should actively engage in these processes. This will improve its international image and contribute to the formation of a national cybersecurity system.

Cross-border cooperation in cybersecurity initiated by international organisations is an example of joint efforts to combat cyber threats, which increases the level of protection of the information space. In addition, the development of new cybersecurity technologies within the framework of international cooperation allows for the creation of more effective means of protection against cyberattacks. Ukraine, which is waging active hybrid warfare, including in cyberspace, participates in international initiatives. It cooperates with NATO countries in the framework of the Locked Shields exercise,

which allows it to improve joint actions in the event of cyberattacks; cooperates with the United States in the framework of the Cybersecurity Cooperation Initiative, which includes intelligence sharing, training and technical assistance; and cooperates with the EU in the field of cybersecurity through the exchange of experience and coordination of actions during cyber incidents.

Since 2015, the National Cybersecurity Index has been used to assess the cyber resilience of countries. It not only helps to measure the ability of states to withstand cyber threats, but also serves as a tool for comparing and improving national security systems. Despite the fact that Ukraine demonstrates a high level of cyber readiness, effective international information exchange requires mutual trust between countries.

Building mutual trust in cyberspace requires the creation of flexible cybersecurity standards that take into account national peculiarities. It is important to conduct a detailed analysis of cyber risks in each country and form joint working groups involving governments, international organisations and businesses. The task of these groups is to develop standards that will allow countries to choose the best solutions to protect their cyber infrastructure. It is also important to introduce mechanisms for testing these standards and obtaining feedback from the states that use them.

In conclusion, cross-border cooperation in the field of cybersecurity plays a key role in shaping global standards for the protection of cyberspace. Given the ever-increasing number of cyber threats that do not recognise state borders, it is international cooperation that ensures effective counteraction to these challenges. As a country facing hybrid threats, Ukraine is actively involved in international initiatives that help it develop its own cyber defence capabilities. At the same time, for successful cooperation with other states, especially within NATO and the EU, it is necessary to continue harmonising national legislation and standards with international ones. The development of universal but flexible cybersecurity standards based on mutual trust between countries can become the basis for more effective counteraction to cyber threats at the global level. Thus, cross-border cooperation in cyberspace is not only a tool for ensuring the security of individual states, but also an important factor in improving security around the world.

ОСОБЛИВОСТІ ВИМОГ ДО КІБЕРЗАХИСТУ ІНФОРМАЦІЙНОЇ КОМУНІКАЦІЇ, ЕКОНОМІКИ ТА ІНШИХ СФЕР ДІЯЛЬНОСТІ ЛЮДИНИ

REQUIREMENTS FOR CYBER PROTECTION OF INFORMATION COMMUNICATION, ECONOMY AND OTHER SPHERES OF HUMAN ACTIVITY

INFORMÁCIÓS KOMMUNIKÁCIÓ, A GAZDASÁG ÉS AZ EMBERI TEVÉKENYSÉG EGYÉB TERÜLETEINEK KIBERBIZTONSÁGÁRA VONATKOZÓ KÖVETELMÉNYEK

HIRES-LÁSZLÓ Kornélia
PhD, főiskolai docens,
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola,
intézményvezető,
Hodinka Antal Nyelvészeti Kutatóközpont
NAGY Mariann Zsuzsanna
II. évfolyamos
nemzetközi kapcsolatok, társadalmi kommunikáció
és regionális tanulmányok szakos hallgató,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

A PISA-TESZTEK PÉNZÜGYI MŰVELTSÉG KUTATÁSA ÉS A KIBERBIZTONSÁG

A kutatási probléma megfogalmazása.

A kiberbiztonság fogalma egyre fontosabbá válik a digitális világ fejlődésével. Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) úgy definiálja a kiberbiztonságot mint „a számítógépes rendszerek, hálózatok és programok integritásának, titkosságának és elérhetőségének védelmét a kiberfenyegetésekkel szemben" (ENISA 2017). A kiberbiztonság nem csupán technikai kérdés, hanem stratégiai szempontból is lényeges, mivel a digitális fenyegetések folyamatosan fejlődnek, éppen ezért az ENISA 2020-ban kidolgozta stratégiai célkitűzéseit, mellyel Európa-szerte a digitális bizalmat és biztonságot szerették volna kialakítani (ENISA 2020). A bizalom fenntartása és szavatolása bármely gazdasági szintéren egyre nagyobb kihívást jelent, ugyanis a szolgáltató egységek online platformjain a kliensek és ügyfelek adatainak biztonságát egyre nagyobb veszély fenyegeti, az online elérésen keresztül az ügyfelek személyes, továbbá a banki adataik válnak elérhetővé a bünözők számára. A kibertámadások terén tapasztalható változásokról éves jelentést tesz közé az ENISA-ügynökség, amely a 2023-as jelentésében bemutatják, 2016-tól 2022-ig hogyan alakult ez a folyamat. Azt is látnunk kell, hogy a technika fejlődésében megjelent a mesterséges intelligencia és az IoT (Internet of Things), melyek új típusú fenyegetéseket generálnak. Miorandi és szerzőtársai (2012) a technikai fejlődésről szóló tanulmányukban kiemelik, hogy a hagyományos védekezési módszerek már nem elegendőek, és új megközelítések szükségesek (Miorandi et al. 2012). A modernizáció következtében a digitális gazdaság dinamikusan növekszik. A vállalatok egyre inkább online platformokat használnak termékeik és szolgáltatásaik népszerűsítéséhez. Az e-kereskedelem, a digitális marketing és a közösségi média révén a cégek globális piacokra juthatnak el, csökkentve ezzel a hagyományos kereskedelem korlátait. A McKinsey Global Institute (2016) tanulmányai is rámutatnak arra, hogy a digitális technológiák integrálása a gazdasági folyamatokba jelentős produktivitásnövekedést eredményezett.

A kiberszféra növekedése azonban nem mentes a kihívásoktól. A kiberfenyegetések, mint például a hackelés, adatszivárgások és kiberbűnözés komoly kockázatot jelentenek a vállalatok és a gazdaság egészére nézve. A Deloitte Könyvvizsgáló és Tanácsadó Kft. 2020-as jelentése hangsúlyozza, hogy a cégeknek fokozottan figyelniük kell a kiberbiztonsági intézkedésekre, mivel a kiberincidensek nemcsak pénzügyi veszteséget, hanem hírnévromlást is okozhatnak (Deloitte 2020). A kiberszféra új üzleti modellek kialakulásához is vezetett. Az olyan szolgáltatások, mint a felhőalapú tárolás, a megosztáson alapuló gazdaság (pl. Uber, Airbnb) és a digitális termékek (pl. szoftverek, e-könyvek) forradalmasították a piaci struktúrákat. Ezek a modellek nemcsak új lehetőségeket teremtenek, hanem új szabályozási kihívásokat is, amelyek a gazdaság hagyományos kereteit feszegetik.

A PISA Programme for International Student Assessment (Nemzetközi Tanulói Teljesítménymérés Program) mérést az OECD-országok 15 éves diákjai körében végzik, és három évente ismétlik a felmérést 1996 óta. A PISA-tesztnek több területe van, mellyel különböző képességeket mérnek fel. Az egyik ilyen terület a matematika-problémamegoldó képesség és matematikai tudás értékelése – a teszt során a diákoknak olyan problémákat kell megoldaniuk, amelyek a matematikai fogalmak alkalmazását igénylik a valós életben. A második az olvasási

készségek, melyben a szövegértés mellett a szövegalkotási készségeket is méri. A feladatok célja, hogy értékeljék, hogyan tudják a diákok értelmezni a szövegeket és következtetéseket levonni azokból. A harmadik részterület a természettudományos készségek mérése, mely a diákok tudományos ismereteit és problémamegoldó képességeit vizsgálja. A teszt célja, hogy megállapítsa, mennyire tudják alkalmazni a természettudományos ismereteiket a mindennapi életben. A PISA-tesztelésnek immár negyedik területévé vált 2015 óta a pénzügyi műveltség, és ezzel új dimenziót adva a teszt célkitűzéseihez. A pénzügyi műveltség célja, hogy felmérje, mennyire képesek a diákok kezelni pénzügyi helyzeteket, döntéseket hozni és kezelni pénzügyeiket. (OECD/INFE 2021, PISA 2018). 2022-ben negyedik alkalommal került megrendezésre, és Magyarország is ekkor csatlakozott a kutatáshoz. A PISA 2022-es pénzügyi műveltségi mérésén összesen 20 ország és gazdaság vett részt, ebből 14 teljes jogú OECD-tag, mellettük 6 szakmai partnerország. A vizsgálat azt értékeli, hogy a 20 ország diákjai milyen mértékben rendelkeznek azokkal az iskola keretein belül és kívül is elsajátítható készségekkel, amelyek szükségesek jelenlegi és jövőbeli sikeres pénzügyi döntéseik meghozatalához, valamint jövőbeli terveik elkészítéséhez. A PISA által mért adatok egyre intenzívebben keltik fel a figyelmét a gazdasági szakértőknek, ugyanis számos elemzést végeznek az országokban mért eredmények és a gazdasági mutatók összehasonlításában. Természetesen vannak olyan szakértők is, akik cáfolják ezeket az összefüggéseket (Feniger–Lefstein 2014). A számok viszont magukért beszélnek, állítják neves szakértők is (Czaika–Parsons 2017), és egyértelműen kimutatják, ha nincs gazdasági krízis, amely elsősorban a gazdaság más szektoraiban bekövetkezett változásokból fakadnak, akkor a humánerőben rejlő potenciál válik az adott ország húzóerejévé.

A kiberbiztonság szempontjából a gazdasági műveltség mérése kulcsfontosságú, mivel a digitális környezet és a gazdasági folyamatok szoros összefonódása egyre nagyobb jelentőséggel bír. A gazdasági műveltség ismerete nemcsak a személyes pénzügyi döntésekhez szükséges, hanem a kiberbiztonsági fenyegetések megértéséhez és kezeléséhez is hozzájárul. A gazdasági műveltség lehetővé teszi a felhasználók számára, hogy tudatosabban értékeljék a kiberbiztonsági kockázatokat. Az egyének és a vállalatok pénzügyi veszteségei szorosan összefüggnek a kiberincidensekkel. A PwC könyvvizsgáló és gazdasági tanácsadó vállalat 2020-as jelentése szerint a kiberbűnözés évente milliárdokat von el a globális gazdaságtól, és a megfelelő kiberbiztonsági intézkedések hiánya súlyos pénzügyi következményekkel járhat (PwC 2020). A gazdasági műveltség mérése segíti a cégeket abban, hogy azonosítsák a potenciális fejlesztési lehetőségeket, és felmérjék a kiberbiztonsági beruházások megtérülését. A gazdasági műveltség terjedése a kiberbiztonság területén segít az etikai és jogi kérdések megértésében is. A szervezeteknek tudomásul kell venniük a pénzügyi és jogi következményeket, amelyek a kiberincidensek következtében felmerülnek. A European Union Agency for Cybersecurity (ENISA 2019) jelentése hangsúlyozza, hogy a jogi keretek megértése elengedhetetlen a megfelelő védelmi stratégiák kialakításához.

A tanulmány célja és relevanciája

A kibertámadások elemzéseit összefoglaló tanulmányok egyértelművé tették, hogy a legnagyobb veszélynek maguk a felhasználók vannak kitéve, ugyanis a támadók rajtuk keresztül tudnak a legegyszerűbben eljutni az adott cég szerveréhez (ENISA 2024). 2022-ben kiberbűnözők világszerte közel 8000 milliárd dollárnyi kárt okoztak a cégeknek és felhasználóknak. Szakértők előrejelzése szerint 2025-re ez a szám eléri, majd meghaladja a 10 500 milliárd dollárt, 2028-ban pedig megközelítheti a 13 820 milliárd amerikai dollárt. Ezek a fenyegetések globális szintűek, s az Európai Unió annak ellenére, hogy számos újítást vezet be a biztonság szavatolása érdekében, valamint növeli a kibertámadások kivédésére szánt pénzforrásokat, a veszélyek nem hanyatlanak, csak növekednek (ENISA 2023). Az országok gazdasági fejlődésének egyik igen fontos faktorává vált a kiberbiztonság szavatolása, vagyis a nemzetközi befektetők és cégek immár nemcsak az adott ország emberi erőforrásait, adóügyleteit, nyersanyagforrásait, kereskedelemi útvonalait elemzik, hanem azt is, hogy az országban milyen törvényeket hoztak és miként tartatják be azokat a kibertér védelme érdekében. Éppen ezért minden uniós tagállam és nemzetállam létrehozta a saját kiberboztonsággal foglalkozó ügynökségét, illetve elfogadtak törvényeket a cégek és a magánszemélyek vagyonának, adatainak biztonsága érdekében, s ezeket a folyamatos támadások változására reflektálva meg is újítják. Az Európai Unió által kidolgozott irányelvek minden tagállam számára egy alapdokumentum:

- NIS I. irányelv (2016/1148/EU): A NIS (Network and Information Security) irányelv célja a hálózati és információs rendszerek biztonságának javítása az EU tagállamaiban. Az irányelv megköveteli a tagállamoktól, hogy kiberbiztonsági stratégiákat alakítsanak ki, és megfelelő intézkedéseket hozzanak a kiberfenyegetések elleni védelem érdekében. Az érintett szolgáltatóknak (pl. energiaszektor, közlekedés, egészségügy) a kiberbiztonsági incidenseket jelenteniük kell.
- NIS II. irányelv (2022/2555/EU): célja a NIS I. irányelv hiányosságainak orvoslása, és a kiberbiztonság szintjének emelése az EU-ban. Az új irányelv szélesebb körben vonja be a szolgáltatókat és az iparágakat, beleértve a közszolgáltatásokat és a digitális szolgáltatókat is. Az érintett szolgáltatóknak részletesebb kiberbiztonsági intézkedéseket kell bevezetniük, és rendszeres kockázatértékeléseket kell végezniük.

GDPR (Általános Adatvédelmi Rendelet): célja a személyes adatok védelme az EU-ban, ami szorosan összefonódik a kiberbiztonsággal. A rendelet megköveteli az adatkezelőktől, hogy megfelelő technikai és szervezési intézkedéseket hozzanak a személyes adatok védelme érdekében. A szervezeteknek 72 órán belül be kell jelenteniük a személyes adatokat érintő incidenseket az illetékes hatóságnak.

Cybersecurity Act (2019): megerősíti az EU kiberbiztonsági ügynökségének, az ENISA-nak (Európai Hálózat- és Információbiztonsági Ügynökség) szerepét. A rendelet keretet ad az EU-szintű kiberbiztonsági tanúsítványok kiadására, amelyek célja a termékek, szolgáltatások és folyamatok biztonságának biztosítása. Az ENISA megerősített szerepet kap a tagállamok kiberbiztonsági kapacitásának fejlesztésében.

A tudományos elemzés újszerűsége

Az elemzések kihangsúlyozzák, hogy a védelmet biztosító szoftverek kialakítása mellett a civil lakosság tájékoztatása az egyik legfontosabb feladat. Számos következménye van annak, amikor a civil lakosság válik áldozatul. A pénzügyi bűncselekmények személyi áldozatai az őket ért pénz- és vagyonvesztésen kívül sokszor maradandó, súlyos érzelmi, pszichológiai és egészségi károsodást is elszenvednek (Davies et al. 2003; Dunn 2007). Illetve arra vonatkozó elemzéseket is olvashatunk, hogy a támadók az áldozatokat sokszor bizonyos személyiségjegyek mentén válogatják ki (FINRA 2016; Goucher 2010). Egy az Egyesült Államokban végzett kibertámadásokról szóló elemzés (Internet Crime Complaint Center – IC3)) alapján azt láthatjuk, hogy a 60 év fölötti lakosság van a legnagyobb veszélyben, és korcsoportonként csökken ennek értéke, kivéve a 20 év alatti korosztályt, náluk ahhoz képest, hogy nem végeznek kereső tevékenységet, kárérték arányban kimagaslóan magas veszteséget élnek meg. Éppen ezért lényeges ennek a korosztálynak célirányos fejletészt biztosítani már a középiskolai tanulmányaik során.

A PISA 2022 vizsgálat során a pénzügyi műveltség mérésére kidolgozott tartalmi keret jelentős lépést jelent a pénzügyi oktatás fejlődésében. Ez a keret a pénzügyi tudás széles spektrumát fedi le, és célja, hogy részletesen feltárja, hogyan értelmezik és alkalmazzák a diákok a pénzügyi ismereteket különböző kontextusokban. A keret nemcsak a korábbi mérések eredményeire épít, hanem figyelembe veszi a tanulók pénzügyi műveltségét befolyásoló legújabb szociodemográfiai/ szocioökonómiai (társadalmi-gazdasági) és pénzügyi változásokat is, valamint a pénzügyi neveléssel kapcsolatos legfrissebb kutatási eredményeket (OECD 2023). A pénzügyi műveltség mérésére szolgáló tartalmi keret négy fő területet ölel fel, amelyek alapvető fontosságúak a pénzügyi tudás teljes körű megértéséhez: a pénz megjelenési formáival és funkcióival kapcsolatos ismeretek, valamint a pénzügyi tranzakciók lebonyolítása és a pénzügyi dokumentumok kezelése; a bevételek és kiadások nyomon követése, a pénzügyi célok kitűzése és a vagyon növelésére irányuló lehetőségek megértése. Összességében tehát a 15 éves korosztály képességeit vizsgálják, hogy mennyire tudják kezelni a személyes pénzügyeket és hatékonyan tervezni a jövőt, miközben tudatosan kezelik azokat a kockázatokat, amelyek a kiber térben érhetik őket. Az eredményekből egyértelműen kirajzolódik, hogy azok az országok, amelyek célirányosan beépítették az oktatási tananyagok közé ezen ismeretek elsajátítását, azok a diákok tudatosabban látják át a gazdasági lehetőségeket, de még a kockázatokat is. Az OECD-országok felnőtt lakossága körében végzett felmérésekben tapasztalt tendenciák (OECD/INFE 2023) rendre visszaigazolódnak a fiatalok körében végzett eredmények kiértékelése

során, vagyis az bizonyos, hogy amilyen pénzügyi műveltséget láthatunk a felnőttek körében, azt megközelíti a 15–16 évesek körében végzett PISA-teszthez kapcsolt felmérés is.

A kiberbiztonsági tudatosság növelése a legfontosabb lépés a fiatalok körében. Az iskolákban és egyetemeken bevezetett kiberbiztonsági képzések nemcsak a technikai készségek fejlesztésére, hanem a kiberfenyegetések megértésére is összpontosítanak. A Cybrary és más online platformok különböző tanfolyamokat kínálnak, amelyek segítenek a diákoknak megismerni a kiberbiztonság alapjait. A jövő generációjának fontos, hogy gyakorlati készségeket sajátítson el, mint például a kódolás, a hálózati biztonság és a problémamegoldás. Az ilyen készségek lehetővé teszik számukra, hogy aktív szereplői legyenek a kiberbiztonsági területnek, és hozzájáruljanak a digitális környezet védelméhez.

Összefoglalás és következtetés

Mint láthattuk, a modern világ fejlődésével a kibertámadások kivédése terén maguk a nemzetközi szervezetek is nehezen boldogulnak. A védelem szavatolása érdekében számos törvényt, szigorítást vezetnek be elsősorban a cégek és a bankok üzemeltetésében. Továbbá az egyértelműen látható, hogy az intézkedések ellenére a kibertérben bűnözők megtalálják védőmechnizmusok rendszerében azokat a kisebb réseket, amelyek révén az ügyfelek bizalmában férkőzve elérik céljukat: megfosztják őket vagyonuktól, vagy rajtuk keresztül megszerzik az adott céghez tartozó kliensek elérhetőségét. A PISA-teszt immár nemcsak az iskolai teljesítményt és a tudás szintjét mérő eszközzé vált, hanem a jövőbeli pénzügyi sikerhez szükséges készségek felmérésének is kulcsszereplője. A pénzügyi műveltség bevezetése a PISA keretrendszerébe azt tükrözi, hogy a pénzügyi tudás egyre fontosabb szerepet játszik a fiatalok felkészültségében a valódi élet kihívásaival szemben. Az ilyen típusú felmérések révén lehetőség nyílik arra, hogy jobban megértsük a pénzügyi tudás hatását, és célzott intézkedéseket hozzunk annak fejlesztésére az iskolai és társadalmi szinten egyaránt. Az oktatási teljesítmény közvetlen kapcsolatban áll a munkaerőpiaci sikerrel és az egyéni életminőséggel, amely közvetetten befolyásolja az országok gazdasági növekedését és társadalmi fejlődését (Lusardi & Mitchell 2014).

Felhasznált források:

1. Czaika, Mathias – Parsons, Christopher R. (2017). The Gravity of High-Skilled Migration Policies *Demography* (2017) 54 (2) pp. 603–630. https://doi.org/10.1007/s13524-017-0559-1
2. Davies, P. – Francis, P. – Jupp, V. (eds.) (2003): *Victimology: Theory, Research and Policy*. New York: Palgrave Macmillan.
3. Deloitte (2020). https://www2.deloitte.com/content/dam/Deloitte/hu/Documents/audit/Transparency%20Report_Deloitte%20Kft_2019_HUN.pdf
4. Dunn, P. (2007): Matching service delivery to need. In: Walklate, S. (ed.): *Handbook of Victims and Victimology.* Abingdon, UK: Routledge, 255–281.
5. ENISA – Európai Unió Kiberbiztonsági Ügynöksége https://www.enisa.europa.eu/about-enisa/about/hu
6. ENISA (2017) A bizottság közleménye az európai parlamentnek, a tanácsnak, az európai gazdasági és szociális bizottságnak és a régiók bizottságának https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52017DC0228
7. ENISA (2020). A Trusted and Cyber Secure Europe. ENISA Strategy https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy
8. ENISA (2023). NIS INVESTMENTS. https://www.enisa.europa.eu/publications/nis-investments-2023
9. ENISA (2024). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
10. FINRA (2016) Financial Industry Regulatory Authority: FINRA risk meter. https://www.finra.org/investors/tools-and-calculators

11. Goucher, W. (2010): Becoming a cybercrime victim. *Computer Fraud and Security*, 10, 16–18
12. Lusardi, A. and O. Mitchell (2014), "The economic importance of financial literacy: Theory and evidence", *Journal of Economic Literature*, Vol. 52/1, pp. 5–44, https://doi.org/10.1257/jel.52.1.5.
13. Lusardi, A., O. Mitchell and V. Curto (2010), "Financial Literacy among the Young*", Journal of Consumer Affairs*, Vol. 44/2, pp. 358-380, https://doi.org/10.1111/j.1745-6606.2010.01173.x.
14. Mayda, A. M. (2010). International migration: a panel data analysis of the determinants of bilateral flows. *Journal of Population Economics*, 23(4), 1249–1274
15. McKinsey Global Institute (2016) https://www.mckinsey.com/mgi/overview/in-the-news/2016
16. Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Netw*. Vol. 10, pp. 1497–1516.
17. OECD (2020), PISA 2018 Results (Volume IV): Are Students Smart about Money?, PISA, OECD Publishing, Paris, https://doi.org/10.1787/48ebd1ba-en.
18. OECD/INFE (2023) International Survey of Adult Financial Literacy. https://www.oecd.org/en/publications/oecd-infe-2023-international-survey-of-adult-financial-literacy_56003a32-en.html
19. PISA (2018). Programme for International Student Assessment (PISA) https://www.oecd.org/pisa/Combined_Executive_Summaries_PISA_2018.pdf
20. PwC (2020) https://www.pwc.com/hu/hu/aboutus/assets/jelentesek/transparency_report%20_fy20-Hungary_hu.pdf
21. Feniger, Y. – Lefstein, A. (2014) How not to reason with PISA data: an ironic investigation. *Journal of Education Policy*, 2014 Vol. 29, No. 6, 845–855, DOI:10.1080/02680939.2014.892156
22. Czaika, M. – Parsons, C. R. (2017). The Gravity of High-Skilled Migration Policies. *Demography: Population Association of America*. DOI 10.1007/s13524-017-0559-1

LOSZKORIH Gabriella
docens, tanszékvezető-helyettes,
Számvitel és Auditálás Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
BÁTORI Vivien
MSc-hallgató,
Nemzetközi Számvitel és Adóügy képzési program,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

A KÉSZPÉNZ NÉLKÜLI ELSZÁMOLÁSOK DIGITALIZÁLÁSA: A DIGITÁLIS KORSZAK ÚJ KIHÍVÁSAI

A mai gazdasági környezetben a számvitel hatékony megszervezése, beleértve a készpénz nélküli elszámolások számvitelét, a vállalkozások sikeres működésének kulcsfontosságú eleme. Ezekben az elszámolásokban a bank a pénzügyi közvetítő szerepét tölti be. Az általa nyújtott szolgáltatások az ügyfeleinek – a vállalkozásoknak, vállalkozóknak és a magánszemélyeknek – a modern gazdasági rendszer fontos részét képezik. A készpénz nélküli elszámolások eljárását törvény szabályozza. A bankokon keresztül történő készpénz nélküli elszámolások segítenek optimalizálni pénzügyi folyamataikat és csökkenteni a készpénzes tranzakcióktól származó felelősségüket, ami hozzájárul a gazdaság stabilitásához.

A készpénz nélküli elszámolások digitalizálása rohamosan fejlődik, ugyanakkor új kihívásokat is nyit a digitális technológiák korszakában. A digitális fizetések növekedése és a pénzügyi folyamatok automatizálása egyszerre jelent lehetőségeket és veszélyeket a gazdaságok és a vállalkozások számára.

A hatályos hazai jogszabályok értelmében hazánk területén minden kifizetés készpénzes vagy készpénz nélküli formában történik.

Készpénzes elszámolások – a gazdálkodó szervezetek és magányszemélyek készpénzes kifizetései az eladott termékekért (áruk, elvégzett munkák, szolgáltatások), valamint az olyan tranzakciókért, amelyek közvetlenül nem kapcsolódnak a termékek (áru, munka, szolgáltatás) és egyéb vagyontárgyak értékesítéséhez [2].

Készpénz nélküli elszámolások – a pénzeszközök a fizető fél számlájáról a kedvezményezett számlájára történő átutalása, valamint a fizető fél által készpénzben elhelyezett pénzeszközöknek a pénzforgalmi szolgáltatók által a kedvezményezett számlájára történő átutalása [3].

Ukrajna Polgári Törvénykönyve szerint: „A jogi személyek közötti elszámolásokat, valamint a magánszemélyek vállalkozói tevékenységével kapcsolatos elszámolásokat készpénzmentes elszámolási formában kell teljesíteni. Ezen személyek közötti elszámolások készpénzben is teljesíthetők, hacsak a jogszabály másképp nem rendelkezik. A magánszemélyek és jogi személyek, valamint az egyéni vállalkozók készpénzes kifizetéseinek maximális összegét az Ukrán Nemzeti Bank állapítja meg” [4].

Ukrajna pénzforgalmi szolgáltatásokról szóló törvénye szerint: „A készpénz nélküli elszámolások – pénzeszközök átutalása a fizető felek számláiról a címzett számláira, valamint a fizető fél által készpénzben elhelyezett pénzeszközöknek a pénzforgalmi szolgáltatók által a címzett számlájára történő átutalása” [5].

Az elszámolási bizonylat a készpénz nélküli elszámolások lebonyolítására és a pénzeszközök átutalására szolgál a fizető számlájáról a kedvezményezett számlájára. Az elszámolási bizonylat formája: papíralapú vagy elektronikus. Az elektronikus elszámolási bizonylat olyan fizetési bizonylat, amelyen az információ elektronikus adatok formájában jelenik meg, és tartalmazza a vonatkozó adatokat; az elszámolási bizonylatot az ügyfél hozza létre, továbbítja, tárolja, átalakítja vizuális formába és továbbítja a banknak anélkül, hogy az ügyfélnek fel kellene keresnie egy bankintézetet. A bank ügyfele saját számlájának távoli karbantartását az alábbi távrendszerek segítségével végezheti: „Ügyfél-bank”, „Ügyfél-Internet Bank”, „Internet Banking” stb.

A készpénz nélküli elszámolások fő szempontjai napjainkban magukba foglalják a következőket: banki átutalások, kártyás tranzakciók, mobilfizetések, elektronikus számlák, bérkártyák és készpénz

nélküli kifizetések. Ezek a technológiák elősegítik a gyorsabb és hatékonyabb pénzügyi tranzakciókat, csökkentik a költségeket, valamint jobbítják a felhasználók és vállalkozások kényelmét.

A fizetési megbízás egy közös elszámolási bizonylat, amely biztosítja a készpénz nélküli fizetést és elszámolást. Meg kell jegyezni, hogy a digitális gazdasággal összefüggésben a készpénz nélküli elszámolások elektronikus fizetési módokon keresztül történnek.

Napjainkban egyre több bank és más pénzügyi intézmény támogatja aktívan a pénzátutalások és egyéb online tranzakciók alkalmazását a felek közötti nagy távolságra történő pénzátutaláshoz, ezzel lehetővé téve a fizetést bármely pénznemben és a világ bármelyik országában. Ez fokozza a gazdasági globalizáció folyamatait, mivel a kereskedelem könnyebbé válik a pénz egyszerű küldésének és fogadásának képessége révén. Az elektronikus pénz kiküszöböli a pénzeszközök fizikai átutalásának szükségességét, és sokkal kényelmesebbé teszi a banki szolgáltatásokat. Az emberek mostantól anélkül végezhetnek személyes banki tranzakciókat, hogy fizikai fiókokat kellene felkeresniük vagy készpénzt kellene maguknál tartaniuk.

A digitális készpénz nélküli elszámolások fő előnyei:

- az automatizált fizetési rendszerek lehetővé teszik a műveletek végrehajtásához szükséges idő jelentős csökkentését és az emberi tényezővel kapcsolatos hibák elkerülését;
- a készpénz nélküli elszámolások digitális formában történő nyilvántartása lehetővé teszi az egyes műveletek nyomon követését, ami csökkenti a csalás kockázatát;
- a digitális fizetési rendszerek használata lehetővé teszi a vállalatok számára a nemzetközi piacokon való működést, a pénzügyi tranzakciók gyors és biztonságos lebonyolítását.

A készpénz nélküli elszámolások előnyei közül érdemes megemlíteni a magasabb védelmet a rablás és pénzhamisítás ellen, valamint a gazdálkodó szervezetek bevételeinek és kiadásainak nagyobb átláthatóságát, ennek eredményeként az árnyékgazdaság, az adóelkerülés és a pénzmosás lehetőségeinek csökkenését [1]. A pénzforgalom digitalizálási folyamatának azonban negatív vonatkozásai is lehetnek. Kritikusai rámutatnak arra a veszélyre, hogy az állam és a pénzintézetek totális ellenőrzést gyakorolnak mind a gazdasági egységek, mind az állampolgárok felett. Véleményünk szerint egy másik fontos érv a kiberkockázatok növekedése – hackertámadások, kiberkémkedések stb.

A készpénz nélküli elszámolások fejlesztése a digitalizáció kontextusában új lehetőségeket kínál a vállalkozásoknak, ugyanakkor megköveteli a kiberbiztonság körültekintő megközelítését és a törvényi előírások betartását.

Felhasznált források:

1. Menaka, B. (2019) Electronic payment in cashless economy: Problem and prospect. *International Journal of Scientific and Technology Research,* 8.120: 2688-2690
2. Про затвердження Положення про ведення касових операцій у національній валюті в Україні: Постанова Національного банку України від 29.12.2017 № 148. URL: https://zakon.rada.gov.ua/laws/show/v0148500-17#Text
3. Про затвердження Інструкції про безготівкові розрахунки в національній валюті користувачів платіжних послуг: Постанова Національного банку України від 29.07.2022 № 163. URL: https://zakon.rada.gov.ua/laws/show/v0163500-22#Text
4. Цивільний кодекс України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text
5. Про платіжні послуги: Закон України від 30.06.2021 № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text

Габріелла ЛОСКОРІХ
доцент, доктор філософії,
заступник завідувача кафедри обліку і аудиту
071 «Облік і оподаткування»
Закарпатського угорського інституту імені Ференца Ракоці II
Оксана ПЕРЧІ
викладач кафедри обліку і аудиту
Закарпатського угорського інституту імені Ференца Ракоці II

КІБЕРБЕЗПЕКА ЯК ВАЖЛИВИЙ ЕЛЕМЕНТ ДЛЯ УСПІШНОГО ВПРОВАДЖЕННЯ ІНІЦІАТИВ BEPS

Одним із ключових елементів BEPS 2.0 є адаптація міжнародного податкового регулювання до цифрової економіки. Великим транснаціональним корпораціям, особливо технологічним гігантам, стало легше переміщувати прибутки та ухилятися від сплати податків завдяки глобальному характеру їх бізнесу, що часто не потребує фізичної присутності. BEPS 2.0 намагається вирішити це питання, встановлюючи нові правила щодо оподаткування таких компаній. Водночас розвиток цифрової економіки вимагає підвищеної уваги до питань кібербезпеки, оскільки компанії використовують цифрову інфраструктуру для ведення бізнесу та зберігання даних.

План дій BEPS (англ. Base erosion and Profit Shifting – BEPS, перекл. з англ. «Розмивання оподатковуваної бази й виведення прибутку з-під оподаткування») – основоположний документом міжнародного значення, розроблений Організацією економічного співробітництва та розвитку (ОЕСР) у співпраці з країнами Великої двадцятки (G20). План BEPS 2.0 є продовженням і розширенням ініціатив, започаткованих у рамках першого етапу Плану дій BEPS. Якщо початковий план був спрямований на боротьбу з ухиленням від сплати податків через розмивання оподатковуваної бази, то BEPS 2.0 фокусується на вдосконаленні міжнародних податкових правил, особливо в контексті цифрової економіки та глобалізації.

Офіційне приєднання до Програми розширеного співробітництва з питань імплементації плану BEPS в 2017 році, поставило перед Україною необхідність безумовного виконання чотирьох мінімальних стандартів (захід 5 щодо шкідливих податкових практик, захід 6 щодо зловживання угодою, захід 13 щодо звітування в розрізі країн та захід 14 щодо механізмів врегулювання спорів). На основі їх виконання та дотримання можливо буде відслідковувати еволюцію податків, які зумовлюють виклики цифрової економіки (захід 1), а також економічний аналіз BEPS (захід 11) [1].

У рамках BEPS ініційовано обмін податковими даними між юрисдикціями (наприклад, через механізми Country-by-Country Reporting). Це означає, що величезні обсяги фінансових та податкових даних передаються між податковими органами різних країн. Захист таких даних від кіберзагроз є ключовим завданням, оскільки витік або кібератака на ці системи можуть спричинити значні збитки як для урядів, так і для компаній.

Державна податкова служба України 3 листопада 2022 року як компетентний орган України приєдналася до Багатосторонньої угоди компетентних органів про автоматичний обмін звітами в розрізі країн (Multilateral Competent Authority Agreement on the Exchange of Country-by-Country Reports) (далі – Багатостороння угода CbC) [2]. Приєднання до Багатосторонньої угоди CbC здійснюється з метою виконання вимог Податкового кодексу України [4] щодо автоматичного обміну звітами у розрізі країн міжнародних груп компаній, а також реалізації Плану дій BEPS (Base Erosion and Profit Shifting), зокрема, Дії 13 BEPS – запровадження додаткової звітності з трансфертного ціноутворення для міжнародних груп компаній [3]. Ця система забезпечить оперативний та безперебійний обмін фінансовими даними між податковими органами різних держав. Такий підхід спрямований на підвищення прозорості діяльності транснаціональних корпорацій і дозволить ефективніше відстежувати податкові ризики, пов’язані з розмиванням податкової бази та виведенням прибутків.

Один із ключових викликів для BEPS – це оподаткування в умовах цифрової економіки, коли транснаціональні корпорації можуть вести бізнес у країнах без фізичної присутності. Кібербезпека в цьому контексті має забезпечувати: захист цифрових платформ (що використовуються для ведення бізнесу) і безпеку платіжних систем (щоб запобігти незаконним переміщенням коштів або втраті контролю над податковими надходженнями).

Отже кібербезпека є фундаментом для успішного впровадження ініціатив BEPS. Кожен аспект кібербезпеки відіграє важливу роль у підтримці стабільності та прозорості міжнародної податкової системи. В умовах, коли міжнародні податкові системи стають все більш взаємопов'язаними, а транснаціональні корпорації активно використовують цифрові платформи, надійний захист від кіберзагроз стає не просто додатковою перевагою, а необхідністю.

Список використаних джерел:

1. Бодров В., Фенюк Я. Глобальні виклики офшоризації та проблеми антиофшорної політики в Україні. *ІІ Міжнародний податковий конгрес [Електронне видання] : збірник матеріалів (м. Ірпінь, 26 листопада 2021 р.).* Ірпінь: Університет ДФС України, 2021.С. 27-33.
2. Державна податкова служба України. Україна приєдналася до Багатосторонньої угоди компетентних органів про автоматичний обмін звітами в розрізі країн. URL: https://zak.tax.gov.ua/media-ark/news-ark/print-629501.html (дата звернення: 29.09.2024).
3. Міністерство фінансів України. BEPS. URL: https://mof.gov.ua/uk/beps-440 (дата звернення: 25.09.2024).
4. Податковий кодекс України: Закон України від 02.12.2010 № 2755-VI. URL: https://zakon.rada.gov.ua/laws/show/2755-17#Text (дата звернення: 25.09.2024).

Анастасія ОМЕЛЬЧЕНКО
студентка 1 курсу магістратури,
факультет психології
Київського національного університету імені Тараса Шевченка

РОЛЬ HR У ФОРМУВАННІ КОРПОРАТИВНОЇ КІБЕРБЕЗПЕКИ: УПРАВЛІННЯ РИЗИКАМИ, ПОВ'ЯЗАНИМИ З ЛЮДСЬКИМ ФАКТОРОМ

Постановка наукової проблеми: Людський фактор є критичним у кібербезпеці, оскільки поведінка працівників впливає на захист компанії. Недотримання протоколів, слабка обізнаність та ненавмисні витоки інформації є ключовими ризиками, які HR може мінімізувати через ефективні кадрові процеси.

Мета дослідження: Дослідити роль HR у зниженні ризиків, пов'язаних з людським фактором, шляхом інтеграції HR-процесів у стратегію кібербезпеки для підвищення стійкості компанії.

Наукова новизна: Запропоновано новий підхід до інтеграції HR та кібербезпеки через управління ризиками: політики найму, навчання, плани реагування на інциденти та моніторинг поведінки. Акцент зроблено на людському факторі як ключовому елементі кібербезпеки.

Людський фактор залишається одним з найбільших вразливих у корпоративній кібербезпеці. Помилки, недбалість чи зловмисні дії працівників часто призводять до витоків даних і фінансових збитків. Кіберзлочинці все частіше використовують людську поведінку для атак, оскільки технічні системи стають дедалі захищенішими. Найпоширеніші ризики включають слабкі паролі, незнання правил безпеки та підвищену вразливість до фішингових атак.

HR може мінімізувати ці ризики, впроваджуючи політики найму та навчання, орієнтовані на кібербезпеку. Важливою є організація регулярних тренінгів з кіберзагроз і мотивація працівників дотримуватись безпекових протоколів. Впровадження систем винагород за активну участь у забезпеченні безпеки може посилити відповідальність персоналу.

Співпраця між HR та IT є важливою для створення надійної системи захисту. HR впливає на поведінку працівників, тоді як IT забезпечує технічну експертизу. Спільні політики щодо доступу до даних, реагування на інциденти та моніторинг поведінки працівників допомагають зменшити ризик внутрішніх загроз. Для інтеграції HR у стратегії кібербезпеки рекомендується впроваджувати постійні програми навчання та оцінки кіберповедінки. Розробка інцидент-менеджмент планів, де HR відіграє ключову роль, допоможе забезпечити ефективну координацію під час кіберзагроз. Таким чином, людський фактор стає не лише джерелом ризику, а й інструментом для підвищення безпеки компанії.

Висновки: Дослідження показало, що інтеграція HR у процеси кібербезпеки здатна суттєво знизити ризики, пов'язані з людським фактором. Через впровадження спеціалізованих тренінгів, впровадження систем мотивації та контролю за дотриманням кібербезпекових протоколів HR може стати ключовим елементом у захисті організації. Створення спільної платформи взаємодії між HR і відділом IT є необхідною умовою для побудови надійної системи корпоративної кібербезпеки.

Список використаних джерел

1. Smith, J. (2021). Human Factor in Corporate Cybersecurity: A Comprehensive Review. *Journal of Cybersecurity Research*, 12(3), 45-60.
2. Williams, K. & Johnson, M. (2022). Integrating HR into Cybersecurity Strategies: Minimizing Human Risks. *Cybersecurity and Management*, 8(1), 78-90.
3. Brown, L. (2021). Employee Awareness and Cybersecurity: The Role of HR Training Programs. *International Journal of HR and Cybersecurity*, 6(2), 22-34.
4. Taylor, P., & Adams, R. (2022). Cybersecurity Threats: How Human Behavior Impacts Corporate Security. *Cyber Defense Quarterly*, 15(2), 91-105.
5. Gomez, D. (2023). The Critical Role of HR in Managing Cybersecurity Risks: A Case Study Approach. *Journal of IT and HR Integration*, 9(4), 112-128

Ростислав РОМАНЮК
магістр 2 курсу спеціальності «Інформаційні системи та технології»
Ужгородський національний університет
***Науковий керівник* – Василь МОРОХОВИЧ**
доцент кафедри інформатики та
фізико-математичних дисциплін
Ужгородський національний університет

ОСОБЛИВОСТІ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ У МОБІЛЬНИХ ФІНАНСОВИХ ДОДАТКАХ

На сьогодні фінансові додатки є популярні, причому база їх користувачів продовжує зростати. Зокрема, за оцінками, попит на бюджетні додатки зросте на 5,4% до 2032 року, досягнувши 359,01 млн доларів США [1]. Все більше користувачів прагнуть мати можливість керувати своїми витратами, доходами, інвестиціями та іншими фінансовими операціями зі смартфона. Для засновників IT проєктів це означає великі можливості для зайняття певних ніш на ринку. Наприклад, програми, орієнтовані на представників певних професій або охоплюють різні групи користувачів, такі як власники бізнесу, звичайні користувачі, люди похилого віку і навіть діти.

Фінансові додатки взаємодіють із платіжними системами, великою кількістю особистої інформації та особистими обліковими записами користувачів. Це чутливі точки, які потенційно можуть бути піддані зловмисному програмному забезпеченню та порушенню безпеки. У таких умовах для розробників інструментів управління особистими фінансами першорядне значення має забезпечення безпеки додатків. Цього можна досягти за допомогою інтеграції з рішеннями безпеки фінансових технологій, складними алгоритмами шифрування даних, політикою доступу до мережі без довіри, фільтрацією DNS, інтеграцією безпечного шлюзу веб-доступу та хмарними заходами безпеки [2].

Найкращими методами захисту персональних даних у мобільних фінансових програмах є: надійна автентифікація користувача, шифрування даних, регулярні оновлення та керування виправленнями, захищена серверна інфраструктура, навчання користувачів щодо безпеки [3].

Надійний процес автентифікації користувача є першою лінією захисту для фінансових програм. Реалізація методів багатофакторної автентифікації, таких як поєднання паролів, біометричних даних і одноразових паролів, додає додатковий рівень безпеки. Це зменшує ризик несанкціонованого доступу, навіть якщо пароль користувача буде зламано. Тому є необхідність використання біометричної автентифікації, наприклад відбитки пальців або технологія розпізнавання обличчя. Також треба реалізувати двофакторну автентифікацію, яка потребує як пароля, так і унікального коду, надісланого на мобільний пристрій користувача.

Мобільні фінансові додатки мають шифрувати конфіденційні дані як у стані спокою, так і під час передачі. Шифрування перетворює звичайний текст у нечитабельний формат, ускладнюючи потенційним зловмисникам доступ до особистої інформації. Для цього необхідно використовувати надійні алгоритми шифрування, такі як AES-256, щоб захистити дані користувача, та шифрувати їх під час передачі за допомогою безпечних протоколів (HTTPS).

Оновлення фінансових додатків має вирішальне значення для забезпечення безпеки. Регулярні оновлення та керування виправленнями гарантують швидке усунення будь-яких вразливостей, що ускладнює зловмисникам використання цих слабких місць. З цією метою треба увімкнути автоматичні оновлення для мобільного додатку, щоб користувачі завжди використовували останню версію, а також регулярно перевіряти бюлетені безпеки та застосовувати патчі, щойно вони стануть доступними.

Безпека фінансових програм виходить за межі простого інтерфейсу користувача. Серверна інфраструктура також має бути укріплена для захисту персональних даних. Розробники додатків повинні дотримуватися найкращих галузевих практик щодо безпечного кодування та використовувати безпечні інфраструктури для захисту всієї системи. Тому потрібно регулярно

проводити оцінку вразливості та тестування на проникнення, щоб виявити потенційні слабкі місця, впроваджувати жорсткі засоби контролю доступу, щоб обмежити неавторизований доступ до серверних систем.

Обізнаність користувачів відіграє важливу роль у захисті персональних даних у фінансових програмах. Розробники додатків повинні надавати чітку та стислу інформацію про заходи безпеки, а також навчати користувачів загальним методам безпеки, щоб мінімізувати ризик витоку даних.

Таким чином, захист особистих даних у мобільних фінансових додатках є надзвичайно важливим. Застосовуючи надійну автентифікацію користувачів, шифрування даних, регулярні оновлення, безпечну серверну інфраструктуру та навчання користувачів, фінансові програми можуть значно зменшити ризик витоку даних і несанкціонованого доступу до конфіденційної інформації. Дотримання цих практик не лише захистить дані користувачів, але й підвищить загальну довіру до фінансових програм.

Список використаних джерел

1. How to build a budgeting app: opportunities, challenges, and practical tips. – [Електронний ресурс]. – Режим доступу: https://leobit.com/blog/how-to-build-a-budgeting-app-opportunities-challenges-and-practical-tips/.
2. Mobile application data security and privacy – best practices. – [Електронний ресурс]. – Режим доступу: https://www.ideosoftware.com/blog/mobile-application-data-security-and-privacy,221.html.
3. Mobile development for financial apps: security and privacy. – [Електронний ресурс]. – Режим доступу: https://moldstud.com/articles/p-mobile-development-for-financial-apps-security-and-privacy.

Victoriia Kurdulian
Evheniy Kucheriavy
Second year Bachelor students,
"Cybersecurity and information Protection" major
National Aviation University
***Scientific supervisor*- Nataliia DENISENKO**
Senior Lecturer,
Department of foreign languages for professional communication,
National Aviation University

INFORMATION SECURITY OF MODERN BUSINESS ORGANIZATIONS

The relevance of business information security is an integral component in today's world. The development of information technologies allows businesses to earn significant benefits by accelerating efficiency and improving the management of various processes. Confidential data, creative activity and customer information are some of the most valuable data. Large companies are attacked dozens of times a day, while cybercriminals constantly scan the information security perimeter and monitor vulnerabilities. That's why companies should prioritize cybersecurity to protect their information, maintain customer trust, and not lose their reputation.

First, let's consider the concept of cyber security. Cybersecurity is a term that describes the set of methods and procedures used by businesses and IT professionals to ensure an adequate level of protection of an organization's confidential electronic data and digital systems from unauthorized intervention and theft for the purpose of extortion, blackmail and business damage.

Most commonly, cybercriminals use tactics such as phishing attacks, malware, and social engineering to compromise systems and steal data. They look for software vulnerabilities, misconfigurations, and human error as entry points.

Today, there is no single algorithm for detecting threats in corporate information systems, due to the fact that each system requires an individual approach, but there are measures that can be used to minimize it:

1. Artificial Intelligence (AI) and Machine Learning (ML) are critical tools for cybersecurity. It can analyze massive amounts of data and detect and respond to anomalies and threats in real time before humans can, reducing the risk of data leakage.
2. Zero trust is a protected behavior, no one can be trusted either inside or outside the organization. Every user and device is considered trustworthy and their information and opinions are guaranteed.
3. Multi-factor authentication (MFA) adds another layer of security by requiring users to provide two or more forms of authentication before access is granted. It can be something they own (for example, a phone) or something they know (for example, a password).

Companies should invest in virtual private networks, firewalls, and biometric authentication to protect against data leaks, malware, and other malicious activities. In addition, organizations need to be aware of the latest cybersecurity technologies and ensure that their employees are properly trained in cybersecurity protocols to better understand the risks associated with working in digital spaces and how to improve them.

Regular software updates are critical to protecting a company's IT infrastructure by addressing security issues, reducing security risks, and using appropriate security tools. In essence, software updates are not just about adding new functionality, they are the foundation of an overall cybersecurity strategy in today's business environment.

To determine if your business is prepared for an emergency, it is important to include security policies and procedures in your emergency management plan. The plan should be regularly reviewed and updated to ensure it is up-to-date. It should include information on who is responsible for which tasks, the reporting chain to be followed and the contact details of all relevant parties. The plan should also include a checklist of actions to be taken in the event of an incident and the location of all relevant documentation.

In short, an information security management system (ISMS) is an essential tool for. Organizations need to continually update and improve their ISMS to adapt to changing trends and opportunities while protecting their assets and continuing to use them.

Олена КОБУС
завідувач кафедри технологій
захисту кіберпростору центру кібербезпеки
Національна академія СБ України
Степан БОНДАРЕНКО
фахівець кафедри технологій захисту кіберпростору
центру кібербезпеки
Національна академія СБ України

КІБЕРЗАГРОЗИ ДЛЯ ВЕЛИКИХ ДАНИХ (BIG DATA): СТРАТЕГІЇ ЗАХИСТУ І БЕЗПЕКИ

З експоненціальним зростанням обсягів даних організації почали покладатися на здатність використовувати, аналізувати та робити висновки з величезних масивів даних. Однак, саме масштаб і складність, які роблять великі дані потужними, також наражають їх на значні кіберзагрози. Витоки даних, хакерські атаки, програми-вимагачі та інсайдерські загрози створюють серйозні ризики для конфіденційності, цілісності та доступності даних,що робить стратегії кібербезпеки критично важливими для будь-якої організації, яка покладається на великі дані. Великі дані вразливі до різноманітних кіберзагроз, які стають все більш витонченими. Складність архітектури даних у поєднанні зі зростаючою залежністю від розподілених і хмарних систем зберігання створює численні точки вразливості. Кіберзлочинці, хактивісти, представники національних держав та зловмисні інсайдери використовують ці вразливості, прагнучи скористатися цінністю, що зберігається у величезних масивах даних. Розуміння природи цих загроз є першим кроком до розробки надійних механізмів захисту.

У лабіринті сучасних обчислювальних парадигм великі дані – онтологічний джаггернаут цифрової економіки – знаходяться на перетині об'ємних інформаційних потоків і всепроникних векторів кіберзагроз. Протеїнова природа кібернетичних супротивників, які використовують обмеженість плинності даних, кидає виклик традиційній ортодоксальності захисту периметру, роблячи його застарілим. Оскільки дані виходять за межі статичних сховищ, заселяючи динамічні хмарні екосистеми, матриця загроз експоненціально розростається, створюючи епістемологічний дисонанс між механізмами захисту і новими онтологіями загроз.

Діалектика між шифруванням і контролем доступу, яка колись вважалася непорушною, тепер видається недостатньою в середовищі, де архітектури нульової довіри (ZTA) повинні одночасно демонтувати і реконструювати саме поняття цифрової довіри. У цій схемі автономність алгоритмів машинного навчання у виявленні сучасних постійних загроз (APT) створює загадкову головоломку: чи може ШІ, який сам є вразливим до ворожих маніпуляцій, по-справжньому зміцнити цілісність таких величезних і різнорідних наборів даних? Більше того, етичні наслідки токенізації блокчейну, хоча і проголошені його криптографічною незмінністю, викликають глибокі питання щодо суверенітету даних у все більш децентралізованому кібер-геополітичному ландшафті. Таким чином, стратегічні імперативи захисту великих даних вимагають зміни парадигми – такої, що виходить за рамки простого технічного захисту і охоплює цілісну інтеграцію прогностичної аналітики на основі штучного інтелекту, гармонізацію регуляторних норм і міцний етос кіберстійкості. Без такого метаморфозного підходу крихка рівновага між корисністю та безпекою даних і надалі залишатиметься недосяжною навіть для найсучасніших архітектур.

Андрій МАЛЬЦЕВ
Студент 2-го курсу спеціальність
«Інженерія програмного забезпечення»
Природничо-гуманітарний
фаховий коледж ДВНЗ «УжНУ»
***Науковий керівник* – Л. ДАНЬКО -ТОВТИН**
викладач вищої категорії, методист
Природничо-гуманітарний
фаховий коледж ДВНЗ «УжНУ»

ТЕХНОЛОГІЯ «ZERO TRUST»

Сучасна структура підприємств стає дедалі складнішою та комплекснішою. Одне підприємство може оперувати кількома внутрішніми мережами, віддаленими офісами з власною інфраструктурою та хмарними службами. Ця складність значно випередила застарілі методи кібербезпеки на основі периметру. Адже після прориву периметру нападникам відкритий шлях всередину організації. Ця проблема призвела до розробки нової моделі кібербезпеки, відомої як «zero trust» («нульова довіра»). Такий підхід насамперед зосереджений на захисті даних і послуг, але може бути розширеним, щоб включати всі активи підприємства / організації. Модель «zero trust» передбачає, що зловмисник присутній у середовищі, що належить підприємству, і що це середовище не є надійнішим ніж будь-яке інше.

«Zero trust» - це набір керівних принципів для організації робочого процесу, проектування систем та операцій, які можна використовувати для покращення стану безпеки. Організаціям потрібно впроваджувати комплексні практики інформаційної безпеки та стійкості, щоб цей принцип працював. Якщо це збалансовано з існуючою політикою кібербезпеки, керування ідентифікацією та доступом, то «zero trust» здатне захистити від багатьох поширених загроз та значно покращити стан кібербезпеки організації. Багато організацій уже мають елементи системи «нульової довіри», а ще більше – прагнуть до неї.

КІБЕРБЕЗПЕКА: ЗАКОРДОННИЙ ДОСВІД

CYBER SECURITY: FOREIGN EXPERIENCE

KIBERBIZTONSÁG: KÜLFÖLDI TAPASZTALATOK

DARÓCI Ádám
oktató,
Matematika és Informatika Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
SZÁNTÓ Kevin
BSc-hallgató,
Informatika szak,
Matematika és Informatika Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

KIBERBIZTONSÁGI STRATÉGIÁK AZ AMERIKAI EGYESÜLT ÁLLAMOKBAN

A kibertérben történő események kétséget kizárva hatással vannak a fizikai világra, ezzel még azok is tisztában vannak, akik teljesen ki akarták zárni magukat a digitális létből. Nagyon jó példa erre a 2016-os amerikai elnökválasztás, amelyben fontos szerepet játszott a közösségi hálózatokon keresztüli befolyásolás egy külső szereplő által [2].

Amerika továbbra is szeretné alakítani a globális kibertér jövőjét és megelőzni a fentebb említett befolyásolásokat, ennek eredménye pedig egy friss, 2023-as nemzeti kiberbiztonsági stratégia kibocsájtása volt, amely a Trump-adminisztráció által 2018-ban kiadott kiberbiztonsági stratégiát váltotta fel. A stratégia sikeressége nagyban függ az amerikai infrastruktúrától és Kína egyre növekvő jelenlététől is, hisz Amerika Kínát az egyik legnagyobb fenyegetésnek tartja. Feltételezve azt, hogy tényleg sikerül megvalósítani a kitűzött céljaikat, az nagyban fogja befolyásolni az amerikai kibertér biztonságát, emellett a szövetségesek nagy része követni fogja az amerikai példát, miközben az ellenfelek továbbra is fenyegetni fogják kibereszközökkel Amerika biztonságát. A sikeresség nagyban függ attól, hogy milyen gyorsan tudnak megbarátkozni a Biden-kormányzat alapelveivel [1].

Az újonnan kiadott stratégia 5 fő pillérre épül. Az első ilyen pillér a kritikus infrastruktúrák védelme. Ebben nagyon fontos elv a kötelező szabályozások szükségessége és felállítása lenne. Ez a pillér hangsúlyozza a kiberbiztonsági kötelező követelmények felállítását, hisz nagyon fontos, hogy a kritikus infrastruktúrák tulajdonosai és működtetői megfelelő kibervédelmet biztosítsanak. Az adminisztráció már egyes szektorokat érintve határozott meg követelményeket ezzel kapcsolatban, míg más szektorokban az új adminisztráció dolga lesz ez. A köz- és magánszféra együttműködtetését is szorgalmazza, mivel elengedhetetlennek tekintik ezt [1].

Ezután egyből kiemelik Kínát mint legnagyobb fenyegetést, ennek megoldására pedig a következő pillérben találjuk a választ, amely a fenyegető szereplők megzavarását és felszámolását taglalja. Ennek a pillérnek az eléréséhez az Egyesült Államok kész alkalmazni a nemzeti hatalom valamennyi eszközét, integrálva az információs, pénzügyi, katonai, titkosszolgálati, rendőri, diplomáciai kapacitásokat. Az Egyesült Államok különösen nagy figyelmet kíván fordítani a kiberbűnözés elleni küzdelemre, azon belül is a zsarolóprogramok legyőzésére [1].

A következő pillér a piaci erők biztonsági szempontú formálása, ami nagyon fontos az ellenálló képesség növelése érdekében. A konkrét cél a digitális gazdaság, amelyben a felelősséget azokra hárítják, akik a kockázat csökkentésének szempontjából a legjobb pozícióban vannak. Ez az intézkedés arra fogja a piacot ösztönözni, hogy biztonságosabb szolgáltatásokat és termékeket értékesítsen, mivel a felelősség a végfelhasználókról azokra hárul, akik tudnak is kezdeni valamit az üggyel [1].

A következő pillér a rugalmas jövőbe való befektetésről szól. Az USA szerint egy ellenálló és virágzó digitális jövő kialakítása a ma megtett befektetéssekkel kezdődik, melyek révén az Egyesült Államok élen tud maradni a biztonságos, rugalmas, következő generációs technológiák és infrastruktúrák innovációjában [1].

Végül, de nem utolsósorban, az ötödik pillér a nemzetközi partnerségek kialakítása a közös célok elérése érdekében. Évtizedek óta dolgoznak nemzetközi szervezetekben a magatartásszabályok megalkotásán, de nem ez az egyetlen rendelkezésre álló módszer, amely erősítené a nemzetközi együttműködést. 2022-ben az USA kiadott egy nyilatkozatot, amely az internet jövőjéről szól, s már

60 állam csatlakozott ehhez. A kibertérben az USA arra törekszik, hogy a felelős állami viselkedés váljon alapvető normává, miközben a felelőtlen magatartást a nemzetközi szövetségek és az egy irányba haladó országok együttműködése révén elkülönítsék és jelentős anyagi terhekkel sújtsák [1].

A felhasznált irodalmakból kiderül, hogy a kiberbiztonság fejlesztése még egy olyan előrehaladott orszgnál is, mint az Egyesült Államok, komoly befektetést igényel. Az ilyen fajta befektetés nem csak anyagilag megterhelő. A felsorolt öt pillér megvalósításához huzamosabb időre lesz szükség, valamint a partnerországok és a magánszektorbeli szervezetek összefogását is igényli. Azonban kijelenthetjük, hogy amennyiben sikerül ezt a tervet megvalósítani, akkor az Egyesült Államok kiberbiztonsága, és így a nemzeti biztonsága is hatalmas fejlődésen megy majd keresztül.

Felhasznált források:

1. Molnár, D., & Nagy, G. (2023). A 2023-as amerikai kiberbiztonsági stratégia áttekintése és értékelése. Hadtudomány, 33(E), 88–100. doi:10.17047/hadtud.2023.33.e.90
2. Csaba K. (2017). A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. Nemzet és Biztonság – Biztonságpolitikai Szemle, 10(3), 38–53. Retrieved from https://folyoirat.ludovika.hu/index.php/neb/article/view/3718

MOLNÁR Ferenc
docens, PhD, tanszékvezető-helyettes,
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
KEREKES Ariána
II. évfolyamos
nemzetközi kapcsolatok, társadalmi kommunikáció
és regionális tanulmányok szakos hallgató,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

GÖRÖGORSZÁG KIBERBIZTONSÁGA

Kulcsszavak: *Görög Nemzeti Kiberbiztonsági Hatóság, kritikus infrastruktúra, Görögország, kibervédelem, kiberbűnözés.*

A digitalizáció fejlődése és a technológiai újítások gyors üteme mélyrehatóan alakítják át Görögország társadalmi és gazdasági életét, ahogy az ország egyre inkább a digitális infrastruktúrára támaszkodik. Az egyre növekvő internetes kapcsolatok és az IoT-eszközök (Internet of Things) elterjedése elősegítette a technológiai fejlődést, de ugyanakkor egyre nagyobb kiberfenyegetések megjelenéséhez is vezetett. Az adatok biztonságának fenntartása, a kritikus infrastruktúrák védelme és a kibertámadásokkal szembeni ellenállóképesség kialakítása létfontosságúak lettek a modern Görögország számára.

Ebben a kontextusban Görögország kiberbiztonsági helyzete és törekvései középpontba kerültek, különös tekintettel az ország 2020–2025-ös Nemzeti Kiberbiztonsági Stratégiájára. Ez a stratégia átfogó megközelítést alkalmaz a kibertámadásokkal szembeni védekezésben, amelynek fő céljai közé tartozik a kibertudatosság növelése, a kritikus infrastruktúrák védelmének megerősítése, valamint a nemzetközi együttműködés kiterjesztése.

Kiberfenyegetések és kibervédelem Görögországban

Az elmúlt években Görögország egyre jelentősebb kiberfenyegetésekkel szembesült. Ezek a fenyegetések változatos formákban jelennek meg, beleértve a zsarolóvírusokat, az adatlopásokat és a kritikus infrastruktúrák elleni támadásokat. A zsarolóvírusok (ransomware) különösen nagy aggodalmat keltenek, mivel ezek a támadások képesek megbénítani egész szervezetek működését, különösen a kormányzati és pénzügyi szektorokban. Az ilyen támadások során a támadók titkosítják az áldozat adatbázisait és rendszereit, és váltságdíjat követelnek a visszaállításukért.

Adatvédelem és Személyes Adatok Biztonsága: Az adatok biztonságának fenntartása kiemelt fontosságú Görögország számára, különösen az állami szektorban, amely jelentős mennyiségű személyes adatot kezel. A görög kormány törekvései közé tartozik a GDPR (General Data Protection Regulation) irányelveinek teljes körű betartása, hogy megvédje a lakosság adatait és biztosítsa azok jogszerű felhasználását. Ezt a görög Adatvédelmi Hatóság (Hellenic Data Protection Authority, HDPA) ellenőrzi, amely szorosan figyelemmel kíséri a személyes adatok kezelését és az adatvédelmi incidenseket.

Kritikus Infrastruktúrák Védelme: A görög kritikus infrastruktúrák, beleértve az energia, közlekedési, egészségügyi és pénzügyi rendszereket, kiemelten fontosak a nemzetbiztonság szempontjából. Az ilyen rendszerek elleni kibertámadások jelentős gazdasági károkat okozhatnak, és komoly társadalmi zavarokhoz vezethetnek. A *Cyber Threats and Critical Infrastructures in Greece* című tanulmány rámutat arra, hogy Görögország energetikai ágazata különösen sebezhető a kiberfenyegetésekkel szemben. Az ország energiahálózatai és olajvezeték-rendszerei például számos digitális rendszert használnak, amelyek célpontjai lehetnek kiberbűnözőknek vagy államilag támogatott támadóknak [3].

A Görög Nemzeti Kiberbiztonsági Stratégia (2020–2025)

A görög kormány a Nemzeti Kiberbiztonsági Stratégiájával jelentős előrelépést tett a kibervédelmi intézkedések terén. Az ország felismerte, hogy az egyre növekvő digitális kapcsolódás mellett elengedhetetlen egy átfogó stratégia kidolgozása a fenyegetések kezelésére. A stratégia kulcsfontosságú elemei a következők:

– a kiberbiztonsági tudatosság növelése: A görög lakosság és vállalatok körében fontos a kiberbiztonsági tudatosság növelése. A kormány célja, hogy széles körű tájékoztató kampányokkal és képzési programokkal segítse a lakosság és a kis- és középvállalkozások kiberbiztonsági felkészültségét. Az oktatási programok célja, hogy a lakosság jobban megértse a fenyegetéseket, és képes legyen megvédeni személyes adatait.

– az állami és magánszektor együttműködése: A kormány felismerte, hogy a kibertámadások elleni védekezés nem valósítható meg a magánszektor bevonása nélkül. A stratégia egyik központi eleme az állami és magánszféra közötti együttműködés javítása, különösen a kritikus infrastruktúrákat működtető vállalatokkal. Ez magában foglalja az információmegosztást, a kiberincidensek gyors bejelentését és a közös védekezési intézkedések kialakítását.

– a kiberbiztonsági kutatások és technológiai fejlesztések támogatása: Görögország a nemzetközi trendekkel összhangban kiemelt figyelmet fordít a kiberbiztonsági kutatások és innovációk támogatására. A kormány célja, hogy ösztönözze az új technológiák fejlesztését és alkalmazását, amelyek segítségével az ország hatékonyabban tud reagálni a kibertámadásokra. Ezenkívül szoros együttműködésre törekszik az EU-val és más nemzetközi szervezetekkel a legújabb kiberbiztonsági fejlesztések terén [2].

Görögország és az Európai Unió kiberbiztonsági együttműködése

Görögország aktívan részt vesz az Európai Unió kiberbiztonsági kezdeményezéseiben, különösen a NIS2 irányelv (Network and Information Systems Directive) végrehajtásában. Az EU ezen irányelve előírja a tagállamok számára, hogy fokozzák kritikus infrastruktúráik védelmét, és biztosítsák, hogy a digitális szolgáltatások megfelelően védve legyenek a kibertámadásokkal szemben. A NIS2 irányelv célja, hogy javítsa a tagállamok közötti információcserét, erősítse a nemzeti kiberbiztonsági hatóságok közötti együttműködést, és harmonizálja a különböző ágazatok kiberbiztonsági előírásait.

Az EU-n belüli szorosabb együttműködés lehetővé teszi Görögország számára, hogy hozzáférjen a legjobb gyakorlatokhoz és technológiákhoz, amelyek elősegítik az ország védelmi képességeinek javítását. Emellett Görögország szorosan együttműködik más nemzetközi szervezetekkel, például a NATO-val is, amelynek kiberbiztonsági központjai hozzájárulnak a tagállamok kibervédelmi képességeinek erősítéséhez [6].

Oktatás és kibertudatosság

Az oktatás és a kiberbiztonsági tudatosság kulcsfontosságú szerepet játszanak Görögország kiberbiztonsági stratégiájában. Az ország felismerte, hogy a megfelelően képzett kiberbiztonsági szakemberek hiánya komoly kockázatot jelent a védekezési képességekre nézve. Ennek érdekében a kormány több kezdeményezést is indított az oktatási intézményekkel és egyetemekkel együttműködve.

A görög felsőoktatási intézmények egyre több kiberbiztonsági képzést kínálnak, amelyek célja a fiatal szakemberek felkészítése a digitális fenyegetésekkel szembeni védekezésre. Ezek a képzések kiterjednek a technológiai ismeretekre, az etikus hackelésre és az adatvédelemre is. Ezen túlmenően a kormány különböző szintű vállalkozások számára kínál képzési programokat, amelyek célja a kibertudatosság növelése [1].

Kihívások és jövőbeli kilátások

Bár Görögország jelentős előrelépéseket tett a kiberbiztonsági stratégiák megvalósításában, számos kihívással kell szembenéznie a jövőben. Az egyik legnagyobb kihívás a kiberbiztonsági szakemberek hiánya, amely korlátozza az ország védekezési képességeit. Ezenkívül a technológia rohamos fejlődése folyamatosan új fenyegetéseket hoz létre, amelyekkel az ország kiberbiztonsági rendszereinek folyamatosan lépést kell tartaniuk.

A jövőben Görögország célja, hogy tovább erősítse kiberbiztonsági rezilienciáját, támogassa a technológiai innovációkat, és fokozza nemzetközi együttműködését a digitális korszak új kihívásaival szemben. Az ország ezen törekvései különösen fontosak egy olyan világban, ahol a geopolitikai konfliktusok és a kibertérben folytatott államilag támogatott támadások egyre növekvő fenyegetést jelentenek. Az ilyen típusú kibertámadások, mint például a kiberkémkedés vagy kiberhadviselés,

egyre kifinomultabbak, és közvetlen veszélyt jelentenek nemcsak a kritikus infrastruktúrákra, hanem az ország politikai és gazdasági stabilitására is [4].

Kiberhadviselés és kiberkémkedés: új frontok a biztonságban

Az elmúlt években Görögország is tapasztalt kibertámadásokat, amelyek gyaníthatóan államilag támogatott aktoroktól származtak, és amelyeket geopolitikai célok motiváltak. Az ilyen típusú támadások célja általában érzékeny információk megszerzése, a politikai rendszerek destabilizálása, vagy a gazdasági előnyök megszerzése. A kiberhadviselés és kiberkémkedés jelentős kihívásokat jelent a görög biztonsági szervek számára, mivel az ilyen támadások felderítése és megelőzése rendkívül nehéz feladat. Ezek a támadások gyakran rejtett módszereket alkalmaznak, amelyek lehetővé teszik, hogy hosszú ideig észrevétlenek maradjanak, miközben komoly károkat okozhatnak [5].

Kiberreziliencia és technológiai szuverenitás

Ahhoz, hogy Görögország sikeresen szembeszállhasson a kiberfenyegetésekkel, kulcsfontosságú a kiberreziliencia folyamatos fejlesztése. Ez azt jelenti, hogy az ország képes legyen ellenállni a kibertámadásoknak, gyorsan helyreállni belőlük, és folyamatosan fejleszteni a védekező képességeit. Az egyik fontos terület a technológiai szuverenitás, vagyis az ország képessége arra, hogy független legyen a külső technológiai szolgáltatóktól, és saját fejlesztéseket, kutatásokat támogasson a kiberbiztonság területén. Görögország a helyi technológiai startupokat és kutatási központokat kívánja ösztönözni, hogy új és innovatív megoldásokat hozzanak létre a kiberfenyegetésekkel szembeni védekezés érdekében. Az EU támogatása és forrásai is fontos szerepet játszanak ebben a törekvésben, hiszen az uniós alapok és projektek lehetővé teszik a legmodernebb technológiák elérését és alkalmazását [6].

Jövőbeni prioritások: digitális átalakulás és adatbiztonság

A digitális átalakulás továbbra is kulcsfontosságú prioritás Görögország számára, mivel az ország célja, hogy egyre inkább integrálja a digitális megoldásokat a közigazgatásban, az egészségügyben, az oktatásban és más ágazatokban. Az adatbiztonság központi kérdéssé válik ebben a folyamatban, különösen a személyes adatok védelme érdekében. Az állami és magánszektornak egyaránt biztosítania kell, hogy az adatkezelés megfeleljen a legszigorúbb adatvédelmi előírásoknak, beleértve a GDPR irányelveit is. Az olyan incidensek, mint a személyes adatok kiszivárgása vagy azok illegális felhasználása, súlyos következményekkel járhatnak a lakosság bizalmára nézve, és aláásható az állami intézmények hitelességét [3].

Kiberbiztonság a közösségi szolgáltatásokban és a kritikus infrastruktúrákban

Az olyan ágazatok, mint az egészségügy, az energiaellátás és a közlekedés, különösen ki vannak téve a kiberfenyegetéseknek, mivel ezek az infrastruktúrák létfontosságúak az ország működése szempontjából. A görög kormány további lépéseket tervez a kritikus infrastruktúrák védelmének megerősítésére, beleértve a hálózati biztonsági előírások szigorítását és az esetleges kiberincidensek kezelésére szolgáló protokollok fejlesztését. Emellett fontos szerepet kapnak a különböző CSIRT-ek (Computer Security Incident Response Team), amelyek gyors reagálást biztosítanak a kiberincidensek esetén, és központi szerepet játszanak a károk minimalizálásában [4].

Nemzetközi együttműködés és a NATO szerepe

Görögország szoros együttműködést folytat nemcsak az Európai Unióval, hanem a NATO-val is a kiberbiztonsági kérdések terén. A NATO kiberbiztonsági központjai és kezdeményezései lehetőséget biztosítanak a tagállamok számára, hogy megosszák egymással tapasztalataikat és legjobb gyakorlataikat. Ez különösen fontos egy olyan dinamikusan változó területen, mint a kiberbiztonság, ahol a fenyegetések folyamatosan fejlődnek, és ahol a nemzetközi együttműködés lehet az egyik leghatékonyabb eszköz a védekezésben [6].

Összegzés

Görögország kiberbiztonsági stratégiája és törekvései folyamatos fejlődésen mennek keresztül, és az ország elkötelezett amellett, hogy lépést tartson a digitális korszak új kihívásaival. A nemzeti kiberbiztonsági stratégia, a technológiai fejlesztések támogatása, a kiberreziliencia növelése, valamint az állami és magánszektor közötti együttműködés mind olyan tényezők, amelyek kulcsfontosságúak lesznek az ország jövőbeni sikerességében a kibertérben. Az EU-val és a NATO-

val való szoros együttműködés további lehetőségeket nyújt Görögországnak arra, hogy felkészülten álljon a kiberhadviselés, kiberkémkedés és egyéb fenyegetések elé. Az ország célja, hogy a jövőben is megőrizze biztonságát és stabilitását, miközben folytatja a digitális átalakulását a globális technológiai térben.

Felhasznált források:

1. Christou, George. Cybersecurity in the European Union and Beyond.
Megjelenés éve: 2018.
Kiadó: Routledge (Letöltés ideje: 2024.10.24.)
2. https://www.enisa.europa.eu/publications (Letöltés ideje: 2024.10.24.)
3. https://www.dpa.gr/ (Letöltés ideje: 2024.10.24.)
4. https://nsa.gov.gr/ (Letöltés ideje: 2024.10.24.)
5. https://ccdcoe.org/ (Letöltés ideje: 2024.10.24.)
6.https://ec.europa.eu/digital-strategy/our-policies/cybersecurity_en (Letöltés ideje: 2024.10.24.)

Наталія ВАРОДІ
габілітований доктор,
доцент кафедри історії та суспільних дисциплін
Закарпатського угорського інституту імені Ференца Ракоці II
Сільвестер ІЖАК
студент II курсу магістратури
за спеціальністю «Історія та археологія»
Закарпатського угорського інституту імені Ференца Ракоці II

СТАН КІБЕРБЕЗПЕКИ У СВІТІ НА БАЗІ ДОСЛІДЖЕННЯ КОМПАНІЇ FLASHPOINT

Постановка наукової проблеми: Різке зростання кількості кібератак та витоків даних у 2023 році свідчить про необхідність більш потужних методів захисту та стратегій кібербезпеки для захисту від нових загроз у 2024 році. *Мета дослідження:* Оцінити сучасні кіберзагрози, проаналізувати їх розвиток у 2023-2024 роках та розробити рекомендації щодо ефективної боротьби з кіберзлочинністю, зокрема програмами-вимагачами та загрозами витоку даних. *Актуальність:* Значне збільшення кількості витоків даних та атак із використанням програм-вимагачів у 2023-2024 роках вимагає нових підходів до захисту інформаційних систем, зокрема через зростаючу активність кіберзлочинних угруповань. *Наукова новизна:* Дослідження представляє нові дані про активність кіберзлочинних угруповань, таких як LockBit, та аналізує недостатньо досліджені вразливості, що ще не мають CVE-ідентифікаторів.

Хоча 2023 рік був складним для фахівців з кібербезпеки, цілком ймовірно, що 2024 рік буде ще складнішим. Компанія Flashpoint, що займається аналізом загроз, вже спостерігала різке зростання показників різноманітних інцидентів у сфері кібербезпеки за перші два місяці цього року. Згідно зі статистикою Flashpoint, у 2023 році було зафіксовано 6077 витоків даних, при цьому зловмисники отримали доступ до понад 17 мільярдів рядків персональних даних (на 34,5% більше, ніж у 2022 році). За перші два місяці цього року цей показник зріс на 429% порівняно з першими двома місяцями минулого року. Понад 60% інцидентів 2023 року припадає на Сполучені Штати Америки. Кількість атак з використанням програм-вимагачів у 2023 році зросла на 84%, а за перші два місяці 2024 року – на 23%.

Незважаючи на великі цифри за 2023 рік, варто виділити одну кібератаку, MOVEit, і пов'язане з нею кіберзлочинне угруповання LockBit. На використання MOVEit припадає 19,3% кібератак, зареєстрованих у 2023 році, що поставило під загрозу 1 049 користувачів. Діяльність LockBit була перервана 20 лютого 2024 року, коли міжнародні правоохоронні органи вилучили їхні сервери та заарештували деяких учасників (операція «Кронос»). З того часу LockBit створили нову темну веб-сторінку, стверджуючи, що їхня діяльність продовжується безперервно. Flashpoint не настільки впевнений у цьому, оскільки вважає, що є кілька ознак того, що вищезгадана операція мала значний вплив на їхню діяльність.-,

Flashpoint підкреслила, що їхні дані та статистика отримані з загальнодоступної інформації. Збір даних компанії базується на різних темних веб-сайтах, блогах про програми-вимагачі, публічних публікаціях та NVD-вразливостях. Компанія також звертає увагу на такі критичні аспекти, як вразливості, які ще не мають CVE-ідентифікатора. У лютому 2024 року аналітики Flashpoint виявили 330 вразливостей, які кіберзлочинці експлуатували в реальних ситуаціях і які ще не мали CVE-ідентифікатора. Ці критичні недоліки впливають на такі компанії, як Adobe, Apple, Google, Microsoft, Siemens та SolarWinds.

У висновках можна зазначити, що значне зростання кількості кібератак і витоків даних у 2023 році, яке триває і в 2024-му, вимагає від державних і приватних структур оперативної реакції. Програми-вимагачі, такі як LockBit, і використання уразливостей без CVE-ідентифікаторів ставлять під загрозу критичні системи. Потрібно підсилити національні та міжнародні механізми кіберзахисту, зокрема впроваджувати проактивні заходи, модернізувати законодавство і впроваджувати нові технології для ефективної протидії цим загрозам.

Список використаних джерел:

1. Unveiling the Top 4 Cyber Threats in 2024 (2024.09.24) URL: Unveiling the Top 4 Cyber Threats in 2024 | Flashpoint
2. Flashpoint 2024 Global Threat Intelligence Report (2024.09.24) URL: Flashpoint 2024 Global Threat Intelligence Report | Flashpoint

Каріна ВАШКЕБА
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 ФРАНЦІЇ

Анотація. *Дослідження присвячене аналізу кібербезпеки у Франції, зокрема її національних стратегій та правових механізмів у контексті сучасних глобальних викликів. Окрему увагу приділено вивченню нормативних актів, таких як Закон LOPMI та Національна кіберстратегія, а також діяльності основних державних інституцій, таких як ANSSI та CNIL, що займаються захистом інформаційних систем і персональних даних. Робота досліджує досвід Франції у впровадженні кіберзахисту на рівні держави та приватного сектору, а також роль міжнародної співпраці у сфері кібербезпеки. Висвітлено ключові загрози, серед яких дезінформація, кіберзлочинність та шпіонаж, і проаналізовано ефективність заходів, спрямованих на їх нейтралізацію. Дослідження акцентує на важливості розвитку кіберграмотності серед населення та інтеграції кібербезпеки у всі сфери суспільного життя.*

Ключові слова: *кібербезпека, Франція, кіберзагрози, дезінформація, кіберзлочинність, ANSSI, CNIL, Національна кіберстратегія, інформаційні системи.*

В умовах стрімкої глобалізації та широкого розповсюдження інформаційних технологій, питання кібербезпеки стає надзвичайно важливим для кожної країни, незалежно від її економічного розвитку або геополітичної позиції. Кіберзагрози, що виникають у цифровому середовищі, зачіпають як державні структури, так і приватний сектор, створюючи ризики для національної безпеки, економічної стабільності та суспільного спокою. Сучасний світ все частіше стає свідком складних і витончених кібероперацій, які можуть порушувати функціонування критичної інфраструктури, викликати хаос у фінансових системах, ставити під загрозу персональні дані громадян та підривати довіру до державних інституцій.

Особливу загрозу становлять деструктивні інформаційні кампанії, спрямовані на дестабілізацію політичної та соціальної ситуації всередині країн. Такі операції впливу можуть викликати масову дезінформацію, спотворювати суспільну думку та розколювати єдиний інформаційний простір держави. Країни, які прагнуть послабити своїх конкурентів або отримати стратегічні переваги, часто використовують кіберзагрози як інструмент для досягнення своїх геополітичних цілей. У цьому контексті кібербезпека стає одним з основних напрямків забезпечення національної стійкості, адже вона включає не лише технічний захист від атак, а й формування стратегії інформаційної стійкості, здатної запобігти дезінформаційним кампаніям та зміцнити довіру громадян до національних інститутів.

Постановка проблеми. Франція, як одна з провідних європейських держав, несе особливу відповідальність за забезпечення безпеки як на національному, так і на міжнародному рівні, особливо після виходу Великої Британії з Європейського Союзу. З огляду на те, що Франція є єдиною державою ЄС з ядерною зброєю та постійним членством у Раді Безпеки ООН, її роль у захисті як європейської, так і глобальної безпеки значно зростає. У цьому контексті важливо розглянути, як кіберзагрози, що дедалі частіше стають інструментом геополітичного впливу та дестабілізації, впливають на національну безпеку Франції.

Кібербезпека стає невід'ємною частиною зовнішньої та внутрішньої безпекової політики Франції. З одного боку, відкриті кордони в межах Шенгенської зони та активні міграційні

процеси з Африки та Азії підвищують уразливість держави перед можливими кібератаками. З іншого боку, активна зовнішня політика Франції в Європі, Середземномор'ї, Африці та на Близькому Сході також створює додаткові виклики для захисту її інформаційного простору. В умовах сучасного цифрового світу кібероперації можуть використовуватися як для безпосереднього впливу на політичні та соціальні процеси в державі, так і для підриву її стратегічної позиції на міжнародній арені.

Проблема дослідження полягає в тому, щоб проаналізувати, які ключові виклики кібербезпеки стоять перед Францією сьогодні, та якими ресурсами й засобами вона володіє для їх подолання. Також важливо дослідити, яким чином кіберзагрози інтегруються в систему загроз національної безпеки Франції, а також як ця держава будує свою стратегію кіберстійкості, співпрацюючи з міжнародними партнерами для протидії кіберзлочинності та дезінформаційним кампаніям.

Аналіз останніх досліджень і публікацій з теми кібербезпеки Франції вказує на високу актуальність проблеми як в контексті національної безпеки, так і в рамках європейської політики у сфері безпеки та оборони. Серед наукових праць, присвячених цій тематиці, можна виділити роботи європейських та українських дослідників, які висвітлюють різні аспекти кіберзахисту та безпеки. У своїх дослідженнях науковці підкреслюють важливість кібербезпеки як стратегічного напрямку зовнішньої політики Франції, зокрема в умовах зростання міжнародних конфліктів та загроз з боку кіберзлочинності.

Роботи авторів, як Ж. Брісет та М. Арзаканян, зосереджуються на аналізі політики Франції в рамках загальноєвропейської стратегії кібербезпеки, яка є важливим компонентом загальної безпекової архітектури ЄС. Вони досліджують інтеграцію кіберзахисту у національну безпекову політику Франції, зокрема її роль як одного з ключових гравців у Європі після виходу Великої Британії з ЄС. Водночас автори, такі як О. Барабанов та В. Барановський, акцентують увагу на інституційних аспектах формування європейської кібербезпеки, аналізуючи участь Франції у міжнародних структурах, таких як НАТО та Європейське оборонне агентство.

Інші дослідники, зокрема І. Бусигіна та М. Стрежньова, фокусуються на викликах, пов’язаних із захистом національних інформаційних систем від іноземних кіберзагроз та дезінформаційних кампаній, які є особливо актуальними в умовах сучасної гібридної війни. Їхні праці аналізують роль Франції у глобальних процесах боротьби з кіберзагрозами, розглядаючи кібербезпеку як один із ключових елементів забезпечення національної стійкості.

Проте більшість наукових робіт зосереджені на зовнішніх аспектах кібербезпеки, залишаючи недостатньо дослідженими питання внутрішньої кіберстійкості Франції, зокрема розвиток її інституційної спроможності протистояти кіберзлочинності та захищати критичну інфраструктуру. Важливим залишається подальше дослідження питань, пов’язаних з координацією зусиль між різними відомствами та агенціями, а також співпрацею з приватним сектором у боротьбі з кіберзлочинністю.

Отже, аналіз наукових праць показує, що хоча кібербезпека є предметом численних досліджень, питання забезпечення національної кіберстійкості Франції вимагає подальшого розгляду, зокрема у контексті її внутрішньої політики та практичної реалізації заходів кіберзахисту.

Метою статті є аналіз сучасних викликів кібербезпеки Франції та оцінка її національної стратегії кіберзахисту в умовах глобалізації та зростання кіберзагроз. Дослідження спрямоване на вивчення заходів, які Франція вживає для забезпечення національної кіберстійкості, захисту критичної інфраструктури, протидії кіберзлочинності та дезінформаційним кампаніям, а також на оцінку її ролі в рамках європейської та глобальної систем безпеки.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ. Основні положення військової доктрини Франції викладені в «Білій книзі», перше видання якої вийшло у 1972 році, ґрунтуючись на ідеях Шарля де Голля про незалежність і велич республіки. Доктрина передбачала захист національних територій, участь у безпеці Європи та захист віддалених регіонів, де Франція

має стратегічні інтереси. Попри зміни у зовнішній політиці, подальші видання «Білої книги» продовжували дотримуватися принципів «голлізму», адаптуючи доктрину до нових глобальних викликів, включаючи розвиток кіберзагроз. У «Білій книзі» 2013 року відзначено переорієнтацію країни на співпрацю з НАТО, ініційовану ще Ніколя Саркозі та продовжену Еммануелем Макроном [3]. Документ «Стратегічний огляд» 2017 року підтвердив зміцнення трансатлантичних зв'язків і розвиток незалежної європейської оборони, що стало основою для створення «Програми розвитку збройних сил на 2019-2025 роки», яка передбачає модернізацію армії та підвищення її спроможностей [10].

Усі зазначені вище документи формують цілісну систему військово-політичних, військово-стратегічних та військово-економічних засад, які складають основу сучасної військової доктрини Франції. Вони відображають поточні пріоритети країни у сфері оборони та безпеки, адаптуючи стратегії до нових викликів, з якими стикається світ. Важливим аспектом цих доктринальних документів є акцент на різноманітних загрозах сучасного світу, зокрема таких, як кібератаки, які стають усе частішим інструментом міжнародних конфліктів і підривають національні інфраструктури.

Сучасна військова доктрина Франції враховує не лише традиційні загрози, але й новітні виклики, що виникають у зв'язку з розвитком інформаційних технологій. Окремо варто зазначити, що в умовах цифровізації та глобальної комунікації особливої актуальності набуває проблема дезінформації, яка стала потужним інструментом впливу на суспільство та міжнародні відносини. Французькі законодавці вже давно визнали дезінформацію серйозною загрозою для національної безпеки, оскільки вона здатна підірвати довіру до державних інститутів, вплинути на політичні процеси та дестабілізувати громадський порядок. Це, в свою чергу, підкреслює важливість кібербезпеки як невід'ємної складової захисту держави в умовах сучасних глобальних загроз.

Регулювання дезінформації у Франції здійснюється, зокрема, на основі Закону про свободу преси, який був ухвалений ще в 1881 році. У статті 27 цього закону детально визначено, що розуміється під терміном «фальшиві новини» та встановлено відповідальність за їх поширення. Так, публікація, відтворення або поширення будь-якими засобами недостовірної інформації, сфабрикованих матеріалів або тих, що були поширені з недобросовісною метою і можуть порушити громадський порядок або сприяти його порушенню, карається штрафом у розмірі 45 000 євро. Якщо ж такі дії ставлять під загрозу дисципліну або мораль у збройних силах чи можуть зашкодити військовим зусиллям країни, штраф може сягати 135 000 євро. Однак, як зазначають експерти, через складність доведення факту того, що певна інформація дійсно порушує громадський порядок або має дестабілізуючий вплив, ці положення закону на практиці застосовуються досить рідко [5].

Ще одним важливим законодавчим актом, спрямованим на регулювання інформаційного простору, є Закон про довіру в цифровій економіці (LCEN, Loi pour la confiance dans l'économie numérique), який було ухвалено 21 червня 2004 року. Цей закон встановлює правову основу для боротьби з контентом в Інтернеті, який сприяє розпалюванню ненависті, дискримінації або порушенню громадського порядку. Закон передбачає механізми, за допомогою яких суд може вимагати видалення з мережі будь-якого контенту, що порушує законодавство в цій сфері. Ці заходи дозволяють оперативно реагувати на випадки поширення незаконного контенту, забезпечуючи баланс між свободою слова та необхідністю дотримання правових норм у цифровому середовищі [7]. Таким чином, закон LCEN слугує важливим інструментом для підтримання безпеки та захисту прав громадян в умовах швидкого розвитку цифрових технологій.

У 2015 році Франція ухвалила Національну кіберстратегію (Stratégie nationale pour la sécurité du numérique), яка звертає увагу на те, що всі цифрові платформи, включаючи соціальні мережі, можуть формувати думку таким чином, який може не відповідати реальним цінностям країни. Часто такі платформи використовуються для поширення дезінформації та пропаганди, що призводить до негативного впливу на суспільну думку. У випадках, коли ці платформи сприяють поширенню цінностей, які суперечать основоположним інтересам

Франції, такі дії підпадають під регулювання законодавства, яке стосується національної безпеки та оборони [11]. Таким чином, кіберстратегія Франції наголошує на необхідності контролю та регулювання цифрового простору з метою захисту країни від інформаційних загроз, що можуть підривати її національні інтереси та безпеку.

Французька стратегія кібербезпеки спрямована на досягнення п'яти основних цілей, які мають на меті створення «цифрової республіки», забезпечуючи при цьому як безпеку, так і стійкість інформаційно-комунікаційних технологій (ІКТ). До цих стратегічних пріоритетів належать:

1) Захист ключових національних інтересів у кіберпросторі, що включає охорону державних інформаційних систем та критично важливих елементів інфраструктури.

2) Забезпечення довіри між учасниками цифрового простору, а також захист конфіденційності та персональних даних користувачів. Це досягається через розробку спеціалізованих кіберзахисних продуктів і надання технічної та юридичної підтримки.

3) Підвищення рівня обізнаності про кібербезпеку та розвиток відповідних можливостей на національному рівні. Це включає в себе освітні ініціативи та підготовку фахівців у цій сфері.

4) Створення сприятливих умов для розвитку підприємництва, залучення інвестицій в ІКТ-сектор та підтримку інноваційного бізнесу, що стимулює економічне зростання в цифровій сфері.

5) Розробка стратегії або «дорожньої карти» для досягнення європейської цифрової автономії, що сприяє зниженню залежності від зовнішніх технологій і зміцненню власного потенціалу у сфері кібербезпеки [11].

Ці пріоритети відображають амбіції Франції у створенні безпечної та інноваційної цифрової інфраструктури, здатної захищати національні інтереси в умовах зростання глобальних кіберзагроз.

У листопаді 2016 року Національна Асамблея Франції ухвалила закон, який має на меті зміцнення незалежності, свободи та плюралізму засобів масової інформації (Loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias). Цей закон зобов'язує медіаорганізації впровадити кодекс етики, який регулює їхню діяльність, а також створити спеціальний комітет з етичних питань. Завданням цього комітету є допомога у вирішенні внутрішніх конфліктів, що можуть виникати всередині редакцій, а також у суперечках між власниками медіа та журналістськими колективами. Такий підхід спрямований на забезпечення більшої прозорості та підвищення довіри до засобів масової інформації, що є важливим аспектом підтримки свободи слова та забезпечення плюралізму думок у суспільстві [8].

У травні 2020 року парламент Франції ухвалив новий закон, який зобов'язує онлайн-платформи видаляти контент, що пропагує педофілію або тероризм, протягом однієї години з моменту його виявлення. Якщо платформи не виконають цю вимогу, їм загрожують штрафні санкції у розмірі до 4% від загального обсягу їхнього доходу. Закон також регулює видалення інших видів «шкідливого» контенту, встановлюючи термін у 24 години для їхнього усунення. Крім цього, впроваджується нова посада – цифровий прокурор, а також створюється спеціальний урядовий орган, який буде відповідати за нагляд і забезпечення дотримання закону, гарантуючи своєчасне видалення незаконного контенту з платформ [2].

У жовтні 2020 року депутати від партії «Вперед, республіка!» внесли на розгляд законопроєкт «Про глобальну безпеку», який охоплював широкий спектр питань, що стосуються діяльності правоохоронних органів. Однак найбільший резонанс у суспільстві викликала стаття 24 цього законопроєкту. Вона передбачала покарання за публікацію фотографій, відеозаписів або будь-яких інших матеріалів, які дозволяють ідентифікувати співробітників поліції або жандармерії. Якщо такі матеріали були поширені з метою завдання фізичної або психологічної шкоди правоохоронцям, правопорушник міг отримати покарання у вигляді одного року ув’язнення або штрафу [4]. Однак через масові акції протесту, під час яких громадськість висловила занепокоєння щодо можливого порушення свободи слова, французький парламент вирішив відкликати цю статтю. Протестувальники вважали, що це

положення могло суттєво обмежити їхнє право на вільне висловлювання та контроль за діями правоохоронців.

Закон LOPMI, ухвалений у січні 2023 року, позиціонував Францію серед лідерів країн, які займають жорсткішу позицію щодо вебсайтів, що використовуються для здійснення злочинної діяльності [9]. Хоча цей закон є новаторським кроком у боротьбі з кіберзлочинністю, його практичне застосування залишається на ранніх стадіях. Через новизну закону прокурорам поки що не вдалося отримати жодних вироків за його використання, але очікується, що найближчим часом він стане ефективним інструментом у протидії незаконній діяльності в мережі.

Також слід наголосити, що у Франції створено низку державних і неурядових інституцій, які займаються питаннями запобігання кіберзлочинності. Однією з найвідоміших серед них є Національна комісія з обчислювальної техніки та свобод (CNIL). Основна мета діяльності CNIL полягає в захисті персональних даних громадян. У сучасному цифровому світі CNIL виконує функцію регулятора у сфері захисту персональних даних, надає підтримку фахівцям у галузі кібербезпеки, а також допомагає громадянам контролювати свої особисті дані та реалізовувати свої права. Починаючи з 2004 року, CNIL отримала право накладати санкції на компанії, які порушують Закон про інформатику, картотеки та свободи, ухвалений у 1978 році [6].

Окрему роль у боротьбі з кіберзлочинністю у Франції відіграє Верховний орган з питань поширення творів та захисту прав в Інтернеті (HADOPI). Ця структура займається регулюванням діяльності, пов’язаної з нелегальним завантаженням інформації, зокрема визначає поняття незаконного скачування та розробляє нормативні акти для протидії такій діяльності. Одним із ключових кроків стало ухвалення Закону про триступеневу заборону доступу до Інтернету, який пройшов схвалення у Вищому конституційному суді Франції у другій редакції. Закон передбачає поступове обмеження доступу до мережі для тих користувачів, які неодноразово порушують авторські права шляхом нелегального завантаження захищеного контенту [6].

У системі правоохоронних органів Франції також діють спеціалізовані підрозділи, спрямовані на боротьбу зі злочинами в сфері інформаційних технологій. Починаючи з 1998 року, Національна жандармерія визначила вирішення проблем, пов'язаних з інноваційними технологіями, як один зі своїх пріоритетів. З цією метою були створені спеціалізовані структури та навчальні заклади. Серед них можна виділити:

1. Відділ кіберзлочинів технічного обслуговування судових досліджень та документації (STRJD), який займається моніторингом Інтернет-мереж з метою виявлення злочинів, пов'язаних із нелегальним обігом даних. Цей підрозділ здійснює перевірку сайтів, Інтернет-ресурсів, груп новин, мереж обміну файлами та соціальних мереж на наявність порушень, таких як злочини проти людей і майна.

2. Комп'ютерний і електронний відділ Інституту кримінального розслідування Національної жандармерії (IRCGN), який розробляє новітні методи та програмне забезпечення для автоматизованого виявлення педофілів та інших кіберзлочинців.

3. Відомчі бригади інформації та судових розслідувань (BDRIJ), що також займаються питаннями боротьби з кіберзлочинністю на рівні департаментів, зокрема розслідуванням порушень у сфері інформаційних технологій.

Ці підрозділи відіграють ключову роль у забезпеченні кібербезпеки та протидії злочинам, що здійснюються через Інтернет.

Одним із ключових суб'єктів боротьби з кіберзлочинністю у Франції є Національне агентство безпеки інформаційних систем (ANSSI), яке відповідає за кібербезпеку країни та тісно співпрацює з державними спецслужбами. Діяльність ANSSI спрямована на впровадження Французької національної стратегії цифрової безпеки, яка була оголошена 16 жовтня 2015 року. Ця стратегія є результатом скоординованих зусиль різних урядових структур і націлена на вирішення проблем, що виникають у цифрову епоху. Водночас наголошено, що цифрова трансформація сприяє не лише інноваціям та економічному

розвитку, але й приносить нові загрози для держави, бізнесу та громадян. Серед цих загроз: кіберзлочинність, шпигунство, пропаганда, саботаж та зловживання персональними даними, що підриває довіру та безпеку в цифровій сфері

ANSSI визначила кілька ключових напрямків у своїй діяльності: забезпечення захисту державних інформаційних систем та критично важливої інфраструктури, підтримка безпеки для важливих економічних і соціальних операторів, а також забезпечення цифрової довіри, конфіденційності та захисту персональних даних. Окрім цього, агентство приділяє велику увагу підвищенню обізнаності суспільства, навчанню та розвитку кібернавичок, як на початкових етапах, так і в рамках безперервної освіти. Також серед пріоритетів ANSSI – підтримка бізнес-середовища у сфері цифрових технологій, розробка промислової політики, стимулювання експорту та глобалізації [1, с. 158]. Важливим елементом залишається забезпечення цифрової стратегічної автономії Франції та підвищення стійкості її кіберпростору.

На основі аналізу досвіду Франції у сфері кібербезпеки можна зробити кілька важливих висновків. По-перше, кібербезпека у Франції є невід'ємною складовою національної безпеки, що підтверджується значною кількістю стратегій, законів та нормативних актів, спрямованих на захист критичної інфраструктури, державних і приватних інформаційних систем. Франція активно розвиває як національні, так і міжнародні механізми захисту від кіберзагроз, співпрацюючи з іншими державами в рамках НАТО та Європейського Союзу. Важливою частиною стратегії є захист персональних даних, розвиток інформаційної грамотності та регулювання цифрового простору для запобігання дезінформації та пропаганди.

Серед перспектив подальших досліджень можна виділити кілька напрямків. Перш за все, необхідно глибше дослідити ефективність впроваджених законів та стратегій, зокрема таких, як LOPMI 2023 року, щодо боротьби з кіберзлочинністю. Важливим є також вивчення питання взаємодії державних інституцій із приватним сектором у сфері кібербезпеки, оскільки ці відносини можуть сприяти створенню більш ефективної та стійкої цифрової інфраструктури. Крім того, особливу увагу слід приділити питанням міжнародної співпраці та обміну досвідом у протидії глобальним кіберзагрозам, що стають дедалі складнішими.

Список використаних джерел:

1. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб’єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького*. *Серія : Право*. 2018. № 6. С. 154-163.
2. France to force web giants to delete some content within the hour. *REUTERS*. 2020. URL: https://www.reuters.com/article/us-france-tech-regulation/france-to-force-web-giants-to-delete-some-content-within-the-hour-idUSKBN22P2JU. (дата звернення: 20.09.2024).
3. Livre blanc sur la défense et la sécurité nationale. 2013. URL: http://www.livreblanc defenseetsecurite.gouv.fr/index.html (дата звернення: 20.09.2024).
4. Loi «Sécurité globale» : la majorité va proposer «une nouvelle écriture complète de l'article 24». 2020. URL: https://www.lefigaro.fr/politique/loi-securite-globalela-majorite-va-proposer-une-nouvelle-ecriture-complete-de-l-article-24-20201130. (дата звернення: 20.09.2024).
5. Loi du 29 juillet 1881 sur la liberté de la presse. URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722. (дата звернення: 20.09.2024).
6. Loi favorisant la diffusion et la protection de la création sur Internet URL : http://www.senat.fr/dossier-legislatif/pjl07-405.html (дата звернення: 20.09.2024).
7. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique . URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte= JORFTEXT000000801164 (дата звернення: 20.09.2024).

8. LOI n° 2016-1524 du 14 novembre 2016 visant à renforcer la liberté, l'indépendance et le pluralisme des médias. URL: https://www.legifrance.gouv.fr/eli/loi/2016/11/14/MCCX1603797L/jo (дата звернення: 20.09.2024).
9. LOI n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768 (дата звернення: 20.09.2024).
10. Revue stratégique 2017 . URL: https://www.defense.gouv.fr/dgris/politique-de-defense/revue-strategique/revue-strategique. (дата звернення: 20.09.2024).
11. Stratégie nationale pour la sécurité du numérique. URL: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf. (дата звернення: 20.09.2024).

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).

Маріанна МАРУСИНЕЦЬ
кандидат філологічних наук, доцент,
доцент кафедри історії та суспільних дисциплін,
старший науковий співробітник, старший дослідник
Науково-дослідного центру імені Тіводора Легоцькі
Закарпатського угорського інституту імені Ференца Ракоці II

ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ НАЦІОНАЛЬНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК: ДОСВІД ІРЛАНДІЇ

Анотація: *аналізується захист критичної національної інфраструктури Ірландії від кібератак, яка охоплює енергетичний і транспортний сектори, сектор фінансових послуг, охорону здоров'я і саму телекомунікаційну систему. Актуалізовано, що досвід Національного центру кібербезпеки Ірландії упродовж останніх десятиліть розробляє та використовує інструменти для компрометації і навіть знищення кібератак, які починаються від витоку даних і можуть закінчуватися руйнуванням фізичної інфраструктури. Оскільки такі загрози походять від широкого кола суб'єктів, що різняться за рівнем доступу до ресурсів і можливостей. Підсумовано, що уряд Ірландії має за мету захистити критично важливі національні інфраструктури від атак, вимагаючи від операторів вжити заходів для управління ризиками для цієї інфраструктури використовуючи мережеву та інформаційну безпеку. В умовах війни досвід Ірландії може бути імплементованим для України.*

Ключові слова: *Ірландія, Північна Ірландія, ЄС, об'єкти критичної національної інфраструктури, кібератаки, кібербезпека.*

Ірландія сьогодні посідає 7-е місце з 28 країн-членів ЄС у рейтингу Європейської комісії щодо впровадження та використання цифрових технологій. Національний центр кібербезпеки розробляє стратегію для розвитку індустрії кібербезпеки Міністерства навколишнього середовища, клімату та комунікацій Ірландії[7]. Хоча розвиток подій у кіберпросторі створює загальні ризики для суспільства, існують окремі сектори, для яких ці інциденти потенційно мають набагато більші наслідки. У широкому сенсі, це ті сектори інфраструктури, що є критично важливими для суспільних та економічних функцій, які часто називають критичною національною інфраструктурою (КНІ), а також системи та дані державного сектору. Традиційна концептуалізація критичної національної інфраструктури охоплює енергетичний і транспортний сектори, сектор фінансових послуг, охорону здоров'я і саму телекомунікаційну систему. Урядові ІТ-системи, в свою чергу, відіграють центральну роль у виконанні багатьох функцій, необхідних для функціонування сучасного суспільства, включаючи соціальні послуги та платіжні системи, збір податків для функціонування демократії. Упродовж останніх десятиліть населення Ірландії стало свідками розроблення і використання інструментів для компрометації і навіть знищення цих систем. Оскільки такі загрози походять від широкого кола суб'єктів, що різняться за рівнем доступу до ресурсів і можливостей. Вони варіюються від окремих осіб, що діють поодинці або в невеликих групах, які займаються атаками типу «набридливий», або пошкодження веб-сайтів і на відмову в обслуговуванні, до «хактивістів», злочинців різного масштабу й національних держав. Серед ризиків вищого рівня організовані злочинні угруповання, які використовують передові технології для зараження і компрометації мереж і даних. На вершині цієї піраміди знаходяться державні структури: військові або охоронні організації, які прагнуть використовувати мережеві та інформаційні системи для проведення операцій, починаючи від витоку даних і закінчуючи руйнуванням фізичної інфраструктури.

Ці суб'єкти загроз, яких зазвичай називають «сучасними постійними загрозами» (СПЗ), причетні до атак у широкому спектрі секторів, але з особливим акцентом на державні ІТ-системи, телекомунікаційні мережі, фінансові послуги та технологічні компанії.

Ресурси, які вони мають у своєму розпорядженні – наполегливість і досвід – означають, що ці суб'єкти становлять особливий виклик, їх важко виявити і важко усунути, а отже, становлять виклик безпеці мережевих та інформаційних систем.

В Ірландії з 2018 року діє Закон про мережеву та інформаційну безпеку, що призвело до більш проактивного підходу до захисту критично важливої національної інфраструктури, включаючи офіційну ідентифікацію операторів і початок реалізації програми заходів безпеки, які включають оцінку і аудит дотримання вимог, відповідно до заходів, що вживаються в усій Європі[4]. Однак ризики залишаються як у секторах, охоплених Регламентом Мережева та інформаційна безпека, так і за його межами. По-перше, дотримання заходів безпеки, передбачених Регламентом Мережева та інформаційна безпека, є методологією зменшення ризиків, а не гарантією абсолютної безпеки. По-друге, Директива та Регламент Мережева та інформаційна безпека чітко обмежені сімома визначеними секторами. Як оцінка критичної національної інфраструктури, проведена Національним центром кібербезпеки під час процесу визначення, так і застосування заходів безпеки після визначення, показали, що частина інфраструктури в державі, яка не підпадає під дію Регламенту Мережева та інформаційна безпека, насправді також є критично важливою, і що існує низка взаємозалежностей між секторами критичної національної інфраструктури, які, ймовірно, можуть призвести до виникнення певних ризиків [1]. Хоча безпека ІКТ у державному секторі стала об'єктом значних інвестицій і уваги, не в останню чергу завдяки появі Загального регламенту захисту даних, природа цього сектору створює певні специфічні виклики. Деякі департаменти і відомства можуть легко продемонструвати відповідність найкращим міжнародним практикам (і міжнародним стандартам, таким як ISO27001) [6], натомість залишаються проблеми із забезпеченням стабільно високого рівня безпеки в урядових департаментах і відомствах.

Особливо це стосується формального управління безпекою інформаційно-комунікаційних технологій, як в цілому, так і в контексті національної секретної інформації та секретної інформації інших держав і міжнародних організацій.

Типові проблеми мають місце і з отриманням Атестату безпеки об'єктів для компаній, що займаються обробкою та зберіганням конфіденційної інформації. Розробляються певні заходи для вирішення цих питань, включаючи використання спільної IT-інфраструктури між відомствами. Однак, окремі фундаментальні виклики залишаються ще не зреалізованими. Для прикладу, технологічний розвиток, який триває в телекомунікаціях, може ускладнити цю ситуацію, через низьку затримку і високу пропускну здатність передачі інформації, розгортання технологій 5G, що слугуватиме ключовою інфраструктурою для низки інших технологій і сценаріїв використання.

До потенційно нових належать послуги, орієнтовані на споживача, такі, як: автономні транспортні засоби, послуги електронної охорони здоров'я та розваги, а також послуги, орієнтовані на промисловість. Відтак мережі 5G стануть ключовими для нового набору послуг, критично важливих для функціонування життєво, суспільних і економічних функцій. Характер цих мереж і технологій також відіграють певну роль : програмну-визначеність і віртуалізацію, що в цьому секторі, ймовірно, знадобляться нові види заходів для забезпечення безпеки як мережі 5G, так і послуг, що залежать від неї [6].

До недавна європейська практика із захисту критичної національної інфраструктури та послуг від кібератак включала два типи дій. Це: створення національної служби реагування на інциденти, як: Національний центр кібербезпеки та запровадження офіційних механізмів обміну інформацією, за допомогою яких власники та оператори можуть ділитися досвідом щодо виникнення загроз. Національний центр також співпрацює з операторами комунальних послуг та аналогічними структурами в інших юрисдикціях з метою управління ризиками для критично важливої національної інфраструктури в Ірландії, включаючи активне управління поточними інцидентами[1]. Однак досвід Європейських країн показав, що існує асиметрія ризиків між суспільними інтересами та інтересами операторів відповідного типу інфраструктури. У багатьох випадках критичні послуги залишаються вразливими, незважаючи на спроби уряду надати операторам інформацію та підтримку. Беручи до уваги

досвід роботи країн-членів ЄС та директиви в галузі телекомунікацій, Європейська комісія в 2013 році опублікувала проєкт «Директиви про мережеву та інформаційну безпеку». Офіційно проєкт був зреалізований у 2016 році і передбачав низку заходів, спрямованих на підвищення стійкості критично важливої національної інфраструктури у 7 секторах: енергетика, транспорт, питна вода, банківські справи, фінансовий ринок, охорона здоров'я та цифрова інфраструктура. Ці заходи включають вимогу до держав-членів ЄС офіційно оцінювати свою інфраструктуру і юридично призначати так званих «операторів основних послуг» – які є критично важливими у кожній державі. Суб'єкти повинні відповідати формальним та вимогам щодо звітування про інциденти [5].

Відтак метою Директиви про мережеву та інформаційну безпеку є:

1) покращення безпеки і стійкісті критичної національної інфраструктури, 2) підвищення обізнаності держав про інциденти кібербезпеки в країнах Європейського Союзу

3) забезпечення узгодженого та кординаційного реагування на рівні ЄС. Одже, Мета уряду Ірландії – захист критично важливої національної інфраструктуру від атак, вимагаючи від операторів вжити заходів для управління ризиками для цієї інфраструктури, в тому числі шляхом створення відповідних планів реагування на інциденти, щоб впоратися з будь-якими загрозами в наданні послуг[2].

Результати оцінки збитків економіки України, понесених внаслідок воєнної агресії росії. В умовах війни досвід Ірландії може бути імплементованим для України.

З початку бойових дій в Україні були пошкоджені 19 аеропортів і цивільних аеродромів; щонайменше 126 залізничних вокзалів і станцій.

За попередніми оцінками, загальний обсяг прямих збитків об’єктів транспортної інфраструктури в Україні склав $36,8 млрд. Станом на 13 червня 2024 року загальна сума прямих задокументованих збитків житлової та нежитлової нерухомості, іншій інфраструктур складали понад $95.5 млрд. Найбільш постраждалими є області України, в яких донині ведуться бойові дії. Це Донецька (25% всіх пошкоджень та руйнувань у грошовому вираженні), Харківська (18% всіх пошкоджень та руйнувань), Луганська (понад 13% всіх пошкоджень та руйнувань), Миколаївська (9%), Запорізька (7%), Київська (7%) та Чернігівська (6%) області [8].

Укладена рамкова домовленість між Державним секретарем з питань оборони Сполученого Королівства Великої Британії і Північної Ірландії та Міністерством з питань стратегічних галузей промисловості України та Міністерством оборони України щодо співробітництва у сфері оборонних матеріалів [9]. Домовленість було укладено під час Конференції британсько-українського оборонного співробітництва, що проходила 8-9 квітня 2024 р. у Києві. У ній взяли участь представники 29 британських та 67 українських оборонних компаній, між ними відбулось 350 зустрічей. Також були присутні члени урядів обох країн. Загалом захід зібрав 350 учасників.

«Велика Британія буде підтримувати Україну стільки, скільки буде необхідно. Тому ми продовжуємо нарощувати нашу підтримку. Ця домовленість та контракти, які в Києві підписали приватні компанії, сприятиме оборонним зусиллям України та довгостроковому відновленню», — сказав міністр з питань торговельної політики Великої Британії Ґреґ Гендс [10].

Список використаних джерел:

1. 'Critical' Irish security strategy still awaited four years on. Irish Examiner. URL: https://www.irishexaminer.com/news/arid-41326741.html
2. Government of Ireland 2022 National Energy Security Framework. Department of the Environment, Climate and Communications. Available at:https://www.gov.ie/en/publication/ea9e4-national-energy-security-framework/
3. Factsheet on the Irish Parliament. Houses of the Oireachtas website. URL: https://www.oireachtas.ie/en/press-centre/factsheet/

4. Keatinge P. The “Specific character” of Ireland’s security and defence policy reflections on neutrality. URL: https://historyiiea.com/wpcontent/uploads/2019/05/The-Specific-Character-of-Ireland’s-Security-and-DefencePolicy-Reflections-on-Neutrality.p
5. Memorandum of Understanding between the Ministry of Defence of the United Kingdom of Great Britain and Northern Ireland and the Department of Defence Ireland.URL:http://opac.oireachtas.ie/AWData/Library3/DEFMemorandum_of_Understanding_between_the_UK_and_Ireland_on_the_enhancement_of_bilateral_engagement_on_certain_aspects_of_defence_and_security_cooperation19012015_174233.pdf
6. National Cyber Security Strategy 2019-2024
URL:file:///C:/Users/user/Desktop/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF.%201516%20%D0%B6%D0%BE%D0%B2%D1%82%D0%BD%D1%8F%202024%20%D1%80/National_Cyber_Security_Strategy.pdf
7. https://www.ncsc.gov.ie/
8. https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/audit-of-war-damage.pdf
9. https://zakon.rada.gov.ua/laws/show/826_001-24#Text
10. https://mspu.gov.ua/news/mizh-minstratehpromom-minoborony-ta-uriadom-velykoi-brytanii-bulo-pidpysano-domovlenist-pro-spivpratsiu-u-sferi-oboronnykh-tekhnolohii

MOLNÁR D. Erzsébet
PhD, docens,
Történelem- és Társadalomtudományi Tanszék,
Lehoczky Tivadar Társadalomtudományi Kutatóközpont vezetője,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
ZSUKOVSZKY Ágnes
II. évfolyamos
nemzetközi kapcsolatok, társadalmi kommunikáció
és regionális tanulmányok szakos hallgató,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

DIGITÁLIS HATÁROK: DÉL-KOREA ÉS MAGYARORSZÁG KIBERBIZTONSÁGI STRATÉGIÁINAK ÖSSZEHASONLÍTÁSA

Kulcsszavak: *Koreai Köztársaság, kiberbiztonság, Magyarország, EU, infrastruktúra*

A Koreai Köztársaságban a kiberbiztonság nagy utat tett meg az elmúlt évtizedekben. Az ország élen jár a technológiai innováció és a digitális infrastruktúra gyors fejlődése terén. Technológiailag fejlett országként Dél-Korea különösen érzékeny a kiberfenyegetésekre és a kiberbiztonsági kihívásokra, amelyek nemcsak a gazdasági és politikai stabilitást, hanem a nemzetbiztonságot is érintik.

Dél-Korea digitális infrastruktúrája az egyik legfejlettebb a világon, beleértve az ország kiterjedt internet-hozzáférését és technológiai vívmányait. A gyorsan fejlődő digitális gazdaság és a technológiai szektorban betöltött kiemelkedő szerepe mellett azonban az ország egyre több kiberfenyegetéssel is szembesül. Az ország, ahol lakosságának több mint 95%-a internetezik, élen jár az 5G-hálózatok bevezetésében is. Az ország legnagyobb technológiai vállalatai, mint például a Samsung és az LG, globális vállalkozások. Ez a magas szintű technológiai fejlettség azonban az ország kiszolgáltatottságát is növeli. A dél-koreai vállalatokat és kormányzati szerveket gyakran érik olyan támadások, mint például az adatlopás, a zsarolóvírusok és a szolgáltatásmegtagadási támadások [6].

Dél-Korea kiberbiztonsági helyzete szoros kapcsolatban áll az ország geopolitikai helyzetével és technológiai fejlettségével. Az ország különösen érzékeny a kiberháborúkra, kiberkémkedésre és más digitális fenyegetésekre, amelyek főként Észak-Koreából erednek. Észak-Korea aktívan alkalmaz kiberfenyegetést a politikai és gazdasági destabilizáció céljából. Az ország ismert olyan támadásokról, mint a 2014-es Sony Pictures elleni kibertámadás, amelyet a Koreai Népi Demokratikus Köztársaság (Észak-Korea) nevéhez kapcsolnak. Továbbá, Dél-Korea vállalatai és kormányzati intézményei is célpontjai lehetnek különféle kiberbűnözői csoportoknak, amelyek pénzügyi haszonszerzés céljából folytatnak támadásokat [5].

Dél-Korea kormányzati szinten is felismerte a kiberbiztonság fontosságát, és ennek megfelelően számos intézkedést hozott az ország védelme érdekében. A Koreai Köztársaság kiberbiztonsági stratégiája a kiberfenyegetések kezelésére és a digitális infrastruktúra védelmére összpontosít. Az ország kormánya 2009-ben létrehozta a Kiberbiztonsági és Információvédelmi Ügynökséget (KISA), amely a kiberbiztonsági politika kidolgozásáért és végrehajtásáért felelős. A KISA feladatai közé tartozik a kiberfenyegetések figyelése, az incidensek kezelése, elhárítása, valamint a nemzeti szintű kiberbiztonsági tudatosság növelése [2]. A KISA emellett együttműködik a nemzetközi partnerekkel, hogy elősegítse a globális kiberbiztonsági stratégiák fejlesztését és a közös fenyegetések elleni védekezést.

A kritikus infrastruktúrák védelme kulcsfontosságú része a dél-koreai kiberbiztonsági politikának. Az ország számos intézkedést hozott annak érdekében, hogy biztosítsa az energiaellátást, a

közlekedési rendszereket és a telekommunikációs hálózatokat a kiberfenyegetésekkel szemben. A kritikus infrastruktúrák védelmét célzó programok, mint például a Kiberbiztonsági Kockázatkezelési Rendszer (CRMS), célja a kiberkockázatok időben való azonosítása és kezelése, valamint a biztonsági intézkedések folyamatos újítása. Ezenkívül a Dél-Korea Kormánya által létrehozott Kiberbiztonsági Akadémia és Kutatóintézetek is hozzájárulnak a kritikus infrastruktúrák védelméhez, és szakértői tudást biztosítanak a legújabb kiberfenyegetések elleni védekezéshez.

A kiberbiztonság nemcsak a technikai megoldásokról szól, hanem a megfelelő képzésről és tudatosságról is. Dél-Koreában nagy hangsúlyt fektetnek a kiberbiztonsági képzésre, melynek célja a szakemberek és a széles közönség felkészítése a kiberfenyegetésekre. Az ország számos programot indított, amelyek célja a kiberbiztonsági ismeretek bővítése és a kiberbiztonsági kultúra erősítése. A koreai egyetemek és felsőoktatási intézmények számos kiberbiztonsági képzést kínálnak, amelyek felkészítik a hallgatókat a kiberfenyegetések kezelésére és a legújabb technológiai fejlesztések alkalmazására.

A Dél-Koreai Kiberbiztonsági Akadémia (KISA Cyber Security Academy) a kiberbiztonsági szakemberek képzésére és továbbképzésére összpontosít, biztosítva ezzel, hogy az ország rendelkezzen a legmagasabb szintű szakmai tudással és tapasztalattal. Ezenkívül a vállalatok is aktívan részt vesznek a kiberbiztonsági tudatosság növelésében, rendszeresen tartanak képzéseket alkalmazottaik számára, hogy azok tisztában legyenek a legújabb kiberfenyegetésekkel és a védekezés módjaival [2].

A dél-koreai kiberbiztonsági politika nemcsak a technológiai megoldásokra összpontosít, hanem a nemzetközi együttműködésre is. Dél-Korea aktívan részt vesz a globális kiberbiztonsági kezdeményezésekben és együttműködési platformokon, például az Egyesült Nemzetek Szervezetének (ENSZ) kiberbiztonsági fórumain és a Nemzetközi Telekommunkációs Unió (ITU) munkacsoportjaiban. Ezek az együttműködések lehetővé teszik az ország számára, hogy tapasztalatokat cseréljen más országokkal, és közösen dolgozzon ki megoldásokat a globális kiberfenyegetések kezelésére [4].

A kiberbiztonsági politikák mellett a kormány fokozott figyelmet fordít a kutatásfejlesztésre is. A Dél-Koreai Kiberbiztonsági Központ (KIC) és más kutatóintézetek rendszeresen végeznek kutatásokat a legújabb kiberfenyegetések és védelmi technológiák terén [2]. Ezek a kutatások hozzájárulnak ahhoz, hogy az ország mindig naprakész legyen a legújabb kiberfenyegetések elleni védekezésben és a legfejlettebb védelmi megoldások alkalmazásában.

Dél-Korea kiberbiztonsága, mint azt már fentebb említettem, az egyik legfejlettebb a világon, ám a jövő számos kihívást és kilátást tartogat az ország számára. Az egyre összetettebb kiberfenyegetések, mint például az államilag támogatott hackerek, a kritikus infrastruktúrák elleni támadások, valamint az IoT-eszközök sebezhetősége új típusú biztonsági kihívásokat jelentenek. Különösen Észak-Korea kiberhadviselési tevékenységei miatt a dél-koreai védelmi stratégia állandó fejlesztést igényel.

A jövő egyik nagy lehetősége az 5G-hálózatok és a mesterséges intelligencia széles körű alkalmazása, amelyek megerősíthetik a kiberbiztonsági rendszereket. Ugyanakkor ezek az új technológiák új támadási felületeket is jelentenek, így szükséges az állandó felkészülés és az innovatív megoldások kidolgozása. Az adatvédelem és a személyes információk védelme szintén kiemelt prioritást kap a jövőben, mivel a digitalizációval egyre több adat kerül a kiberbűnözők célkeresztjébe.

Dél-Koreának ezért folytatnia kell a nemzetközi együttműködést a kiberbiztonság terén, különösen az Egyesült Államokkal és más szövetségesekkel, hogy hatékonyabban tudjon fellépni a

globális fenyegetésekkel szemben[3]. Emellett a helyi szakértők képzése és a biztonságtudatosság növelése is kulcsszerepet játszik a fenntartható fejlődésben.

Magyarország kiberbiztonsági helyzete más kihívásokkal néz szembe, mint Dél-Korea. Bár Magyarország digitális fejlettsége nem éri el a dél-koreai szintet, ott is komoly figyelmet fordítanak a kiberbiztonságra, különösen az EU-s szabályozásoknak és az uniós tagállamokkal való együttműködésnek köszönhetően. Magyarország internetpenetrációja az elmúlt években folyamatosan növekedett, és jelenleg a lakosság több mint 80%-a használ internetet [6]. Az ország infrastruktúráját és informatikai rendszereit azonban folyamatosan támadások érik, különösen a pénzügyi és kormányzati szektorokban. Magyarország gyakran válik célpontjává nemzetközi kibertámadásoknak, köztük zsarolóvírusoknak és kémkedési próbálkozásoknak.

Magyarország kiberbiztonsági stratégiáját elsősorban az EU-s jogszabályok és irányelvek határozzák meg. Az országban 2013-ban létrehozták a Nemzeti Kibervédelmi Intézetet, amelynek feladata a kiberbiztonsági incidensek kezelése és megelőzése. Magyarország az EU-n belül is aktívan részt vesz a kiberbiztonsági együttműködésekben, például az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) keretében [1].

A Dél-Korea és Magyarország kiberbiztonságának összehasonlítása rávilágít mindkét ország eltérő fejlődési útjára és prioritásaira ezen a területen. Dél-Korea kiemelkedő technológiai infrastruktúrával és erős kiberbiztonsági stratégiákkal rendelkezik, mivel az ország erősen digitalizált, és nagy hangsúlyt fektet a nemzetbiztonságra, a gazdasági növekedésre és a kibertámadásokkal szembeni védelemre. Magyarország ugyanakkor az EU irányelvekhez igazodva fejleszti kiberbiztonsági kapacitásait, ám infrastrukturális és technológiai téren elmarad Dél-Koreától. Magyarország kiberbiztonsági stratégiája inkább a nemzeti szabályozások és európai együttműködés keretein belül mozog [3].

Összességében azt láthatjuk, hogy Dél-Korea kiberbiztonsági intézkedései majdnem a legfejlettebbek, míg Magyarország még fejlődési szakaszban van, azonban folyamatosan igyekszik erősíteni védelmét a nemzetközi és európai irányelvekhez igazodva.

Felhasznált források:

1. Korean Internet & Security Agency (KISA) (https://www.kisa.or.kr/eng/main/main.jsp) (Letöltés ideje: 2024.10.22.)
2. Korean Cyber Security Strategy (https://www.mpss.go.kr/eng/main.do) (Letöltés ideje: 2024.10.22.)
3. Nemzeti Kibervédelmi Intézet – Magyarország (https://nki.gov.hu) (Letöltés ideje: 2024.10.20.)
4. OECD Cybersecurity Report (https://www.oecd.org/sti/ieconomy/cybersecurity.htm) (Letöltés ideje: 2024.10.22)
5. South Korea's National Cybersecurity Policy (https://www.mofa.go.kr/eng/wpge/m_21991/contents.do) (Letöltés ideje: 2024.10.23.)
6. https://eucpn.org/sites/default/files/document/files/HU%20cybercrime.pdf (Letöltés ideje: 2024.10.24.)

CSATÁRY György
docens, PhD, tanszékvezető,
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
VASS Jázmin
II. évfolyamos
nemzetközi kapcsolatok, társadalmi kommunikáció
és regionális tanulmányok szakos hallgató,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

KIBERBIZTONSÁGI STRATÉGIÁK AZ EGYESÜLT ÁLLAMOKBAN

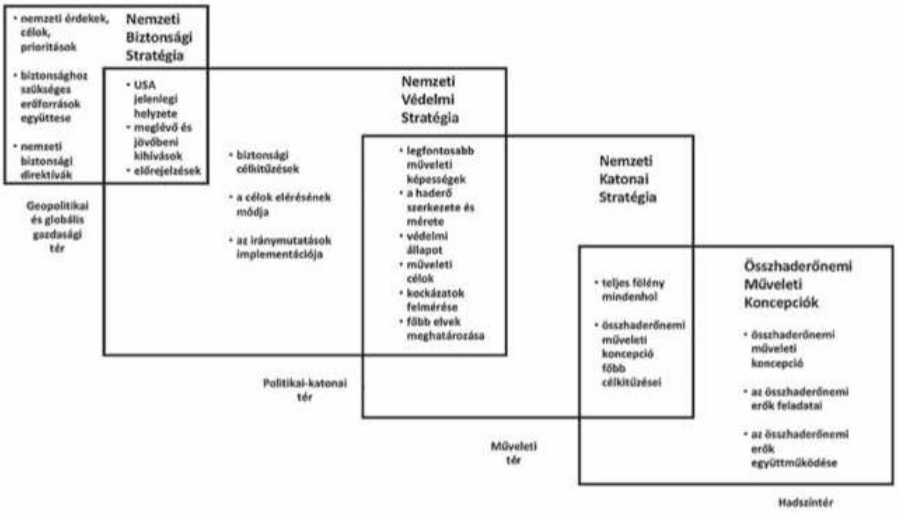
Kulcsszavak: *kiberbiztonság, USA, szabályok, stratégia, nemzetvédelem*

A mai fejlődő világban a média behálóz mindent és mindenkit. El sem tudnánk képzelni a napunkat egy hír elolvasása vagy egy videó megtekintése nélkül. Mindig próbáljuk minden erőnkkel megvédeni az adatainkat az interneten, mindig beszélünk a kibertámadásokról, de vajon mikor tudjuk valóban biztonságban érezni magunkat a fenyegetésektől?

A kiberbiztonság az informatikai rendszerek, adatbázisok és hálózatok védelmét jelenti a támadásokkal szemben. Célja a rendszerek titkosságának megőrzése és védelme. A kiberbiztonság foglalja magába az olyan intézkedéseket, mint a tűzfalak, antivírus programok és a felhasználói tudatosság növelése is.

Amikor az Egyesült Államokról beszélünk, akkor egy nagyon fejlett gazdaságot látunk, nagyon modern technikákkal és intézkedésekkel. A világ vezető hatalmaként meghatározó szerepet tölt be számos kiberteret érintő kérdésben. Már közel három évtizede az ország gazdasága nagyban támaszkodik a kibertérre, amely meghatározza a kiberbiztonság fontosságát és tevékenységeit az országban.

Azonban, ahhoz hogy megértsük a biztonsági intézkedéseket az Egyesült Államokban, ismernünk kell kiberbiztonsági rendszerét is, amely elég összetett az országban. A nemzeti védelmi stratégia megjelenik a nemzeti biztonsági stratégiák mellett.



Az USA legfontosabb stratégiai dokumentumainak rendszere

Az USA nemzeti biztonsági stratégiája

Az Egyesült Államok legújabb nemzeti biztonsági stratégiáját 2017 decemberében adták ki Donald J. Trump elnök aláírásával [3]. A dokumentum négy fő fejezetben, úgynevezett pillérekben mutatja be mindazon stratégiai célokat, amelyek az amerikai érdekek és értékek védelme érdekében regionálisan vagy akár globálisan szükségesek. A kibertér védelme rögtön az első pillérben, azaz *Az amerikai emberek, a szülőföld és az amerikai életmód (Pillar I.: Protectthe American People,*

theHomeland, az the American Way of Life) című részben jelenik meg. Ez a fejezet gyakorlatilag a veszélyforrásokat veszi számba, amelyek közvetlenül vagy közvetett módon veszélyeztetik az amerikai embereket és életüket. A dokumentum kiemeli a kiberkorszak kihívásaira adandó válaszok és a másik oldalról az abban rejlő lehetőségek kihasználásának fontosságát: „Amerika reakciója a számítógépes kor kihívásaira és lehetőségeire meg fogja határozni a jövőbeli jólétünket és biztonságunkat" [3].

A kibertérrel kapcsolatban a dokumentum leszögezi, hogy akár állami, akár nem állami szereplők rosszindulatú kibertámasásokat képesek végrehajtani a világon bárhol, bárhonnan és bármely célpont ellen. Ezzel kapcsolatban a stratégia így fogalmaz: „Számos ország a kiberképességét mások befolyásolására, és néhányan az autokratikus rezsimek védelmére, azok kiterjesztésére használják. A számítógépes támadások a modern konfliktusok kulcsfontosságú elemévé váltak."

A kibertérben ezért a következő feladatokat kell végrehajtani:

- a kibertámadást végrehajtó személyek, csoportok vagy országok azonosításának képességét növelni kell, hozzájárulva a gyors válaszreakciók kialakításához,
- növelni kell a kibervédelem eszközkészletét és szakmai hátterét,
- javítani kell a hatóságok és eljárások integrációját az Egyesült Államok kormányán belül, hogy a szükséges számítógépes intézkedéseket végre lehessen hajtani [3].

Az USA nemzetvédelmi stratégiája

A 2018. év elején jelent meg az USA új Nemzetvédelmi Stratégiája, melynek fő célja az Egyesült Államok versenyképes katonai előnyének a helyreállítása. Ez magában foglalja azt is, hogy megakadályozza Kínát és Oroszországot abban, hogy akár az Egyesült Államokat, akár szövetségeseit támadva megpróbálja felrobbantani a második világháború óta fennálló nemzetközi rendet.[2].

A stratégia a kihívásokat elemezve megállapítja, hogy a hagyományos négy hadviselési dimenzió mellé a kibertér is bekerült, amelyre ugyanolyan figyelmet kell fordítani, mint a tradicionálisan meglévő négyre: a vonalharcászat, a koncentrált tűzerő, mobil hadviselés, hibrid hadviselés [2].

A dokumentum a veszélyforrások bemutatásánál kitér a kibertérben jelentkező veszélyekre is, hangsúlyozva, hogy ebben a tekintetben az Egyesült Államok is célpont, ráadásul, mivel itt nincsenek határok, ezért a kibertámadások vagy akár a korábban már említett információs befolyásolás gyakorlatilag bárhonnan bekövetkezhet.

„A Védelmi Minisztérium priorizálja mindazokat a beruházásokat, amelyek az űrben lévő ellenálló képességre és az ott folyó műveletekre irányulnak. A kibervédelemre, a kiberrugalmasságra és -képességek folyamatos integrációjára nagy hangsúlyt fektetünk a katonai műveletek teljes spektrumába" [2].

Vannak azonban úgynevezett szabályok, amelyek a kiberbiztonság fenntartására vonatkoznak. Ezeket a szabályokat a CCDCOE, a NATO Együttműködő Kibervédelmi Kiválósági Központja fogalmazta meg 2011-ben *Ten Rules for Cyber Security* címmel (The NATO Cooperative Cyber Defense of Excellence) [1].

1. **A területi szabály –** az állam területén belül található információs infrastruktúra az adott állam területi szuverenitása alá tartozik.
2. **A felelősség szabály –** az a tény, hogy egy állam területén információs rendszerből kibertámadást indítottak, azt bizonyítja, hogy a cselekmény az adott államnak tulajdonítható.
3. **Az együttműködési szabály –** az a tény, hogy egy kibertámadást egy állam területén található információs rendszereken keresztül hajtottak végre, kötelezettséget teremt az áldozat országgal való együttműködésre.
4. **Az önvédelemszabály –** mindenkinek jogában áll megvédeni önmagát.
5. **Az adatvédelmi szabály –** az információs infrastruktúra monotoring adatait személyesnek tekintjük, hacsak máskent nem rendelkezik (az EU-ban elterjedt értelmezés).
6. **A gondossági kötelezettség szabálya –** mindenkinek felelőssége az észszerű biztonság megvalósítása saját információinak infrastruktúrájában.
7. **A korai figyelmeztetés szabálya –** köteles értesíteni a potenciális áldozatokat az ismert, közelgő kibertámadásokról.

8. Az információhoz való hozzáférés szabálya – a nyilvánosságnak joga van tájékoztatást kapni az életét, biztonságát és jólétét fenyegető veszélyekről.

9. A büntethetőségi szabály – minden nemzetnek felelőssége, hogy a leggyakoribb kiberbűncselekményeket belefoglalja anyagi büntetőjogába.

10. A megbízási szabály – egy szervezet cselekvése (és szabályozási) képessége a megbízásából fakad.

Végezetül, véleményem szerint a kiberbiztonság az Amerikai Egyesült Államokban nagyon fejlett és törekednek arra, hogy minél jobb és újabb technológiákat hozzanak létre a fejlesztése érdekében. A kiberbiztonság egy érzékeny téma, amelyre a többi országnak is fokozott figyelmet kell fordítania.

Felhasznált források:

1. Eneken Tikk. Ten Rules of Cyber Security, 2011. (2024.09.18)
2. Kovács László. Kiberbiztonság és -stratégia, 2018. (2024.09.19)
3. John Bolton. The RoomWhereIt Happenned: A White House Memoir, 2020. (2024.09.19)

DARCSI Karolina
adjunktus,
Történelem- és Társadalomtudományi Tanszék,
Lehoczky Tivadar Társadalomtudományi Kutatóközpont kutatója,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
HUBER Alex
II. évfolyamos
nemzetközi kapcsolatok, társadalmi kommunikáció
és regionális tanulmányok szakos hallgató,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

KIBERBIZTONSÁG NÉMETORSZÁGBAN

Németország nemcsak gazdasági mutatói és lakosságszáma alapján Európa vezető állama, hanem a digitális és kiberbiztonság terén is kiemelkedő eredményeket tud felmutatni. Az ország a digitális piacot érintően igen kiterjedt és fejlett szabályozással rendelkezik, és sikeresen integrálódott a nemzetközi folyamatokba is.

A tanulmány Németország digitális és kiberbiztonsági helyzetét vázolja fel, ismertetve a főbb vonatkozó dokumentumokat és a szervezeti hátteret. Bár impozánsak az elért eredmények, a következő években további fejlesztésekre van szükség valamennyi területen ahhoz, hogy Németország a lehető legteljesebb mértékben képes legyen állami intézményeit és állampolgárait a kibertámadásoktól megvédeni.

Kulcsszavak: kiberbiztonság, Németország, digitális biztonság [1].

Németországban igen korán, már 1980 években bevezették az internetet. Ekkoriban még a Deutsche Telekom volt az egyetlen szolgáltató, amely a BXT (Bildschirmtext) hálózatot használta.

A Deutsche Telekom egészen 1995-ig őrizte monopol helyzetét Németországban, csak ezt követően nyitották meg a piacot a magánvállalkozások előtt. S bár a privatizáció lezajlott, a német állam és a szövetségi kormányok még mindig magukénak tudhatják a Deutsche Telekom részvényeinek egyharmadát, és jelenleg is ez az „állami vállalat” az ország legnagyobb internetszolgáltatója [2].

A Digitális Agenda 2014–2017 elnevezésű stratégiai dokumentumot a német szövetségi kormány 2014 augusztusában adta ki. A digitális teret illetően ez a dokumentum szerepel a stratégiai hierarchia csúcsán, mivel ezt maga a szövetségi kormány jegyzi meg. Az agenda a német lakosságot a középpontba helyezve három alapvető stratégiai célt rögzített: az elterjedését és a foglalkoztatottság szintjének növelését, a digitális lehetőségekhez való hozzáférése és a részvétel biztosítására, valamint a bizalom és a biztonság megteremtése. Az e célok megvalósításához szükséges alapot az alkotmányban rögzített értékek biztosítják, amelyek érvényesülését nemcsak a valós, hanem a virtuális világban is biztosítani kell [3].

A digitális infrastruktúra vonatkozásában az egyik fontos lépése a 2016. január 27-i gyors internethálózatok kiépítését megkönnyítő szabályozást tartalmazó törvény elfogadása volt.

A fiatalok ösztönzésképpen külön kormányzati segítséget kapnak a digitális gazdasági vállalkozások és munkahelyek megteremtéséhez, az IT-vállalatok és startupok működtetéséhez. Ezzel kapcsolatban összességében elmondható, hogy Németország már jelenleg is igen jó mutatókkal rendelkezik.

A német kiberbiztonsági szervezetrendszer

A német stratégiafejlődés mozgatórugója a szövetségi belügyminisztérium, amely szorosan együttműködik a Külügyminisztériummal, a Védelmi Minisztériummal, a Gazdasági és Energetikai Minisztériummal és az Igazságügyi Minisztériummal.

2011-ben a kormány felállította a Nemzeti Incidenskezelő Központot (Nationales Cyber-Abwehrzentrum – NCAZ), melynek feladata a kormányzati szervek közötti műveleti szintű kooperáció és IT-incidensek esetén a válaszlépések összehangolása.

A NCAZ az incidensekre való gyors reagálás érdekében nemzeti irányítási-vezetési és elemzőközponti funkciókat lát el. Emellett tájékoztatja a társadalmat a kibertámadásokról, sérülékenységekről és az elkövetőkről.

A Belügyminisztérium irányítása alá tartozó Szövetségi Információbiztonsági Hivatal (Bundesamt für Sicherheit in der Informationstechnik – BSI) felel az incidenskezelő központ feladatainak végrehajtásáért. Más hatóságok, mint a Szövetségi Alkotmányvédelmi Hivatal (Bundesamt für Verfassungsschutz – BfV), a Civil Védelem és Katasztrófavédelmi Szövetségi Hivatal (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – BBK), a Szövetségi Bűnügyi Hivatal (Bundeskriminalamt – BKA), a Szövetségi Rendőrség (Bundespolizei – BPOL), a Bűnügyi Vámhivatal (Zollkriminalamt – ZKA), a Szövetségi Hírszerzési Hivatal (Bundesnachrichtendienst – BND), a német hadsereg (Bundeswehr) és a kritikusinfrastruktúra-üzemeltetőket felügyelő hivatalok is együttműködnek egymással az incidenskezelő központon belül a konkrét eseteknek megfelelően. A központ incidens esetén a Szövetségi Belügyminisztériumot közvetlenül tájékoztatja [4].

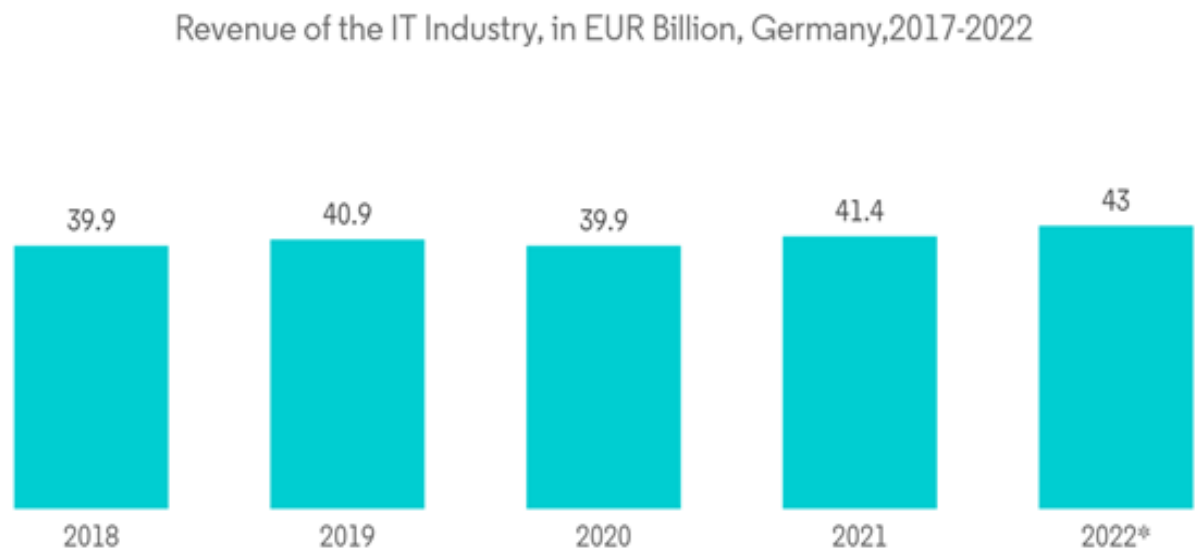
A Szövetségi Bűnügyi Hivatal (Bundeskriminalamt – BKA) szintén a Belügyminisztérium irányítása alá tartozik, és magasan szervezett, kiemelt jelentőségű bűnügyek kapcsán a kibertérben is tevékeny. Külön kiberbűnözési részleggel is rendelkezik, ahol az ilyen bűncselekményekkel kapcsolatos kompetenciák és információk összefutnak [5].

Németország kiberbiztonsági piaci részesedése

A német kiberbiztonsági piac méretét 2024-ben 12,60 milliárd USD-ra becsülik, 2029-re pedig várhatóan eléri a 21,47 milliárd USD-t, ami 11,25%-os CAGR-növekedést jelent a 2024–2029 közötti előrejelzési időszakban [8].

A kereskedelmi platformok megjelenésével járó kibertámadások száma növekedni kezdett. Az okoseszközök terjedése és a felhőmegoldások elterjedése csak néhány tényező a piac növekedésében. A kiberfenyegetések az intelligens és IoT-technológiával rendelkező eszközök használatának növekedésével várhatóan tovább fognak fejlődni. Ennek megfelelően a cégek haladó kiberbiztonsági megoldásokat fogadnak el és alkalmaznak a kibertámadások észlelésére, minimalizálására és kockázatának mérséklésére, ezáltal elősegítve a piac növekedését.

A német kiberbiztonsági piac félig konszolidált olyan jelentős szereplők jelenlétével, mint a Cisco Systems, az IBM, a Dell Technologies, a Fortinet és az Intel Security. A piac szereplői olyan stratégiákat alkalmaznak, mint például a partnerségek vagy a felvásárlások, hogy bővítsék termékkínálatukat, s fenntartható versenyelőnyre tegyenek szert.



Németország diverzifikált kiberbiztonsági ökoszisztémával rendelkezik, ahol a kiberbiztonsággal foglalkozó induló vállalkozások, kutatószervezetek és egyetemek széles spektruma található. Az ország kormányzati politikája különösen támogató, olyan erőfeszítéseket tesz, mint a Nemzeti Kiberbiztonsági Stratégia és a Kiberbiztonsági Törvény [6].

A kibertámadások számának növekedése a régióban várhatóan növeli a kiberbiztonsági megoldásokat. A német Szövetségi Információbiztonsági Hivatal (BSI) 2022-ben például azt állította, hogy a fogyasztók általános aggodalma a közelmúltban enyhén emelkedett az elmúlt három évhez képest. A válaszadók körülbelül 29%-a azt nyilatkozta, hogy volt már internetes bűncselekmény áldozata.

A korábbi években ez az arány 25% volt. A válaszadók negyede tapasztalt csalást és lopást az internetes vásárlás során.

A kiberbiztonsági piacon kulcsfontosságú az olyan kockázatok kezelése, mint a harmadik felek szállítóinak kockázatai, a felügyelt biztonsági szolgáltatók, mint a (MSSP-k) változásai, valamint a felhőalapú stratégia felé való elmozdulás. Mivel a vállalkozások egyre inkább külső beszállítókra számítanak különféle szolgáltatók és technológiák tekintetében, a kapcsolódó kockázatok is növekednek.

Az elmúlt néhány évben a biztonsági rendszerek megnehezítették a támadók számára a kritikus adatok elérését. Ennek eredményeként a hétköznapi felhasználók egyre inkább óvakodnak az internet biztonságától. Azok a megoldások, amelyek néhány évvel ezelőtt működtek, most irrelevánsak. A kibertámadások azonosításához és helyreállításához a szervezeteknek több erőforrásra van szüksége, és magasabb felkészültségre. Sok esetben előfordulhat, hogy a szervezetnek napokra teljesen le kell állítani a tevékenységét, hogy felépüljön egy incidens vagy támadás után. Rossz tervezés és nem megfelelő infrastruktúra esetén az incidens utáni felépülési idő jelentősen hosszú lehet.

A kiberbűnözők a kibertámadások lehetőségeit látták a COVID–19-világjárványban. Az otthonról dolgozó alkalmazottak sebezhetővé váltak.

A világjárvány után megnőtt a kiberbiztonság iránti igény, mivel a hónapokig tartó üzletmenet-folytonossági tervek (BCP) végrehajtását tervező vállalkozások – beleértve az információbiztonsági megfigyelést és a karanténkörülmények között történő reagálást – a kiberbiztonság fokozására összpontosítottak. Így a digitalizáció és a méretezhető IT-infrastruktúra iránti növekvő kereslet mellett a vizsgált piac gyorsan növekszik.

Az információs technológia (IT) és a távközlés létfontosságú a vállalkozások, a kormányzati szervek és a szervezetek számára. A robusztus kiberbiztonsági intézkedések iránti igény döntő jelentőségűvé vált az összekapcsolt hálózatok, a felhőalapú számítástechnika és a digitális kommunikáció növekvő függőség miatt. Az informatikai és telekommunikációs végfelhasználók a globális kiberbiztonsági piac jelentős részét alkotják, mivel meg akarják védeni érzékeny adataikat, hálózataikat és kommunikációjukat a fejlődő kiberfenyegetésekkel szemben [7].

Bár az EU-n belül sokat költenek a kiberbiztonságra, és jóval fejlettebb technológiával bírnak, mint az egykori posztszovjet térség országai, mégis, még maga Németország sincs kellően felkészülve egy esetleges nagyszabású kibertámadásra, mivel nem rendelkezik működő válságkezelő rendszerrel – figyelmeztetett a Szövetségi Információbiztonsági Hivatal (BSI) vezetője 2024 nyarán. A német kiberbiztonsági hatóság, a BSI (Bundesamt für Sicherheit in der Informationstechnik) vezetőjének nyilatkozata szerint a német kibervédelem szervezetrendszere nem alkalmas egy összehangolt kibertámadás kezelésére, ezért folyamatosan szükséges azt fejleszteni és bővíteni.

Felhasznált források:

1. https://folyoirat.ludovika.hu/index.php/neb/article/view/3615/2898
2. https://folyoirat.ludovika.hu/index.php/neb/article/view/3615/2898
3. https://folyoirat.ludovika.hu/index.php/neb/article/view/3615/2898
4. https://folyoirat.ludovika.hu/index.php/neb/article/view/3615/2898
5. https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/2_2021_MIC_RP.pdf
6. https://www.globenewswire.com/news-release/2024/09/16/2946526/0/en/Germany-Cybersecurity-Market-Share-Analysis-Industry-Trends-Growth-Forecasts-2024-2029.html
7. https://www.globenewswire.com/news-release/2024/09/16/2946526/0/en/Germany-Cybersecurity-Market-Share-Analysis-Industry-Trends-Growth-Forecasts-2024-2029.html
8. Dublin, 2024. szeptember 16. (GLOBE NEWSWIRE) – Németország kiberbiztonsága – Piaci részesedés elemzése, iparági trendek és statisztikák, növekedési előrejelzések (2024–2029).

CSATÁRY György
PhD, docens, tanszékvezető,
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
SZENYKÓ Volodimir
II. évfolyamos
nemzetközi kapcsolatok, társadalmi kommunikáció
és regionális tanulmányok szakos hallgató,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

KIBERBIZTONSÁG AZ EURÓPAI UNIÓ ÉLETÉBEN

Kulcsszavak: *kiberbiztonság, Európai Unió, Európai Bizottság, NIS.*

Az Európai Unió kiberbiztonsága kulcsfontosságú kérdés, mivel a digitális világban egyre több fenyegetés éri az államokat, vállalatokat és polgárokat.A kiberbiztonság a számítógépes rendszerek, hálózatok és adatok védelmét jelenti az illetéktelen hozzáférésekkel, adatlopásokkal, támadásokkal és egyéb kiberbűncselekményekkel szemben. Az EU gazdasága és társadalma egyre inkább függ a digitális technológiáktól, a hálózati rendszerektől és az online szolgáltatásoktól. A pénzügyi, egészségügyi, közlekedési, energetikai rendszerek és a kommunikáció jelentős része már digitális alapon működik. Ez a növekvő digitalizáció azonban sebezhetővé tette ezeket az infrastruktúrákat a kibertámadásokkal szemben. A kibertámadások jelentős gazdasági veszteségeket okozhatnak, például adatlopások, szolgáltatáskimaradások vagy pénzügyi csalások révén. Egy súlyos támadás veszélyeztetheti a vállalatok működését, a kritikus infrastruktúrákat és a lakosság biztonságát is, de gyakran geopolitikai konfliktusok eszközei is lehetnek, mivel egyes országok államilag támogatott kiberműveletekkel igyekeznek gyengíteni más államokat vagy destabilizálni kormányokat. Ezért az EU-nak fontos volt, hogy erősítse a tagállamok közötti együttműködést és koordinációt ezen fenyegetések kezelését illetően, hiszen az EU közös biztonsága is függ ettől.

Az EU ezért olyan rendszereket épített ki, amelyek csökkenthetik a kockázatokat. A kormányoknak biztosítaniuk kell, hogy a kritikus infrastruktúrák – mint az energiaellátás, a közlekedés, az egészségügyi rendszerek – védettek legyenek a kibertámadásokkal szemben. A NIS és NIS2 irányelvek ezeket az ágazatokat célozzák, hogy erősítsék az információs rendszereik biztonságát. A NIS (Network and Information Systems) irányelv az Európai Unió első kiberbiztonsági szabályozása, amelyet 2016-ban fogadtak el.

A kibertámadások és a kiberbűncselekmények Európa-szerte egyre gyakoribbá és egyre kifinomultabbá válnak. Ez a tendencia a jövőben várhatóan tovább fog erősödni, mivel 2025-re világszerte előreláthatólag 41 milliárd készülék kapcsolódik majd az internethez.

Amennyiben a nyílt és biztonságos kibertér kiépítése érdekében erőteljesebb kiberbiztonsági intézkedéseket hozunk, az nagyobb bizalmat teremthet a polgárok körében a digitális eszközök és szolgáltatások iránt. Az EU ezért komplex szabályozásokat, intézményeket és együttműködési mechanizmusokat hozott létre a kiberfenyegetések kezelésére és a digitális tér biztonságának növelésére [1].

Az EU kiberbiztonsági stratégiája

Az Európai Bizottság és az Unió külügyi és biztonságpolitikai főképviselője új uniós kiberbiztonsági stratégiát terjesztett elő. Társadalmunk digitális átalakulása, amelyet a Covid–19-válság fokozott, kiterjesztette a fenyegetettségi teret, és olyan új kihívásokat állított, amelyek innovatív válaszokat igényelnek. A kibertámadások száma továbbra is növekszik, és egyre kifinomultabb támadások érkeznek az EU-n belüli és kívüli forrásokból egyaránt.

Az EU-nak ezért vezető szerepet kell vállalnia a biztonságos digitalizációra irányuló erőfeszítésekben. Az alapvető szolgáltatásokra és a kritikus infrastruktúrákra vonatkozó világszínvonalú megoldások és kiberbiztonsági szabványok normáinak, valamint az új technológiák fejlesztésének és alkalmazásának erősödnie kell. A kormányok, a vállalkozások és a polgárok közös felelőssége lesz a kiberbiztonságos digitális átalakulás biztosítása.

Ez a stratégia leírja, hogy az EU hogyan tudja kiaknázni és megerősíteni valamennyi eszközét és forrását ahhoz, hogy technológiailag szuverén legyen. Azt is meghatározza, hogy az EU miként fokozhatja együttműködését világszerte olyan partnerekkel, amelyek osztják a demokráciával, a jogállamisággal és az emberi jogokkal kapcsolatos értékeinket.

Az EU technológiai szuverenitásának az összes összekapcsolt szolgáltatás és termék rezilienciáján kell alapulnia. Mind a négy kiberközösségnek – a belső piaccal, a bűnüldözéssel, a diplomáciával és a védelemmel foglalkozóknak – szorosabban együtt kell működnie a fenyegetésekkel kapcsolatos közös tudatosság érdekében. Készen kell állniuk arra, hogy közösen reagáljanak, amikor kibertámadás történik, hogy az EU meg tudja védeni magát.

Ez a stratégia kiterjed az olyan alapvető szolgáltatások biztonságára, mint a kórházak, az energiahálózatok, a vasutak és a folyamatosan növekvő számú összekapcsolt tárgyak otthonainkban, irodáinkban és gyárainkban. A stratégia célja volt, hogy kollektív képességeket építsen ki a nagyobb kibertámadásokra való reagáláshoz. Felvázolja továbbá, hogy világszerte együtt kell működni a partnerekkel a kibertér nemzetközi biztonságának és stabilitásának biztosítása érdekében. Emellett azt is felvázolja, hogy a közös kiberbiztonsági egység a tagállamok és az EU rendelkezésére álló kollektív erőforrások és szakértelem felhasználásával hogyan tud a leghatékonyabb választ adni a kiberfenyegetésekre.

Az új stratégia célja, hogy olyan globális és nyitott internetet biztosítson, amely erős biztosítékokkal rendelkezik az európai polgárok biztonságára és alapvető jogaira nézve. Az előző stratégiák keretében elért előrehaladást követően a dokumentum konkrét javaslatokat tartalmaz három fő eszköz alkalmazására vonatkozóan. Ez a három eszköz a szabályozási, beruházási és szakpolitikai kezdeményezések. Az uniós fellépés három területét fogják érinteni: reziliencia, technológiai szuverenitás és vezető szerep; működési kapacitás a megelőzésre, az elrettentésre és a reagálásra; együttműködés a globális és nyitott kibertér előmozdítása érdekében.

Az EU elkötelezett amellett, hogy az elkövetkező hét évben példátlan mértékű beruházások révén támogassa ezt a stratégiát. Ez megnégyszerezné a korábbi beruházási szinteket. Bizonyítja, hogy az EU elkötelezett az új technológiai és iparpolitikája, valamint a gazdaságélénkítési menetrend iránt [2].

Az EU kiberbiztonsági szabályai

Az EU szabályai megkövetelik a tagállamoktól, hogy kidolgozzák és végrehajtsák saját nemzeti kiberbiztonsági stratégiájukat. Ez ösztönzi az államokat arra, hogy rendszerezett és átfogó megközelítést alkalmazzanak a kiberbiztonsági fenyegetések kezelésére. Ennek eredményeként a tagállamok olyan intézményeket és hatóságokat hoznak létre, mint a nemzeti kiberbiztonsági ügynökségek és CSIRT-ek (Computer Security Incident Response Teams), amelyek a kibertámadások kezeléséért felelnek. A szabályok hozzájárulnak a kiberbiztonsági szabványok egységesítéséhez a tagállamok között. Ez azt jelenti, hogy minden tagállamban azonos követelményeket kell alkalmazniuk a kritikus fontosságú infrastruktúrákat üzemeltető ágazatoknak és szolgáltatóknak. Ez csökkenti a különbségeket a különböző országok biztonsági rendszerei között, és biztosítja, hogy az EU egész területén magas szintű kiberbiztonsági védelem legyen érvényben.

Különösen nagy hangsúlyt fektetnek a kritikus infrastruktúrák, például az energiaellátás, közlekedés, pénzügyi szolgáltatások és egészségügy védelmére. A tagállamoknak gondoskodniuk

kell arról, hogy ezek a rendszerek ellenállóak legyenek a kibertámadásokkal szemben, és biztosítaniuk kell, hogy a működésük folyamatosan fenntartható maradjon, még egy támadás esetén is. Ez komoly befektetéseket és technológiai fejlesztéseket igényel, de hosszú távon stabilabb és biztonságosabb működést eredményez.

A NIS és NIS2 irányelvek komoly szankciókat tartalmaznak a kiberbiztonsági szabályok megszegése esetén. A tagállamoknak be kell vezetniük olyan jogszabályokat, amelyek megfelelő bírságokat és egyéb büntetéseket írnak elő azoknak a szervezeteknek, amelyek nem tesznek eleget a kiberbiztonsági kötelezettségeknek. Ez ösztönzi a vállalatokat és állami intézményeket arra, hogy komolyan vegyék a kiberbiztonsági előírásokat.

Az EU-s szabályok hatására a tagállamok nagyobb hangsúlyt fektetnek a kiberbiztonsági oktatásra és tudatosságnövelésre. Programokat indítanak a lakosság, vállalatok és állami intézmények számára, hogy jobban megértsék a kiberfenyegetéseket, és hatékonyabban tudják kezelni azokat. Ezzel a társadalom és a gazdaság egészének kiberbiztonsági felkészültsége nő.

Célja, hogy erősítsék a tagállamok védekezőképességét a kibertérben megjelenő fenyegetésekkel szemben, és egységes keretet biztosítsanak a kritikus infrastruktúrák védelmére. A legfontosabb szabályozás a NIS (Network and Information Systems) irányelv, amely 2016-ban lépett életbe, majd 2022-ben a továbbfejlesztett NIS2 irányelv jelent meg. E szabályok főként a kritikus ágazatokat – energia, közlekedés, egészségügy, pénzügyi szolgáltatások – és a digitális szolgáltatókat célozzák meg. A szabályozások előírják a tagállamok számára, hogy nemzeti kiberbiztonsági stratégiát dolgozzanak ki, hozzanak létre nemzeti kiberbiztonsági hatóságokat és CSIRT-eket (Computer Security Incident Response Teams), amelyek felelősek a kibertámadásokra adott válaszokért. Az EU elősegíti a tagállamok közötti együttműködést és információmegosztást is, hogy hatékonyabban kezeljék a közös kiberfenyegetéseket.

Ezek a szabályok erősítik a tagállamok kiberbiztonsági infrastruktúráját, harmonizálják a szabványokat és növelik a tudatosságot, hogy hatékonyabban lehessen megvédeni a digitális rendszereket a növekvő kiberfenyegetésekkel szemben [3].

Az Európai Unió és Ukrajna kiberbiztonságának megerősítése

Európai Unió az Európai Békekeret révén támogatja az Ukrán Fegyveres Erők kiberbiztonsági képességeinek megerősítését. Utoljára 3 millió euróval finanszírozta Ukrajnát.

Az Ukrajna elleni teljes körű orosz agresszió kezdete óta az Európai Unió segíti az ukrán fegyveres erőket a kibertér védelmében. Ukrajnában a kiberfenyegetésekkel szembeni védekezőképesség fokozására, és a biztonsági, illetve védelmi ágazatokban folytatott együttműködés megerősítésére irányuló átfogó megközelítés részeként elindítottak egy kiberlabort, megnyitottak egy tantermet, további biztonsági hardvereket és szoftvereket biztosítottak, és kiberbiztonsági képzéseket tartottak.

A kiberlabor technológia lehetővé teszi a felhasználó számára, hogy egy valósághű, meggyőző és hiteles virtuális környezetet hozzon létre a kibertámadásokra adott megfelelő és időben történő válaszlépések gyakorlására, amelynek során a diákok valós időben reagálnak a kibertámadás-szimulációkra és védekeznek. Ebben a szimulált környezetben az Ukrán Fegyveres Erők katonai személyzete megtanulhatja, hogyan lehet jobban megbirkózni a nagyfokú stresszel, azonosítani és vizsgálni a különböző hálózati rendszerek sebezhetőségeit. A kiberosztályterem pedig 15 munkaállomást, a kiképzéshez és a kibervédelmi gyakorlatokhoz szükséges felszerelést biztosít. A projekt keretében biztonsági szoftvereket és hardvereket szereztek be, telepítettek és konfiguráltak az ukrán fegyveres erők számára, valamint szakmai képzést biztosítottak.

De sajnos a technológiai és szakemberhiány a kiberbiztonság terén még így is komoly kihívást jelent mind Ukrajna, mind az Európai Unió számára, különösen a növekvő kibertámadások és a gyorsan fejlődő digitális technológiák fényében. A kiberbiztonság területén világszerte, így

Ukrajnában és az EU-ban is súlyos probléma a magasan képzett szakemberek hiánya. A komplex támadások elleni védekezéshez speciális tudással rendelkező szakértőkre van szükség, akik képesek az új fenyegetések gyors felismerésére és elhárítására. Bár egyre több program és tanfolyam létezik, sok országban, köztük Ukrajnában, az oktatási rendszerek nem biztosítanak elegendő számú jól képzett szakértőt. Technológiai és szakemberhiány miatt a szervezetek és az országok sebezhetőbbé válnak a kibertámadásokkal szemben. Ez különösen igaz a kritikus infrastruktúrák (pl. energia, közlekedés, kommunikáció) esetében, amelyek célpontjai lehetnek az ellenséges kiberműveleteknek. Ha nincs elegendő szakember, a kibertámadásokra adott válaszidő megnövekedhet, ami nagyobb kárt okozhat, és hosszabb helyreállítási időszakot eredményezhet.

A projektet az Európai Békekeret támogatja: „Kibervédelmi komponens – az Európai Békekeret támogatási intézkedése Ukrajna fegyveres erőinek támogatására” 2022 márciusától 2024 áprilisáig tart. Célja az ukrán fegyveres erők kibervédelmi képességeinek fokozása. A kibervédelmi komponens teljes költségvetése 3 millió EUR. A projektet az Észt Elektronikus Kormányzati Akadémia hajtja végre [4].

Felhasznált források:

1. https://www.consilium.europa.eu/hu/policies/cybersecurity/ (Letöltve: 2024.09.24.)
2. https://digital-strategy.ec.europa.eu/hu/policies/cybersecurity-strategy (Letöltve: 2024.09.24.)
3. https://eur-lex.europa.eu/hu/legal-content/summary/the-eu-cybersecurity-act.html (Letöltve: 2024.09.24.)
4. https://www.eeas.europa.eu/delegations/ukraine/ (Letöltve: 2024.09.25.)

Yelyzaveta MOLNAR D.
PhD (History)
Associate Professor at the Department of History and Social Sciences
director of the Tivadar Lehoczky Social Sciences Research Centre
Ferenc Rákóczi II Transcarpathian Hungarian College of Higher Education
Orsolya MÁTÉ
2nd year student
Department of History and Social Sciences, major of international relations, public communications and regional studies at the Ferenc Rákóczi II Transcarpathian Hungarian College of Higher Education

CANADA'S CYBERSECURITY

Key words: *cybersecurity, technology, COVID-19, threat.*

In today's interconnected world, cybersecurity has become a pivotal concern for nations, and Canada is no exception. As technology advances, so too do the threats that jeopardize the security of individuals, organizations, and the country's critical infrastructure. With increasing reliance on digital systems, the potential for cyberattacks grows, impacting everything from personal data to national security. The rise of the internet and digital technologies has transformed how businesses operate and how individuals communicate, but it has also opened the door to malicious actors seeking to exploit vulnerabilities. Cybersecurity threats can range from ransomware attacks that lock users out of their systems to data breaches that compromise sensitive personal information. These threats are not just technical issues; they can have significant economic and social implications, affecting public trust and national security.

Canada's cybersecurity environment is characterized by a diverse array of threats. These range from cybercrime perpetrated by individuals and organized groups to state-sponsored attacks targeting critical infrastructure. Recent years have seen a surge in incidents of ransomware, phishing, and data breaches, significantly impacting both private enterprises and public institutions. According to the Canadian Centre for Cyber Security (CCCS), sectors such as healthcare, finance, and energy are particularly vulnerable, often serving as attractive targets for cybercriminals looking to exploit weaknesses. In 2021, the Canadian Centre for Cyber Security (CCCS) reported a staggering increase in ransomware incidents, with a 151% rise compared to the previous year. This trend is echoed globally; according to Cybersecurity Ventures, ransomware attacks are projected to occur every 11 seconds by 2021, up from every 40 seconds in 2016. This alarming statistic underscores the urgency for effective cybersecurity measures (CCCS, 2022).

The COVID-19 pandemic further exacerbated the cybersecurity landscape, as many organizations rapidly transitioned to remote work, inadvertently expanding their attack surfaces in unprecedented ways. With employees accessing corporate networks from home, often on personal devices and unsecured Wi-Fi connections, potential vulnerabilities multiplied significantly. According to a report by the Cybersecurity and Infrastructure Security Agency (CISA), this shift led to a noticeable increase in cyber incidents, emphasizing how the rapid adoption of remote work arrangements created new opportunities for cybercriminals (CISA, 2020).

Cybercriminals quickly adapted to this new normal, launching targeted phishing campaigns that exploited the heightened fears and uncertainties surrounding the pandemic. For example, studies from cybersecurity firms indicated that the volume of phishing emails surged, with some organizations reporting increases of up to 600% during the early months of the pandemic (Mimecast, 2020). These attacks were often crafted to appear as communications from trusted entities, such as health organizations or government agencies, containing urgent information about COVID-19 protocols, vaccine availability, or financial assistance. Such messages lured individuals into clicking on malicious links or downloading harmful attachments, which compromised both personal and organizational data.

Moreover, many employees lacked adequate cybersecurity training and awareness. As companies rushed to implement remote work policies, training sessions were often abbreviated or overlooked altogether. A study by IBM found that 95% of cybersecurity breaches are due to human error,

highlighting the critical role that employee awareness plays in maintaining security (IBM, 2021). The abrupt transition meant that many workers were unprepared for the increased risks associated with remote work, leaving significant gaps in knowledge about safe online practices. As a result, employees became more susceptible to social engineering tactics, creating an environment ripe for exploitation.

In addition to phishing attacks, cybercriminals exploited security gaps in home networks. Many employees relied on personal routers and devices that were not configured with the same level of security as those found in corporate environments. A report from the Federal Bureau of Investigation (FBI) indicated that unpatched software vulnerabilities and weak home network security were frequently targeted by cybercriminals, allowing unauthorized access to sensitive corporate information (FBI, 2020). Without robust firewalls and intrusion detection systems, home networks became easy targets for attackers seeking unauthorized access to organizational systems.

This evolving landscape underscores the urgent need for effective cybersecurity measures tailored to remote work environments. Organizations must not only reinforce their existing cybersecurity frameworks but also adopt new strategies to address the unique challenges posed by remote work. This includes implementing multifactor authentication, conducting regular security assessments, and providing comprehensive cybersecurity training to employees, ensuring they are equipped to recognize and respond to potential threats (Chaffey, 2021).

The pandemic has fundamentally altered the way we work, and as a result, the need for a proactive approach to cybersecurity has never been more critical. Organizations must recognize that the shift to remote work is likely to persist in some capacity, necessitating a long-term commitment to cybersecurity investment and innovation. According to the World Economic Forum, the ongoing hybrid work model may become a standard practice, which means that businesses must adapt their cybersecurity strategies accordingly (World Economic Forum, 2021). By adopting a forward-thinking mindset and prioritizing the security of remote work environments, organizations can better protect themselves against the evolving tactics of cybercriminals, ultimately safeguarding their operations and sensitive data.

Moreover, the rapid adoption of new technologies, including cloud computing and the Internet of Things (IoT), has expanded the attack surface available to malicious actors. Each connected device and online service presents potential vulnerabilities that can be exploited. The literature indicates that as the digital landscape evolves, so too must the strategies employed to mitigate these threats (Dunn Cavelty, 2013). The challenge lies in ensuring that security protocols keep pace with technological advancements.

In response to these challenges, the Canadian government has implemented several initiatives aimed at strengthening the nation's cybersecurity posture. Recognizing the increasing complexity of cyber threats, the 2018 National Cyber Security Strategy emphasizes a multi-faceted approach that encourages collaboration among government agencies, private sector stakeholders, and civil society. This strategy underscores the need for resilience by focusing on prevention, response, and recovery from cyber incidents (Public Safety Canada, 2018).

A central tenet of the strategy is the promotion of partnerships across various sectors. The government acknowledges that cybersecurity is a shared responsibility and that effective defense requires the engagement of all stakeholders. Research highlights the importance of public-private partnerships in enhancing cybersecurity resilience, as these collaborations facilitate information sharing, threat intelligence, and best practices (NIST, 2020). For instance, the Canadian Cyber Security Strategy fosters cooperation between the Canadian Centre for Cyber Security (CCCS) and private sector entities, enabling organizations to access timely threat assessments and resources.

Furthermore, the strategy highlights the importance of building a robust cybersecurity workforce. The Canadian government has recognized that a skilled workforce is essential for developing and maintaining effective cybersecurity measures. The 2018 strategy outlines plans to enhance education and training in cybersecurity fields, promoting initiatives that engage educational institutions and industry players. Literature indicates that organizations with a strong emphasis on training and

development are better equipped to handle cyber threats, as employees become more adept at recognizing and responding to potential risks (Cybersecurity Workforce Framework, 2017).

In addition to workforce development, the National Cyber Security Strategy places a strong emphasis on public awareness and education. Recognizing that human error is a significant factor in many cyber incidents, the strategy aims to equip Canadians with the knowledge and skills needed to navigate the digital landscape safely. Programs aimed at raising awareness about cybersecurity best practices are crucial, as studies show that informed users are less likely to fall victim to cyber attacks (Holt et al., 2020). Campaigns targeting schools, businesses, and community organizations help instill a culture of cybersecurity, ultimately leading to greater resilience at the societal level.

Another key aspect of the strategy is the commitment to enhancing the security of critical infrastructure. The Canadian government has identified critical sectors—such as energy, healthcare, and finance—that are essential for national security and economic stability. By establishing sector-specific frameworks, the government seeks to ensure that these sectors have the necessary protocols and resources to withstand and recover from cyber incidents. Research underscores the importance of protecting critical infrastructure, as disruptions in these sectors can have cascading effects on the broader economy and public safety (Heidt et al., 2018).

Lastly, the strategy emphasizes the need for continuous adaptation and improvement in cybersecurity practices. As cyber threats evolve, so too must the measures employed to combat them. This includes investing in research and development of new technologies and strategies to enhance threat detection and response capabilities. The literature suggests that an agile and adaptive approach to cybersecurity is essential for organizations to stay ahead of potential threats (Dunn Cavelty, 2013). By fostering an environment of innovation and collaboration, Canada can better position itself to face the challenges of an ever-changing cyber landscape.

In conclusion, the 2018 National Cyber Security Strategy represents a comprehensive approach to enhancing Canada's cybersecurity posture. By emphasizing collaboration, workforce development, public awareness, protection of critical infrastructure, and continuous improvement, the government aims to build a resilient and secure digital environment. As Canada moves forward, the ongoing commitment to these principles will be crucial in addressing the multifaceted nature of cyber threats and safeguarding the nation's digital future.

The establishment of the CCCS as a central authority for cybersecurity in Canada has been a significant development. The CCCS provides critical resources, threat intelligence, and guidance to both the public and private sectors. Its role is to foster a culture of cybersecurity awareness and preparedness across the nation. In 2021, the CCCS issued over 100 threat advisories, informing organizations about emerging threats and vulnerabilities (CCCS, 2022).

One notable initiative is the Cybersecurity Strategy for the Federal Government, which aims to improve the security of government networks and systems while also setting an example for the private sector. This strategy includes measures for enhancing incident response capabilities and protecting sensitive information. It also promotes information sharing between government and industry to create a more unified defense against cyber threats.

While government efforts are crucial, the private sector plays an equally important role in Canada's cybersecurity landscape. Many businesses, particularly small and medium-sized enterprises (SMEs), are often ill-prepared for cyber threats. The Canadian Internet Registration Authority (CIRA) notes that a significant number of SMEs lack basic cybersecurity measures, making them susceptible to attacks (CIRA, 2021). Initiatives like CyberSecure Canada aim to address this gap by providing resources and certification to help businesses bolster their cybersecurity practices.

Public awareness is also a critical factor. Educational campaigns focused on promoting cyber hygiene and best practices are essential in equipping citizens and organizations with the knowledge needed to defend against cyber threats. Research indicates that informed users are less likely to fall victim to cybercrime, making education a key component of prevention strategies (Holt et al., 2020). Programs in schools, community organizations, and workplaces play a vital role in raising awareness about potential risks and teaching people how to protect themselves online.

Furthermore, partnerships between government and the private sector have proven effective in addressing cybersecurity challenges. Information sharing initiatives, such as the Cyber Security Information Sharing Partnership (CSISP), facilitate the exchange of threat intelligence, allowing organizations to stay ahead of emerging threat.

Despite significant progress, Canada's cybersecurity landscape faces several ongoing challenges. The rapid pace of technological advancement often outstrips existing regulatory frameworks, creating gaps in security and oversight. Emerging technologies like artificial intelligence and machine learning introduce new vulnerabilities that must be addressed proactively (Kshetri, 2021). Additionally, the growing sophistication of cyber threats necessitates continuous adaptation and investment in cybersecurity measures.

The issue of cybersecurity skills shortages also poses a challenge. The demand for cybersecurity professionals far exceeds the available talent pool, leading to gaps in expertise that can hinder an organization's ability to defend against attacks. Educational institutions are beginning to respond by offering more cybersecurity programs, but it will take time to develop a workforce equipped to meet the increasing demands of the industry.

Another significant challenge is the evolving nature of cyber threats. Cybercriminals are becoming increasingly sophisticated, employing advanced tactics and techniques to breach defenses. State-sponsored attacks add another layer of complexity, as nation-state actors often have substantial resources at their disposal, enabling them to conduct prolonged and targeted campaigns against critical infrastructure.

Looking to the future, Canada must prioritize research and development in cybersecurity technologies while fostering a culture of innovation. Collaborative efforts between academic institutions, government, and the private sector can drive advancements in threat detection and response capabilities. Additionally, the literature emphasizes the need for a more robust legal framework to address the complexities of cybercrime, ensuring that laws keep pace with technological evolution (Brenner, 2010).

Furthermore, establishing a national cybersecurity training and certification program could help bridge the skills gap and prepare more professionals for careers in cybersecurity. Encouraging diversity in the cybersecurity workforce can also enhance innovation and problem-solving capabilities. Engaging underrepresented groups and promoting STEM education among youth will be crucial in building a more resilient workforce.

Canada's cybersecurity landscape is a complex interplay of challenges and opportunities. As cyber threats become increasingly sophisticated, the nation must continue to adapt its strategies to safeguard critical infrastructure, businesses, and citizens. By investing in education, fostering collaboration, and embracing innovation, Canada can enhance its resilience against an ever-evolving array of cyber threats. The ongoing commitment to a comprehensive approach will be essential in securing Canada's digital future.

References

5. Brenner, S. W. (2010). *Cybercrime: Criminal threats in the information age*. Santa Clara Computer and High Technology Law Journal.
6. Canadian Centre for Cyber Security (CCCS). (2022). *Cyber Threat Assessment 2022*. Government of Canada.
7. Chaffey, D. (2021). *Cybersecurity in a Post-Pandemic World: Strategies for Remote Work*. Smart Insights.
8. Federal Bureau of Investigation (FBI). (2020). *Cyber Crime: A Report on Cyber Incidents During the COVID-19 Pandemic*.
9. Canadian Internet Registration Authority (CIRA). (2021). *Cybersecurity for SMEs: A national snapshot*.
10. Dunn Cavelty, M. (2013). *Cybersecurity: An international perspective*. Routledge.
11. Holt, T. J., et al. (2020). *Cybersecurity awareness and education: The importance of public awareness campaigns*. Journal of Information Systems Security.

12. Kshetri, N. (2021). *Cybersecurity and the role of emerging technologies*. International Journal of Information Management.
13. Public Safety Canada. (2018). *National Cyber Security Strategy*.

Світлана КАЛАУР
доктор педагогічних наук, професор,
професор кафедри соціальної роботи та
менеджменту соціокультурної діяльності,
керівник Центру післядипломної освіти
Тернопільський національний педагогічний
університет імені Володимира Гнатюка
svitlanakalaur@gmail.com
Микола НАГОЛЮК
здобувач третього (освітньо-наукового)
рівня вищої освіти спеціальності 015
«Професійна освіта (за спеціалізаціями)»,
начальник відділу прикордонної служби № 3,
з прикордонного загону імені Героя України полковника Євгенія Пікуса
Тернопільський національний педагогічний
університет імені Володимира Гнатюка
naholiuk111@ukr.net

МОЖЛИВОСТІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СУЧАСНИХ УМОВАХ ОХОРОНИ ЗОВНІШНІХ КОРДОНІВ ЄВРОПЕЙСЬКОГО СОЮЗУ

Нині, зі зростанням ролі інформаційних технологій процеси прикордонного контролю стали більш автоматизованими. Завдяки впровадженню широкомасштабних інформаційних систем це, з одного боку, полегшило законну торгівлю і подорожі, а з іншого – посилило внутрішню безпеку Європейського Союзу (далі – ЄС). Однак посилення цифровізації кордонів зробило їх більш вразливими до кіберзагроз для тих, хто хоче порушити, або ввести в оману прикордонників. У міру того, як технологічний прогрес продовжує поширюватися, полегшуючи повсякденне життя завдяки зростанню автоматизації і зв'язку, недержавні суб'єкти також намагатимуться отримати вигоду з гонки за технологічною перевагою між державними суб'єктами. Усі зацікавлені сторони отримують вигоду від розвитку штучного інтелекту, обчислювальної техніки, безпілотних систем, матеріалів, тривимірного друку і енергоефективності, які сприяють подальшому зменшенню небезпечного впливу на довкілля, а досягнення в галузі геоінженерії підтримують більш масштабні та ефективні заходи з пом'якшення наслідків зміни клімату, у спробі контролювати погодні умови [1].

Управління зовнішніми кордонами може ще більше виграти від синергії з обороною, особливо в контексті можливостей і їх розвитку, де збігаються вимоги до засобів спостереження і зв'язку, а також до систем, які використовують технології, що дозволяють дистанційне пілотування, штучний інтелект і доповнену реальність. Систематичне використання існуючих широкомасштабних інформаційних систем ЄС – наприклад, Шенгенської інформаційної системи, Візової інформаційної системи та Європейської бази даних дактилоскопії з питань надання притулку – і перспективних нових систем, таких як Система контролю в'їзду-виїзду та Європейської системи авторизації інформації про подорожі, а також їхня оперативна сумісність мають вагоме значення для підвищення якості процесів управління кордонами. Ці системи дозволяють покращити попередню перевірку пасажирів та/або вдосконалити моніторинг перетину кордону, допомагають виявляти потенційні порушення і сприяють своєчасному обміну важливою інформацією між державами. Нові та модернізовані інформаційні системи та їхня інтероперабельність сприяє безперешкодному та безпечному руху через пункти пропуску через кордон, що не лише покращує управління ризиками, але й прокладає шлях до вдосконалення автоматизованих процесів прикордонного контролю, подальшої гармонізації операційних процедур на кордоні і, як наслідок, підвищує загальну ефективність. Відзначимо, що завдяки ефективному впровадженню і використанню інформаційних систем ЄС разом з національними базами даних, спрощенню процедур перетину кордону і забезпеченню високого рівня якості даних,

Європейська прикордонна і берегова охорона може працювати разом, щоб забезпечити належний попередній контроль і належну ідентифікацію.

Для ефективного запобігання та вирішення проблем із несанкціонованим перетином зовнішніх кордонів необхідне впровадження заходів на основі аналізу розвідданих та оцінки ризиків із використанням оперативних даних майже в режимі реального часу. Ці дані повинні стосуватися рівня впливу на різні ділянки зовнішнього кордону. Вони можуть включати застосування передових можливостей спостереження та моніторингу, зокрема в прикордонних районах. Це передбачає використання інтегрованих мереж датчиків на наземних, морських, повітряних і космічних платформах. Отримані з цих джерел дані об'єднуються та обробляються за допомогою штучного інтелекту, щоб ефективніше виявляти, ідентифікувати та відстежувати випадки несанкціонованого перетину кордону. Водночас наголосимо, що передові інформаційні технології повинні розроблятись з огляду на безпеку особистих даних та проходити відповідне оцінювання стосовно їх можливого впливу на дотримання основоположних прав осіб, які перетинають кордон.

Список використаних джерел:

1. Council of the European Union. 13926/3/06. FRONT 207, COMIX 826. Integrated Border Management; Strategy deliberations.
   URL: http://register.consilium.europa.eu/pdf/en/06/st13/st13926-re03.en06.pdf

Lubov PANTELLEIEVA
Second year Bachelor students,
"Cybersecurity and information Protection" major
National Aviation University
***Scientific supervisor* – Natalia BILOUS**
Associate professor,
Department of foreign languages for professional communication
National Aviation University

CYBERSECURITY: A GLOBAL PRIORITY

In recent years, cyberattacks have increased worldwide, often fueled by escalating international conflicts. As a result, nations are investing heavily in cybersecurity measures to prevent data leaks, mitigate damage, and protect the integrity of their information systems.

What is Cybersecurity?

Cybersecurity refers to a set of technical, organizational, and legal measures designed to safeguard information systems. Each country has developed its own institutions and frameworks to achieve these goals.

Cybersecurity in the United States

The U.S. has implemented several cybersecurity laws, enforced by specialized executive agencies. Some key pieces of legislation include:

1. The National Cybersecurity Protection Act
2. The Cybersecurity Enhancement Act

The U.S. strategy focuses on preserving and enhancing the benefits of digital networks for societal and economic development. As President Barack Obama stated on May 29, 2009:

"This world—cyberspace—is a world that we depend on every single day… [it] has made us more interconnected than at any time in human history."

Cybersecurity in Australia

In Australia, the cyber police cooperate with the U.S. Department of Homeland Security to bolster cybersecurity. The country has also passed the Amendments to Cybercrime Legislation and established Australia's Cybersecurity Strategy, which follows a four-step approach:

1. Protection and Prevention
2. Investigation
3. Disruption and Prosecution
4. Recovery
5. Cybersecurity in Poland

Poland's Ministry of Administration and Digital Technology has its own strategy. The country aims to establish a legal and organizational framework for cybersecurity while improving the distribution and exchange of information among users.

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

THE ROLE OF ARTIFICIAL INTELLIGENCE IN INFORMATION SECURITY

A MESTERSÉGES INTELLIGENCIA SZEREPE AZ INFORMÁCIÓBIZTONSÁG TERÜLETÉN

JAKAB Enikő
PhD, docens,
Matematika és Informatika Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
PAPP Gabriella
adjunktus,
Matematika és Informatika Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

MESTERSÉGES INTELLIGENCIA ALAPÚ OKTATÁSI ESZKÖZÖK BIZTONSÁGA: KIHÍVÁSOK ÉS MEGOLDÁSOK

A mesterséges intelligencia (MI) rohamos térnyerése számos területhez hasonlóan az oktatásban is változásokat irányoz elő. Az MI-alapú oktatási eszközök hirtelen elterjedése új tanulási lehetőségeket is rejt magában. Emellett az oktatás digitalizálódásával az MI-alapú oktatási eszközök egyre relevánsabbá válnak.

A mesterséges intelligencia az oktatással összefüggésben számos kérdést vet fel (technikai, etikai, biztonsági, pénzügyi stb.), amelyekre válaszokat kell találnunk a hatékony integráció megvalósításához. Éppen ezért a kutatásunk során szeretnénk megvizsgálni az MI-alapú oktatási eszközök mindennapi tanítási gyakorlatban való felhasználásának kihívásait, azonosítani ezen eszközök alkalmazásával járó adatvédelmi és kiberbiztonsági problémákat. Emellett célunk az is, hogy felmérjük, a tanárok és a diákok mennyire tudatosak a biztonsági kérdések terén, hogy milyen eszközök és módszerek alkalmazhatók a biztonság javítására az oktatási folyamatban.

Az MI oktatásban való alkalmazása nem teljesen új keletű jelenség, hiszen már korábbi kutatások is foglalkoztak vele (Garito 1991; Luckin et al. 2016). Azonban a mesterséges intelligencia gyors fejlődése és egyre szélesebb körű alkalmazása új kihívásokat vet fel az oktatási gyakorlatban. Jelenleg még nem áll rendelkezésünkre teljes kép arról, hogy a mesterséges intelligencia milyen mértékben és módon fogja formálni az etika, a méltányosság, valamint az adatbiztonság kritikus kérdéseit (Hamilton 2024). Ezekre a kérdésekre adott válaszok alapvetően befolyásolhatják a technológia hosszú távú fenntarthatóságát és elfogadottságát az oktatásban, különösen a digitális eszközök széles körű elterjedése mellett. Ugyanakkor a mesterséges intelligencia oktatásban való alkalmazásának kritikus elemzése alulreprezentált a témában írt kutatásokban. A meglévő tanulmányok gyakran a technológia előnyeire és hatékonyságára összpontosítanak, miközben a potenciális kockázatok és a negatív következmények kevésbé kerülnek górcső alá. A biztonsági kérdések alapos megértéséhez elengedhetetlen olyan módszerek integrálása, amelyek mélyreható elemzést nyújtanak a kiberbiztonsági kockázatokról és az adatvédelemről. Mivel a diákok személyes adatai és tanulási szokásaik védelme kiemelten fontos, a kutatás releváns témát érint, amely közvetlen hatással van az oktatás minőségére és a tanulók biztonságára. A tanárok és diákok kiberbiztonsági tudatosságának felmérése fontos lépés a digitális írástudás fejlesztésében. Kutatásunkkal szeretnénk rávilágítani, hogy milyen szinten ismerik az érintettek az MI-eszközök biztonsági kihívásait, és milyen intézkedéseket hoznak a kockázatok csökkentésére.

A kutatás során felmérjük az MI-alapú oktatási eszközök közoktatásban való felhasználásának jelenlegi helyzetét, főként a kiberbiztonsági kérdésekre kitérve. Ezen kérdések áttekintésével azonosíthatjuk a biztonsági és adatvédelmi kihívásokat. Felmérést végzünk az ilyen eszközök használatából adódó tudatosság és a biztonsági gyakorlatok elemzésére. Javaslatokat fogalmazunk meg, hogy elősegítsük az MI-eszközök biztonságos és hatékony alkalmazásának lehetőségeit, beleértve a technikai és oktatási megoldásokat is – a középiskolás diákok körében.

A kutatásunk irányát ezen eszközök oktatási környezetben történő alkalmazásának biztonsági vonatkozásaira, az eszközök beépítésének hatékonyságára, valamint a tanárok és diákok tudatosságának és felkészültségének növelésére helyezzük. Fontos, a mesterséges intelligencia alapú technológiai eszközökre támogató, nem helyettesítő eszközként tekintünk, melyek célja a tanár-diák munkájának, valamint a tanulási-tanítási folyamat hatékonyságának javítása. Emellett gyakorlati

megoldásokat is bemutatunk a biztonsági kockázatok csökkentésére, valamint az MI-eszközök felelős és eredményes integrálására az oktatási rendszerbe.

Kulcsszavak: *kiberbiztonság az oktatásban, MI-alapú oktatási eszközök, tanár-diák kiberbiztonsági tudatosság, MI alkalmazások felelős integrálása.*

Felhasznált források:

1. Garito, M. A. (1991). Artificial intelligence in education: evolution of the teaching-learning relationship. British Journal of Educational Technology: Journal of the Council for Educational Technology, 22(1), 41–47. URL: https://doi.org/10.1111/j.1467-8535.1991.tb00050.
2. Luckin, R., Holmes, W., Griffiths, M., & Forcier, L. B. (2016). Intelligence unleashed: An argument for AI in education.
3. Ilana Hamilton (2024): Artificial Intelligence In Education: Teachers' Opinions On AI In The Classroom. URL: https://www.forbes.com/advisor/education/it-and-tech/artificial-intelligence-in-school/

TEMETŐ Ádám
MSc szintű, 1. évfolyamos
középiskolai oktatás (matematika) szakos hallgató,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
SZTOJKA Miroszláv
PhD, docens,
Matematika és Informatika Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

HOGYAN FORMÁLJA A MESTERSÉGES INTELLIGENCIA AZ INFORMÁCIÓBIZTONSÁG JÖVŐJÉT?

A mesterséges intelligencia (MI) rohamos fejlődése átalakítja az információbiztonság területét. Ez a technológia nemcsak új lehetőségeket kínál a kiberbiztonság megerősítésére, hanem kihívásokat is jelent. Az MI alkalmazása az adatvédelem és az adatbiztonság területén forradalmi változásokat hoz, miközben új megközelítéseket tesz szükségessé a hagyományos biztonsági módszerek, mint például a kétfaktoros hitelesítés terén.

A mesterséges intelligencia alapjai

A mesterséges intelligencia (MI) egy olyan számítógépes rendszer, amely képes az emberi intelligenciához hasonló kognitív funkciókat utánozni, mint például a tanulás és a problémamegoldás. Az MI nagy mennyiségű adatot elemez, statisztikai algoritmusokat használ fel összefüggések keresésére, és ezek alapján ad eredményt a felhasználóknak.

A mesterséges intelligenciát három fő típusra oszthatjuk:

Mesterséges keskeny intelligencia (ANI): Ez a jelenleg létező AI-típus, amelyet „gyenge AI”-nak is neveznek. Az ANI egy szűken meghatározott feladatot képes az embernél hatékonyabban elvégezni.

Mesterséges általános intelligencia (AGI): Ez a típus képes lenne minden intellektuális feladatot ellátni, amit egy ember tud. Az AGI-rendszerek tanulhatnak a tapasztalatokból, észlelhetik és előrejelezhetik a mintákat.

Mesterséges szuperintelligencia (ASI): Ez a hipotetikus típus elméletileg képes lenne az embert csaknem minden területen túlszárnyalni, beleértve a tudományos kreativitást, az általános bölcsességet és a társadalmi készségeket is.

A mesterséges intelligencia alapja a gépi tanulás és a mély tanulás elve. A gépi tanulás során a számítógépes rendszerek algoritmusok segítségével mintázatokat azonosítanak az adatokban, amelyek alapján adatmodelleket készítenek és előrejelzéseket végeznek.

A mély tanulás a gépi tanulás egy fejlettebb formája, amely az emberi agy felépítése által inspirált neurális hálózatokat alkalmaz. Ezek a mély neurális hálózatok összetett neurális csomópontokból állnak, és minden egyes válasz újabb kapcsolódó kérdésekhez vezet.

Az MI működéséhez két fő feltétel szükséges:

Nagy mennyiségű adat: A „big data” korában élünk, ahol az élet minden területén adatokat gyűjtenek.

Betanítási technika: Ez jellemzően statisztikai módszerekből áll, és magába foglalja a gépi tanulást, a mélytanulást, a megerősítő tanulást és a természetes nyelvfeldolgozást.

Az MI-rendszerek képesek előrejelzéseket nyújtani vagy a meglévő adatok mintázatán alapuló műveleteket végrehajtani. Tanulni tudnak a hibáikból, így növelve pontosságukat. Egy fejlett mesterséges intelligencia képes az új információkat rendkívül gyorsan és precízen feldolgozni, ami lehetővé teszi a használatát bonyolult helyzetekben, például önvezető autókban, képfelismerő rendszerekben vagy virtuális asszisztensekben.

Az MI használata nagy hatással van a 21. században, társadalmi és gazdasági változásokat hozva, befolyásolva a munkapiacot, egészségügyet, több különböző iparágat, oktatást, és megkönnyítve az információáramlást. Az MI alkalmazása az információbiztonság területén is forradalmi változásokat hoz, új megközelítéseket téve szükségessé olyan hagyományos biztonsági módszerek terén, mint például a kétfaktoros hitelesítés.

Az MI az információbiztonságban

A mesterséges intelligencia (MI) forradalmasítja az információbiztonság területét. Az MI-alapú rendszerek képesek nagy mennyiségű adatot elemezni és értelmezni, ami lehetővé teszi a fenyegetések gyorsabb és hatékonyabb felismerését és kezelését.

Az MI kulcsfontosságú szerepet játszik a kiberfenyegetések felismerésében és megelőzésében. A gépi tanulási algoritmusok képesek elemezni a hálózati forgalmat, azonosítani a szokatlan mintázatokat, és gyorsan reagálni a potenciálisan veszélyes eseményekre. Az MI-rendszerek folyamatosan tanulnak az új adatokból, így lépést tudnak tartani a folyamatosan fejlődő fenyegetésekkel.

Az MI segítségével a biztonsági szakemberek azonosíthatják a szervezeten belül használt összes végpontot, és naprakészen tarthatják azokat a legújabb biztonsági megoldásokkal. Ez csökkenti a támadási felületet, és növeli a rendszer általános biztonságát.

Az anomáliadetektálás az MI egyik legfontosabb alkalmazási területe az információbiztonságban. Ez a technika lehetővé teszi a rendellenes események felismerését a nagy adathalmazokban. Az MI-algoritmusok képesek azonosítani a szokatlan tevékenységeket és viselkedési mintákat, amelyek potenciális biztonsági fenyegetésekre utalhatnak.

Az MI-alapú anomáliadetektálás különösen hatékony a következő területeken:

Hálózati forgalom elemzése: Az MI figyeli a hálózati forgalmat és azonosítja a gyanús mintázatokat, amelyek kibertámadásra utalhatnak.

Felhasználói viselkedés elemzése: Az MI értékeli a felhasználói tevékenységeket és felismeri a szokatlan vagy gyanús viselkedést, ami segíthet az adatszivárgások vagy belső fenyegetések azonosításában.

Rendszerteljesítmény monitorozása: Az MI figyeli a rendszer teljesítményét és azonosítja a rendellenes működést, ami biztonsági problémákra utalhat.

Automatizált védekezés

Az MI nemcsak a fenyegetések felismerésében segít, hanem az automatizált védekezésben is kulcsszerepet játszik. Az MI-rendszerek képesek gyorsan és hatékonyan reagálni a felismert fenyegetésekre, csökkentve ezzel az emberi beavatkozás szükségességét és minimalizálva a potenciális károkat.

Az automatizált védekezés főbb előnyei:

Gyors reagálás: Az MI-rendszerek azonnal képesek válaszolni a felismert fenyegetésekre, ami kritikus fontosságú a kibertámadások elhárításában.

Skálázhatóság: Az MI lehetővé teszi a nagy mennyiségű biztonsági esemény egyidejű kezelését, ami emberi erőforrásokkal nem lenne megvalósítható.

Folyamatos tanulás: Az MI-rendszerek folyamatosan fejlődnek és alkalmazkodnak az új fenyegetésekhez, így a védelem hatékonysága idővel növekszik.

Emberi erőforrások optimalizálása: Az automatizált védekezés lehetővé teszi, hogy a biztonsági szakemberek a komplexebb feladatokra összpontosítsanak.

Az MI használata az információbiztonságban jelentős előrelépést jelent, de fontos megjegyezni, hogy önmagában nem garantál teljes védelmet. Az emberi szakértelem és felügyelet továbbra is elengedhetetlen a hatékony kiberbiztonság fenntartásához. Az MI és az emberi tudás kombinációja nyújthatja a legjobb védelmet a folyamatosan fejlődő kiberfenyegetések ellen.

Kihívások és etikai kérdések

A mesterséges intelligencia (MI) rohamos fejlődése számos kihívást és etikai kérdést vet fel az információbiztonság területén. Ezek a problémák nemcsak a technológia fejlesztőit és felhasználóit érintik, hanem a társadalom egészét is. Az MI alkalmazása az információbiztonságban új lehetőségeket teremt, de egyben új kockázatokat is hordoz magában.

Az adatvédelem az egyik legégetőbb kérdés az MI és az információbiztonság területén. Az MI-rendszerek hatalmas mennyiségű adatot gyűjtenek és elemeznek, amelyek között gyakran találhatók személyes és érzékeny információk. Az adatvédelmi kockázatok között szerepel az adatok jogosulatlan felhasználása, a magánélet megsértése és az adatszivárgás veszélye.

Az Európai Unió Általános Adatvédelmi Rendelete (GDPR) szigorú szabályokat határoz meg az adatkezelésre vonatkozóan. A GDPR előírja, hogy az adatkezelésnek jogszerűnek, tisztességesnek és átláthatónak kell lennie. Az MI-rendszerek fejlesztőinek és üzemeltetőinek biztosítaniuk kell, hogy az adatgyűjtés és -felhasználás megfeleljen ezeknek az elveknek.

Az adattakarékosság elve különösen fontos az MI esetében. Ez azt jelenti, hogy csak a feltétlenül szükséges adatokat szabad gyűjteni és tárolni. Az adatkezelőknek képesnek kell lenniük indokolni, miért van szükségük az adott személyes adatokra.

Az MI-rendszerek által hozott döntések átláthatósága szintén kulcsfontosságú kérdés. Az érintetteknek joguk van tájékoztatást kapni arról, ha egy döntés kizárólag automatizált adatkezelésen alapul, és ez rájuk nézve jelentős hatással bír.

Az átláthatóság az MI-rendszerek esetében különösen nagy kihívást jelent. Az MI algoritmusai gyakran olyan összetettek, hogy még a fejlesztőik sem tudják pontosan megmagyarázni, hogyan jutnak el egy adott döntéshez. Ez a „fekete doboz" probléma komoly etikai kérdéseket vet fel, különösen olyan területeken, ahol az MI-rendszerek döntései jelentős hatással lehetnek az emberek életére.

A GDPR előírja, hogy a tájékoztatásnak tömörnek, átláthatónak, érthetőnek és könnyen hozzáférhetőnek kell lennie. Ez különösen nehéz feladat az MI esetében, ahol a döntéshozatali folyamatok gyakran rendkívül összetettek.

Az átláthatóság növelése érdekében a fejlesztőknek olyan módszereket kell kidolgozniuk, amelyek lehetővé teszik az MI-rendszerek döntéseinek magyarázatát és értelmezését. Ez nemcsak jogi követelmény, hanem a felhasználók bizalmának megnyerése szempontjából is kulcsfontosságú.

Az MI-rendszerek használata során felmerülő károk esetén a felelősség kérdése komoly kihívást jelent. Ki a felelős, ha egy MI-rendszer hibás döntést hoz, és ez kárt okoz? A fejlesztő, az üzemeltető, vagy maga a rendszer?

Az Európai Parlament állásfoglalása szerint az MI-rendszerek üzemeltetőjét terheli a felelősség, mivel ő kontrollálja a rendszerrel kapcsolatos kockázatokat. Ez hasonló a veszélyes üzemi felelősséghez, ahol az üzembentartó felel a károkért.

Az állásfoglalás javasolja egy objektív felelősségi rendszer kialakítását a magas kockázatú, autonóm MI-rendszerek esetében. Ez azt jelentené, hogy az üzemeltető minden esetben felelős lenne a károkért, függetlenül attól, hogy bizonyítható-e a hibája.

A felelősség kérdése különösen összetett olyan esetekben, amikor az MI-rendszer döntését külső beavatkozás, például hackertámadás befolyásolja. Ilyenkor nehéz megállapítani, hogy ki a felelős a bekövetkezett kárért.

Az MI-rendszerek fejlesztőinek és üzemeltetőinek ezért különös figyelmet kell fordítaniuk a biztonsági intézkedésekre és a kockázatkezelésre. Az elszámoltathatóság elve szerint képesnek kell lenniük bizonyítani, hogy minden szükséges lépést megtettek a károk megelőzése érdekében.

Az információbiztonság területén az MI alkalmazása számos előnnyel jár, de egyben új kihívásokat is teremt. Az adatvédelem, az átláthatóság és a felelősség kérdései olyan komplex problémákat vetnek fel, amelyek megoldása elengedhetetlen az MI etikus és biztonságos használatához. A jövőben várhatóan további szabályozásokra és iránymutatásokra lesz szükség ezeken a területeken, hogy az MI-rendszerek használata összhangban legyen az alapvető emberi jogokkal és etikai normákkal.

Következtetés: A mesterséges intelligencia egyre nagyobb szerepet játszik az információbiztonság területén, és jelentős hatást gyakorol a kibervédelmi stratégiákra. Az MI-alapú rendszerek képessége a nagy mennyiségű adat gyors elemzésére és a fenyegetések valós idejű felismerésére új lehetőségeket teremt a biztonság megerősítésére. Ugyanakkor ezek a fejlett technológiák új kihívásokat is hoznak magukkal, különösen az adatvédelem, az átláthatóság és a felelősség terén.

Ahogy az MI továbbra is fejlődik, kulcsfontosságú lesz megtalálni az egyensúlyt a technológia előnyeinek kihasználása és a potenciális kockázatok kezelése között. Ez azt jelenti, hogy folyamatos párbeszédre és együttműködésre van szükség a technológiai szakemberek, jogalkotók és etikai szakértők között, hogy olyan keretrendszereket alakítsanak ki, amelyek biztosítják az MI etikus és biztonságos használatát az információbiztonság területén. A jövőben az MI és az emberi szakértelem

együttes alkalmazása lehet a kulcs a hatékony kibervédelemhez és a digitális világ biztonságának megőrzéséhez.

Felhasznált források:

1. Nguyen, Phuoc Dai & Rajnai, Zoltan. (2019). The obstacles of autonomous cars before taking the wheel in the future. 155.
2. BARTA, Gergő. Mesterséges intelligencia módszerek alkalmazása az informatikai rendszerek biztonsági auditjában. 2021. PhD Thesis. Magyar Agrár- és Élettudományi Egyetem.
3. CSABA, Kollár. A mesterséges intelligencia kapcsolata a humán biztonsággal. Nemzet-biztonsági szemle, 2018, 6.1: 5–23-5–23.
4. https://www.horvath-partners.com/hu/horvath-akademia/webinariumok/az-eu-szabalyozasatol-a-vallalati-sikerekig-utmutato-a-mesterseges-intelligencia-ai-strategiai-bevezetesehez (Megtekintés dátuma: 2024.09.26.)

BOROS József
BSc szintű, 4. évfolyamos
középiskolai oktatás (matematika) szakos hallgató,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
KUCSINKA Katalin
Phd, docens, tanszékvezető,
Matematika és Informatika Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

A MESTERSÉGES INTELLIGENCIA ÉS A FŐISKOLÁS HALLGATÓK MATEMATIKAI KOMPETENCIATESZTEK EREDMÉNYEINEK ÖSSZEHASONLÍTÁSA

A mesterséges intelligencia egyre jelentősebb szerepet kap az információbiztonság területén, mivel képes a nagy mennyiségű adat elemzésére, amely segíti a fenyegetések azonosítását és megelőzését. Az AI matematikai kompetenciáinak fejlettsége alapvető elemei az információbiztonság területen történő előre lepéseknek. Ezek a módszerek lehetővé teszik a rendszerek számára, hogy azonosítsák a szokatlan mintázattokat és a potenciális fenyegetéseket, így proaktívan védekezhetnek a kibertámadások ellen. Ezért lehet érdekes megvizsgálni, hogy milyen szintre tehető a mesterséges intelligencia matematikai kompetenciája, korábbi tanulmányok már foglalkoztak a 15 éves tanulók és az AI matematikai kompetenciáinak összehasonlításával a PISA-eredmények alapján [3].

A munkánk célja megvizsgálni hogyan teljesítenek a mestereséges intelligencia különböző nagy nyelvi modelljei a diákok által megírt teszteken, illetve, hogy felfedezhető-e különbség a felsőoktatásba belépő hallgatók és az AI-eredményei között.

A tanulmányhoz a II. Rákóczi Ferenc Főiskola első éves hallgatóinak a 2023/2024-es tanév során megírt kompetenciamérésen elért eredményeit és feladatait használtuk. A feladatsor összeállítása korábbi kutatási eredmények figyelembe vételével történt, melyről többek között [1,2] irodalomban olvashatunk. A felmérésben 135 hallgató vett részt, az ő válaszaikat dekódoltuk, rendeztük, így minden hallgatóhoz tudtunk rendelni egy pontszámot. Majd a következő lépésben ezeket a feladatokat kiadtuk különböző, szabad hozzáférésben elérhető, nagy nyelvi modelleknek, hogy oldják meg azokat, a kapott válaszokat, a hallgatók eredményeihez hasonlóan pontoztuk. A kísérletben Claude, Gemini, Chat GPT alkalmazásokat vizsgáltuk.

Azt kaptuk, hogy az említett nagy nyelvi modulok közül Chat GPT képes a legeredményesebb az említett típusú feladatok megoldásában. A főiskolai oktatásba belépő hallgatók eredményeivel való összehasonlítás alapján azt kaptuk, hogy míg az Alakzatok tájékozódás témakörben a hallgatók átlagosan jobb eredményt értek el, mint bármelyik AI alkalmazás, addig az többi témakörben a diákok szerzetek alacsonyabb pontszámokat.

A következő lépésben összehasonlítottuk a matematika szakos hallgatók és az AI-eredményeit. Itt már azt az eredményt kaptuk, hogy az ember teljesít jobban, mint a gép.

Tehát összességében elmondhatjuk, hogy jelen állás szerint, bár az AI nagy nyelvi modelljei közelítik az emberi teljesítményt a matematikai kompetencia terén, de még nem érte el a tudományág irányába érdeklődést mutató személyek szintjét

Felhasznált források:

1. Belinszki Bálint, Palincsár Ildikó, Szepesi Ildikó, Szipőcsné Krolopp Judit, Takácsné Kárász Judit: Országos kompetenciamérés 2021 Feladatok és jellemzőik matematika 10. évfolyam/Oktatási Hivatal Köznevelési Mérés Értékelési Osztály/ Budapest, 2020, 191 o.

2. Krolopp, Judit, & Vári, Péter. Egy nemzetközi felmérés főbb eredményei (TIMSS). Online document. Download date: 2024.09.20. URL: https://ofi.oh.gov.hu/en/egy-nemzetkozi-felmeres-fobb-eredmenyei-timss

3. OECD: Putting AI to the test: How does the performance of GPT and 15-year-old students in PISA compare? OECD Education Spotlights, No. 6, OECD Publishing, Paris, 2023 https://doi.org/10.1787/2c297e0b-en

Юрій БІРКОВИЧ
студент 4 курсу спеціальності «Інформаційні системи та технології»
Ужгородський національний університет
***Науковий керівник* – Василь КУТ**
к. т. н., доцент,
завідувач кафедри інформатики
та фізико-математичних дисциплін
Ужгородський національний університет

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ПЕРСПЕКТИВА РОЗВИТКУ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Штучний інтелект (ШІ) є одним з головних каталізаторів стрімкого розвитку інформаційних систем та ефективної обробки значних масивів даних. З розвитком заходів щодо захисту даних, з'явилося багато зловмисного програмного забезпечення (ПЗ), яке здатне динамічно змінюватися, роблячи себе важкою ціллю для традиційних сигнатурних методів виявлення шкідливого ПЗ. Саме в цьому випадку важливу роль може відіграти машинне навчання та ШІ, даючи можливість прогнозувати та адаптуватися до кіберзагроз, що еволюціонували [1].

Метою доповіді є демонстрація основних аспектів розвитку ШІ в розрізі антивірусного програмного забезпечення, а також аналіз шляхів використання ШІ для завчасного виявлення та знешкодження модифікованого шкідливого програмного забезпечення.

Якщо розглянути відомі статті по даній тематиці, то можна зазначити, що в них акцент спрямований більш на теоретичну складову питання, без конкретних прикладів, які можуть допомогти проілюструвати та підтвердити написане [2].

Традиційне антивірусне ПЗ працює на основі сигнатурного методу, сутність якого полягає в тому, що створюється набір певних рис, характерних для конкретного сімейства вірусів, та проводиться порівняння з використанням цих сигнатур. Даний метод є ефективним для виявлення та знешкодження добре відомих вірусів, але не для модифікованих або нових. Серед подібних шляхів еволюції кіберзагроз можна виділити наступні: поліморфне шкідливе ПЗ, яке може динамічно змінювати свою сигнатуру, ускладнюючи розпізнавання; експлойти нульового дня, які націлені на атаку ще не виявлених вразливостей, є особливо небезпечними; соціальна інженерія в свою чергу націлена на маніпуляцію людьми з метою розголошення конфіденційної інформації. Як результат виникає потреба в більш досконалих засобах захисту інформації, оскільки стандартний сигнатурний метод є малоефективним для виявлення подібних динамічних загроз. В таких випадках доцільно використовувати метод евристичного аналізу. Евристичний аналіз – це метод який використовується для виявлення раніше невідомого шкідливого ПЗ на основі часткового збігу. Саме в цьому методі, виходячи з його специфіки, доцільніше всього використовувати ШІ для аналізу великих обсягів даних. Але на практиці можна спостерігати не таку високу ефективність подібного підходу. Пов'язано це з великою кількістю хибних спрацювань та відносно низькою точністю виявлення загроз. Поруч з цим є також можливі випадки коли зловмисники спонукають ШІ до неправильного прогнозування, що в свою чергу може виявитися перевагою для кіберзагроз. Для вирішення цих проблем рекомендується використовувати точніше налаштовані моделі ШІ. Також не потрібно забувати, що в основі більшості моделей ШІ стоїть машинне навчання, яке в свою чергу потребує масивів даних, щоб мати змогу ефективно працювати. Тому такого роду підхід виявиться недієздатним проти принципово нових вірусів або проти експлойтів нульового дня. Хоча, зараз тенденції спонукають компанії до розробки ШІ, який зможе швидко та достатньо ефективно виявляти та знешкоджувати шкідливе ПЗ. Однією з таких компаній є Darktrace – лідер на глобальному ринку ШІ для кіберзахисту. Революційність їхнього ШІ полягає в тому, що разом з аналізом попередніх атак, ШІ також вивчає систему вашого підприємства, шукає паттерни та закономірності і в разі навіть мінімальних відхилень, досить точно може вирізняти причини, класифікувати їх, групувати та ізолювати. Даний підхід називається кластеризацією

та використовується в некерованому машинному навчанні. Може здатися, що такий метод є досить неконфіденційним, оскільки ШІ має доступ до всіх пристроїв вашої системи, та значної кількості даних, але як зазначають розробники, дані зберігаються та оброблюються локально, на відміну від інших ШІ, які відсилають зібрані дані в публічне хмарне сховище. Подібний підхід вже зараз є одним з головних векторів розвитку антивірусного ПЗ й для інших учасників ринку [3,4].

Як висновок, можна зазначити, що незважаючи на потенційні проблеми ШІ, його імплементація в антивірусне ПЗ є закономірним кроком розвитку традиційних засобів кібербезпеки, які стикаються із значними викликами. Вже зараз ШІ активно використовується на ринку такими компаніями як: Cylance, Darktrace та інші [5]. Вони беруть участь в розробці та удосконаленні моделей, які зможуть прогнозувати та адаптуватися до нових динамічних загроз.

Список використаних джерел

1. How AI Detects Computer Viruses – [Електронний ресурс] – Режим доступу: https://www.linkedin.com/pulse/how-ai-detects-computer-viruses-dovetechnologies/
2. Застосування штучного інтелекту для виявлення та реагування на кіберзагрози – [Електронний ресурс] – Режим доступу: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf?sequence=3&isAllowed=y
3. Anthony Lawrence Paul (2024). The Role of Artificial Intelligence in Enhancing Data Security – [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/381004546_The_Role_of_Artificial_Intelligence_in_Enhancing_Data_Security
4. Основні напрями застосування технологій штучного інтелекту у кібербезпеці – [Електронний ресурс] – Режим доступу: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf?sequence=3&isAllowed=y
5. Built for novel threats: Cyber AI – [Електронний ресурс] Режим доступу: https://darktrace.com/cyber-ai

Maryna VASYLYK
Candidate of Pedagogical Sciences,
Associate Professor of the Department of Foreign Languages
Vasyl Stefanyk Precarpathian
National University Ukraine

PECULIARITIES OF USING ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

The ever-increasing complexity of technology, which is intensified by widespread dependence on the Internet, creates a favourable environment for the emergence of new cyber threats. In this regard, the integration of advanced artificial intelligence (AI) into various aspects of human activity is becoming crucial.

In the field of computer science, artificial intelligence refers to machines endowed with the ability to perform tasks that traditionally require human intelligence. Artificial intelligence algorithms demonstrate the ability to identify basic patterns in huge amounts of data, thereby increasing their operational efficiency over time [1].

It is worth noting that in the field of cybersecurity, artificial intelligence is becoming a powerful tool for strengthening defences against ever-changing threats. Its ability to quickly analyse complex patterns in huge amounts of data allows for effective detection of anomalies and identification of potential breaches. Such predictive skills minimise the impact of cyberattacks.

In addition, the emergence of neural network models based on the principles of the human brain has significantly expanded the possibilities of cybersecurity. These models demonstrate exceptional learning abilities, adapting to the changing threat environment and improving their strategies over time. The combination of AI and machine learning methodologies has accelerated the paradigm shift in proactive threat detection and neutralisation.

IT professionals in the cybersecurity field mostly use artificial intelligence to improve complex algorithms that are specifically designed to detect and mitigate the effects of cyberattacks [2]. These algorithms engage in a comprehensive structural analysis of large amounts of data, thereby identifying discernible patterns that signal existing or potential threats. Operating at speeds and on a scale beyond human capabilities, AI systems quickly identify both potential and actual cyber threats, facilitating timely response and significantly reducing the risks inherent in cyber attacks and their consequences.

Although the capabilities of artificial intelligence in detecting cybersecurity threats are well known, its potential goes far beyond this area. AI allows for the automation of routine cybersecurity tasks, greatly simplifying the work of Internet technology professionals at all levels. The algorithm of an AI-based cyber threat protection system should work autonomously and perform the following actions

- scan networks for vulnerabilities with high accuracy;
- detect new threats in real time;

Such a proactive approach goes beyond mere detection, it nips security breaches in the bud.

All of the above underscores the importance of developing means and methods of protecting against cyber threats using AI, as well as training company employees and PC users in security. After all, with the emergence of AI as a tool for hackers, cybersecurity has become even more challenging.

References

1. V. Bohomia, A. Hudz Artificial Intelligence: Current State and Prospects for Application. *Modern Information Technologies in the Field of Security and Defence.* Vol. 46, No. 1 (2023). PP. 13-17.
2. Bostrom N. Superintelligence: ways, dangers, strategies. *Kyiv: Nash format,* 2020. 452 p.

Олександр ГУМЕННИЙ
кандидат педагогічних наук, завідувач лабораторії електронних навчальних ресурсів,
Інститут професійної освіти НАПН України

КОНЦЕПТУАЛЬНА МОДЕЛЬ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМУ КІБЕРЗАХИСТУ НАВЧАЛЬНОЇ ЦИФРОВОЇ ПЛАТФОРМИ

Постановка наукової проблеми. У сучасному світі зростання залежності від цифрових платформ у професійній освіті викликає необхідність підвищення рівня захисту даних від кіберзагроз.

Метою дослідження є розробка концептуальної моделі інтеграції штучного інтелекту у систему кіберзахисту навчальної цифрової платформи. Актуальність цієї теми зумовлена необхідністю підвищення ефективності кіберзахисту освітніх платформ, що використовуються для професійної підготовки робітників, і відсутністю ефективних механізмів, які б могли оперативно реагувати на кіберзагрози.

Наукова новизна роботи полягає в інтеграції адаптивної системи кіберзахисту на основі штучного інтелекту для навчальних цифрових платформ, яка не лише реагує на відомі загрози, але й має здатність до самонавчання та адаптації до нових атак. Порівняно з дослідженнями Bilge L. та Dumitraş T. (2012), що акцентують увагу на обмеженнях традиційних методів виявлення атак «нульового дня», наша система забезпечує більш проактивний підхід, запобігаючи як відомим, так і новим загрозам завдяки машинному навчанню.

Публікації ENISA (2020) висвітлюють загальні питання безпеки ШІ та його використання в цифрових екосистемах, однак наша робота зосереджується на специфічному застосуванні в освітніх платформах для професійної підготовки, що додає практичну цінність у цій галузі. У порівнянні з дослідженнями Malatras A. та Dede G., наша система відрізняється тим, що її адаптивний характер уможливлює їй оперативно реагувати на змінюваний ландшафт кіберзагроз в освітньому середовищі.

Таким чином, робота пропонує унікальне рішення для кіберзахисту освітніх платформ, яке поєднує в собі передові алгоритми ШІ та механізми самонавчання для підвищення ефективності виявлення і нейтралізації новітніх загроз.

Короткий виклад поставленого завдання. Розробка концептуальної моделі включає аналіз сучасних підходів до кіберзахисту освітніх платформ, визначення основних кіберзагроз та розробку алгоритмів штучного інтелекту для їх виявлення й усунення. Особливу увагу було приділено адаптивним системам, що можуть навчатись на основі нових даних і вдосконалювати свої функції у процесі роботи.

Висновки. Основні результати дослідження показують, що інтеграція штучного інтелекту у систему кіберзахисту навчальної цифрової платформи забезпечує ефективніший захист від новітніх кібератак. Це відкриває можливості для більш безпечної та стабільної роботи платформ, що використовуються для професійної підготовки робітників у галузі машинобудування.

Список використаних джерел

1. Bilge, L., & Dumitraş, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, 833–844. https://doi.org/10.1145/2382196.2382284
2. European Union Agency for Cybersecurity (ENISA). (2020). *AI cybersecurity challenges: Threat landscape for artificial intelligence*. Publications Office of the European Union. https://doi.org/10.2824/238222
3. Malatras, A., & Dede, G. (2020). *Artificial intelligence in cybersecurity: Threat landscape and challenges*. European Union Agency for Cybersecurity (ENISA). https://op.europa.eu/en/publication-detail/-/publication/7b988d77-75e8-11ea-a07e-01aa75ed71a1

Олена ГУРСЬКА
кандидат педагогічних наук, доцент кафедри іноземних мов професійного спрямування
Антон ЛУЧИЦЬКИЙ
студент 2 курсу спеціальності «Кібербезпека та захист інформації», Національний авіаційний університет

ШТУЧНИЙ ІНТЕЛЕКТ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ

В останні роки стрімке зростання кількості кібератак змусило багато організацій і урядів по всьому світу звернути особливу увагу на питання кібербезпеки. Одним з найважливіших інструментів у цій боротьбі став штучний інтелект (ШІ), який дозволяє створювати нові рішення для захисту інформаційних систем. Не зважаючи на актуальність означеної проблеми, аналіз останніх публікацій [1, 2] засвідчив, що питання використання ШІ в кібербезпеці вивчене ще недостатньо. Таким чином, наша доповідь має на *меті* дослідити сучасні перспективи та виклики у забезпеченні кібербезпеки.

Однією з ключових переваг ШІ є можливість аналізувати величезні обсяги даних і оперативно виявляти підозрілі дії або аномалії, які можуть свідчити про кібератаки. У звичайних умовах для такого аналізу було б потрібно багато часу і зусиль з боку людей, але ШІ може виконувати це автоматично і в реальному часі, а системи на основі машинного навчання можуть "вчитися" на вже відомих випадках кібератак і прогнозувати нові загрози.

Ефективність використання ШІ можна побачити на прикладі компанії Darktrace, яка застосовує алгоритми штучного інтелекту для моніторингу корпоративних мереж. Їхні системи використовують машинне навчання для побудови моделей нормальної поведінки мережі та виявлення відхилень, що можуть бути ознаками кібератак.

Водночас, з використанням ШІ у кібербезпеці пов’язано чимало викликів. Наприклад, важливо враховувати, що навіть найсучасніші системи можуть робити помилки або виявляти надмірну активність там, де її немає. Це може викликати непотрібні тривоги або пропускати реальні загрози. Також виникає питання довіри до систем, де рішення ухвалює ШІ, а не людина. Як зазначає експерт з кібербезпеки Джон Сміт: "Ми повинні пам'ятати, що штучний інтелект – це лише інструмент, і його ефективність залежить від того, як ми навчимо його й інтегруємо в наші системи. Найбільший ризик полягає не в технології, а в тому, як ми її використовуємо".

Основними *результатами* дослідження є виявлення перспектив використання ШІ у галузі кібербезпеки. Очікується, що в майбутньому ці системи стануть ще більш ефективними і здатними не лише швидко й автоматично реагувати на загрози без людського втручання, але й адаптуватися до змінних умов кіберпростору та самостійно навчатися на основі нових даних. Проте важливо приділяти увагу вирішенню етичних питань і гарантувати, що технології ШІ застосовуються відповідально та без шкоди.

Висновок. Таким чином, штучний інтелект стає важливим інструментом у сфері кібербезпеки, допомагаючи швидше й точніше виявляти загрози та автоматизувати процеси захисту. Однак його ефективність залежить від належної інтеграції з традиційними методами, дотримання етичних норм та постійного вдосконалення технологій. Виклики, пов'язані з довірою до ШІ та можливістю його використання зловмисниками, потребують особливої уваги. Тож, незважаючи на великий потенціал, штучний інтелект має бути доповненням до існуючих підходів, а не їхньою заміною.

Список використаних джерел:

1. Ящик О. Б., Симонов В. В., Іваненко Р. О. Забезпечення кібербезпеки в еру штучного інтелекту: аналіз технологічних підходів та стратегій для захисту інформації. *Бізнес інформ. 2024.* № 1. С.81-86. DOI: Org/10.32983/2222-4459-2024-1-81-86
2. Welukar, J. N., & Bajoria, G. P. (2021). Artificial Intelligence in Cyber Security-AReview. *International Journal of Scientific Research in Science and Technology*. 2021. P. 488–491.

Олександр ДУБІВ
аспірант кафедри програмного забезпечення систем
Ужгородський національний університет

РЕАЛІЗАЦІЯ БАЗОВОЇ КІБЕРБЕЗПЕКИ У ГЕНОМНИХ ВЕБ-ДОДАТКАХ: ШИФРУВАННЯ, БЕЗПЕКА ДАНИХ ТА ЗАХИСТ ВІД ВТРУЧАННЯ НА ПРИКЛАДІ ІСНУЮЧОГО ВЕБ-ПРОЄКТУ

У сучасному цифровому середовищі безпека даних стає однією з ключових вимог для будь-яких веб-додатків, що обробляють особливо чутливу інформацію, зокрема геномні та медичні дані. Незважаючи на значні переваги новітніх технологій у галузі біоінформатики, вони також відкривають нові можливості для потенційних загроз, зокрема втручання в конфіденційність, цілісність, доступність та автентичність даних. Останніми роками сектор охорони здоров'я перетворився на одну з пріоритетних цілей для зловмисників: щорічно з 2020 року викрадається понад 29 мільйонів медичних записів. Особливо під час пандемії значно зросла кількість атак, коли пацієнти масово перейшли до онлайн-платформ [1]. Це сигналізує про нагальну потребу у впровадженні багаторівневих стратегій захисту для забезпечення безпеки таких систем.

Розробники веб-додатків повинні передбачати і впроваджувати комплексний захист чутливих даних, що охоплює: безпеку мережевої інфраструктури, анонімізацію та захист персональних даних, використання кращих стандартів і практик проектування і написання програмного коду, запобігання XSS-атакам та SQL-ін'єкціям, захист від автоматизованих атак (ботів), моніторинг та управління ризиками та ін.

Автором розроблено робочий прототип спеціалізованої інформаційної системи дослідження геному української популяції з прив'язкою до місцевості, що можна було б відносно легко вбудувати у новостворені або існуючі онлайн-ресурси заради представлення результатів геномних наукових досліджень. Для виконання поставленої мети було розроблено модуль-плагін для CMS WordPress під назвою "Genes-UA". Поточна версія плагіну складається з трьох основних підсистем: "Індивідуальні звіти", "Проектний звіт" та "Геоінформаційний звіт". Веб-додаток вже успішно застосовується та доступний в мережі Інтернет, тому у межах даної роботи розкриємо практичні заходи і техніки що були використані для підвищення його безпеки і захисту чутливих даних.

Безпека мережевої інфраструктури. Протокол HTTPS (HyperText Transfer Protocol Secure) є стандартом де-факто для веб-додатків, що включають обробку форм, автентифікацію та управління доступом, особливо коли йдеться про роботу з чутливими даними, такими як індивідуальні геномні профілі. HTTPS є розширенням стандартного HTTP, що використовує сертифікати SSL/TLS для шифрування всього трафіку між клієнтським браузером і сервером. Цей протокол гарантує, що дані, що передаються між користувачем і веб-додатком, захищені від перехоплення, модифікацій або витоку внаслідок атак типу «man-in-the-middle». Шифрування трафіку також забезпечує додаткову безпеку при передачі анонімізованих даних, що є важливим для підтримки високих стандартів конфіденційності у нашій системі. HTTPS забезпечує збереження цілісності даних під час їх транспортування, а також сприяє побудові довіри серед учасників клінічного дослідження, які отримують доступ до своїх генетичних даних через особисті кабінети.

Анонімізація та захист персональних даних. У проекті "Genes-UA" реалізовано підхід до мінімізації збору та збереження персональних даних, що суттєво знижує ризик їх витоку, ідентифікації даних та прив'язки до конкретної особи та використання зловмисниками.

Задачею підсистеми “Індивідуальні звіти” - є персоніфікований доступ до геномних профілів більш як 6000 учасників проєкту. У базі даних веб-системи не зберігаються прізвища, адреси чи контактні дані учасників, що унеможливлює встановлення зв’язку геномного профілю з конкретною особою. Єдине, що присутнє у таблиці з ідентифікаційних даних - це ім’я учасника, виключно для персоніфікації повідомлень.

Для доступу до персональних звітів ми впровадили систему, яка поєднує два фактори: дату народження та одноразовий унікальний 8-значний число-буквений код, що окремо надсилається користувачу через безпечний канал (електронна пошта чи sms-розсилка на контактні дані, вказані в анкеті). Ці два параметри шифруються та хешуються, і саме обчислений хеш на формі входу в особистий кабінет користувача виступає ідентифікатором людини, що гарантує, навіть у разі компрометації бази даних, неможливість зловмиснику пов’язати ці дані з конкретними особами. Застосування додаткового шифрування таблиць профілів БД з використанням хешу як індивідуального ключа запобігає можливості прямого зчитування або відновлення оригінальних значень.

Такий підхід забезпечує високий рівень захисту інформації від доступу сторонніх осіб, навіть якщо фізично доступ до бази буде отримано. Ця технологія забезпечує власнику унікального коду за датою народження отримання доступу до свого звіту, що підвищує загальну безпеку системи.

Безпечне проєктування програмного забезпечення. Безпечне проєктування програмного забезпечення є ключовим аспектом у захисті веб-додатків від різних видів атак, зокрема XSS (міжсайтовий скриптинг) та SQL-ін'єкцій. Для підвищення безпеки веб-додатку ми широко використовуємо вбудовані функції фреймворку WordPress, що направлені на вирішення питань кібербезпеки, таких як wp_nonce_field і wp_verify_nonce, які запобігають CSRF (міжсайтовим підробкам запитів). Для захисту від XSS-атак ми використовуємо функції очищення та фільтрації вхідних даних (esc_html(), esc_attr() та sanitize_text_field(), що унеможливлює виконання шкідливого коду у браузері користувача. Для запобігання SQL-ін'єкції, які можуть призвести до несанкціонованого доступу до бази даних, використовується підготовка запитів (prepared SQL statements) у всіх взаємодіях із базою даних. Це дозволяє гарантувати, що введені користувачем дані не можуть змінити структуру SQL-запиту та виконати небажані дії, тим самим знижуючи ризик SQL-ін'єкцій до мінімуму.

Захист від автоматизованих атак. Такі атаки можуть здійснюватися ботами для отримання несанкціонованого доступу до системи або для сканування вразливостей. У нашому додатку реалізована інтеграція з reCAPTCHA v3, яка ефективно розпізнає та блокує ботів. ReCAPTCHA дозволяє визначати чи є користувач людиною без потреби в додаткових діях з боку користувача, завдяки аналізу поведінкових патернів [2]. Це суттєво знижує ризик доступу ботів до обмежених ресурсів та захищає систему від спроб злому або перевантаження.

У нашому дослідженні продемонстровано комплексний підхід до забезпечення кібербезпеки в рамках веб-додатка для обробки геномних даних. Основні впроваджені механізми безпеки, такі як шифрування трафіку за допомогою HTTPS, анонімізоване зберігання персональних даних із використанням хешування, шифрування даних, а також застосування reCAPTCHA для захисту від автоматизованих атак, є стандартом де-факто для захисту чутливої інформації в сучасних системах.

Безумовно, впровадження принципів безпечного програмування дозволяє запобігти вразливостям, що можуть виникати через атаки типу XSS та SQL-ін'єкції. Проте, для збереження актуальності заходів безпеки, необхідно постійно проводити аудит системи, оперативно реагувати на нові загрози та оновлювати захисні механізми.

Для покращення рівня безпеки проєкту можна впровадити наступні відсутні наразі додаткові заходи: двофакторна аутентифікація (2FA), регулярне оновлення та моніторинг вразливостей (особливо слабкого місця - CMS WordPress), інтеграція з сервісами на кшталт Cloudflare для захисту від DDoS-атак, які можуть порушити роботу сайту.

Список використаних джерел

1. Alarming Cybersecurity Facts and Statistics. November 10, 2022 / Cayley Wetzig, Head of Marketing Communications https://thrivedx.com/resources/article/cyber-security-facts-statistics.
2. Google reCAPTCHA / https://www.google.com/recaptcha/about/.
3. Ankur Shukla, Basel Katt, Livinus Obiora Nweke, Prosper Kandabongee Yeng, Goitom Kahsay Weldehawaryat I am running a few minutes late; my previous meeting is running over. System security assurance: A systematic literature review \Computer Science Review, Volume 45, 2022, 100496, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2022.100496, https://www.sciencedirect.com/science/article/pii/S1574013722000338.
4. Fahad A. Alzahrani, / Estimating Security Risk of Healthcare Web Applications: A Design Perspective, / Computers, Materials and Continua, Volume 67, Issue 1, 2020, Pages 187-209, ISSN 1546-2218, https://doi.org/10.32604/cmc.2021.014007, https://www.sciencedirect.com/science/article/pii/S1546221820001551.

Антон ДІВИНЕЦЬ
студент 4 курсу спеціальності «Інформаційні системи та технології»
***Науковий керівник* – Наталія ШУМИЛО**
старший викладач кафедри інформатики
та фізико-математичних дисциплін,
Ужгородський національний університет

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Штучний інтелект (ШІ) стає ключовим елементом сучасної кібербезпеки, особливо у контексті захисту критичної інфраструктури, такої як: енергетичні системи, транспортні мережі, водопостачання та фінансові структури. В умовах зростання складності та кількості кібератак, традиційні методи захисту виявляються недостатніми для своєчасного виявлення та реагування на нові загрози. Використання ШІ для кіберзахисту надає можливість автоматизувати процеси моніторингу та аналізу великих обсягів даних, які дозволяють оперативно виявляти аномалії, прогнозувати кіберзагрози і блокувати атаки на початкових етапах.

Одним із ключових напрямків використання ШІ у кіберзахисті є виявлення аномалій у системах критичної інфраструктури. Завдяки машинному навчанню, алгоритми можуть "вивчати" нормальну поведінку систем і виявляти відхилення, які можуть свідчити про потенційну кібератаку. Наприклад, компанія Darktrace, яка спеціалізується на кібербезпеці, використовує методи ШІ для аналізу трафіку в мережах своїх клієнтів.[1]

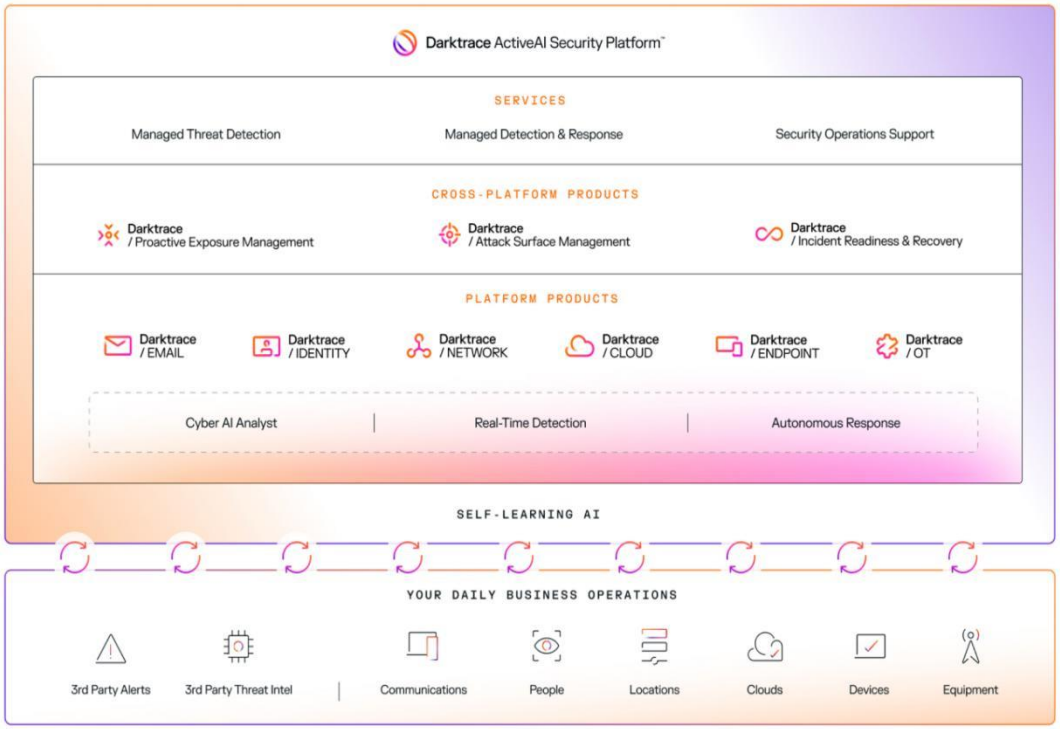


Рис. 1 Платформа захисту з використанням методи ШІ компанії Darktrace

Дана платформа здатна самостійно розпізнавати відхилення у поведінці мережі та блокувати підозрілі дії в режимі реального часу. Це дозволяє виявляти навіть ті атаки, які ще не мають відомих шаблонів або сигнатур, що є критично важливим для захисту від нових загроз, таких як “атаки нульового дня”. Також дана платформа здатна працювати автономно, а саме автоматично визначає підозрілу активність та вживати протоколи захисту для екосистеми структури.

Інший приклад застосування ШІ — це автоматизація процесів реагування на інциденти. Використання алгоритмів ШІ для управління кіберінцидентами значно зменшує час реакції на загрозу. Платформа, така як IBM QRadar, використовують машинне навчання для автоматизації процесів аналізу інцидентів та генерування рекомендацій для швидкого вирішення проблем. Це особливо важливо для захисту критичних систем, де навіть короткочасний збій може мати катастрофічні наслідки, наприклад, у сфері енергопостачання чи водопостачання.[2]

Енергетичний сектор є одним із найвразливіших до кібератак, і приклади інцидентів у цій сфері демонструють, наскільки важливо інтегрувати ШІ в системи безпеки. Станом на 2021-2023 роки країна-агрессор проводить дуже багато кібератак, що місяця кількість атак варіюється, проте можна чітко зазначити, що імплементування ШІ могло би зменшити їхню кількість та збільшити ефективність роботи системи захисту.

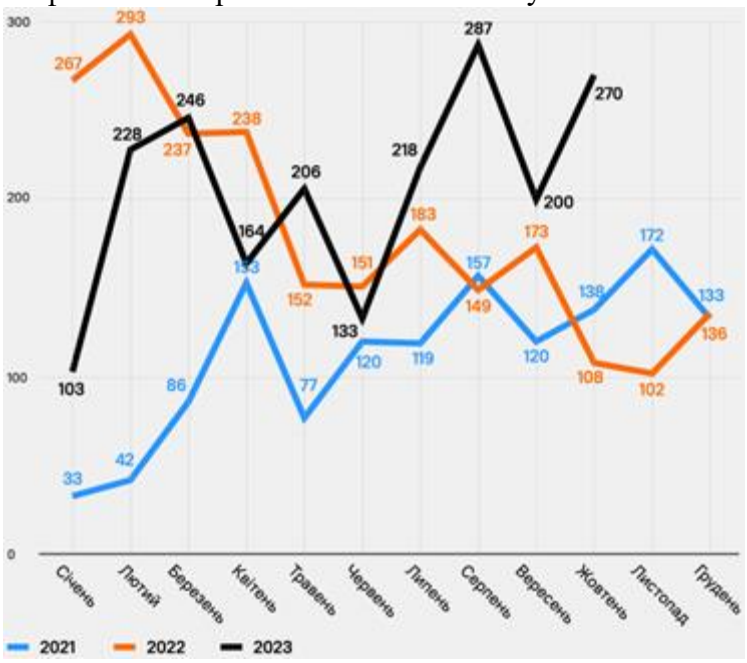


Рис. 2 Зображення графіку кібератак країни агресора у 2021-2023 роках [3]

Фінансові інституції також активно впроваджують ШІ для забезпечення кібербезпеки своїх систем. Наприклад, американська компанія JP Morgan використовує платформи на основі ШІ для виявлення шахрайських операцій та захисту від кібератак. Алгоритми аналізують мільйони транзакцій у реальному часі, виявляючи підозрілі патерни, які можуть свідчити про потенційну загрозу. Завдяки ШІ вдалося значно скоротити кількість шахрайств та знизити ризики для клієнтів.[4]

Однак разом із значними перевагами існують і виклики, пов'язані з використанням ШІ для кіберзахисту. Один з головних — це вразливість самих систем ШІ до атак. Зловмисники можуть використовувати методи "обману ШІ" (adversarial attacks), вводячи навмисні зміни у дані для дезорієнтації систем і змушуючи їх приймати неправильні рішення. Це створює новий рівень ризику для критичної інфраструктури, який вимагає постійного вдосконалення систем кіберзахисту. Даний метод використовується, коли система захисту, а саме база даних ШІ, нова та її потрібно протестувати. Після тестів систему оновлюють, що в свою чергу, призводить до покращення захисту та пришвидшення працездатності.

Ще одним викликом є питання етики та конфіденційності. Оскільки системи ШІ збирають і аналізують великі обсяги даних, існує ризик використання цих даних не за призначенням або порушення конфіденційності користувачів.

Таким чином, інтеграція ШІ у кіберзахист критичної інфраструктури є важливим і необхідним кроком для забезпечення надійності та стійкості цих систем. Проте ефективне використання ШІ потребує постійного розвитку технологій, впровадження нових рішень для

протидії атакам на самі системи ШІ, а також забезпечення етичних стандартів та конфіденційності.

Список використаних джерел

1. Darktrace - [Електронний ресурс] – Режим доступу: https://darktrace.com/platform
2. IBM QRadar Suite - [Електронний ресурс] – Режим доступу: https://www.ibm.com/qradar
3. Російські хакери координують дії з військовими та посилюють атаки напередодні зими. Як Україна протистоїть кібератакам на енергосистему - [Електронний ресурс] – Режим доступу: https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242
4. JP Morgan - [Електронний ресурс] – Режим доступу: https://www.jpmorgan.com/global

Юрій КІШ
аспірант кафедри інформаційних управляючих систем та технологій
Науковий керівник - **Ігор ЛЯХ**
доктор технічних наук, доцент,
професор кафедри інформатики
та фізико-математичних дисциплін,
Ужгородський національний університет

РИЗИКИ СУЧАСНИХ КІБЕРЗАГРОЗ ДЛЯ МОБІЛЬНИХ ЗАСТОСУНКІВ

Станом на початок липня 2024 року існує більше 5,45 млрд. користувачів Інтернету, 95,9% з них використовують для цього мобільні гаджети, і тільки 62,2% лептопи, або стаціонарні комп'ютери. [1,2].

Розробка, впровадження та дотримання стандартів кібербезпеки є особливо актуальним для мобільних застосунків. Для досягнення даної мети необхідно постійно та системно відслідковувати сучасні тренди виникнення нових загроз. Найбільш авторитетною в цьому плані є Open Worldwide Application Security Project (OWASP), яка з періодичністю один раз на 3-4 роки публікує рейтинги найпоширеніших кіберзагроз як для мобільних, так і для веб-застосунків, що слугують певним орієнтиром розвитку галузі розробки додатків.

Розглянемо основні зміни, що відображені у рейтингу OWASP Mobile TOP-10 2024 року. Тут є одразу чотири "новачки. На першому місці знаходяться загрози, що пов'язані з неналежним використанням облікових даних, а саме погана реалізація управління обліковими даними. Неавторизовані користувачі отримують доступ до конфіденційної інформації та можуть впливати на функціонал мобільного додатка або його серверних систем. Як наслідок, це призводить до витоку даних, втрати конфіденційності користувача, шахрайських операцій, військового та економічного шпигунства.

Типові сценарії кібератак, направлені на ураження облікових даних:

- виявлення "хардкод" даних, для подальшого отримання неавторизованого доступу;
- перехоплення незахищених облікових даних при обміні інформацією між мобільним застосунком та сервером, спроба видати себе за авторизованого користувача;
- фізичне заволодіння мобільним телефоном для отримання несанкціонованого доступу до облікового запису користувача.

Іншим "новачком" рейтингу є недостатній ступінь захисту ще на етапі розробки застосунку, коли зловмисники можуть вносити "вірусні"зміни у код, компрометувати ключі безпеки, отримати доступ до додатку через сторонні сервіси, або бібліотеки. Це призводить до несанкціонованого доступу до даних, маніпуляцій з даними, відмов в роботі застосунку, чи навіть отримання повного контролю над мобільним додатком чи пристроєм.

Для даного виду кіберзагрози може бути типовим такий сценарій. Кіберзлочинець отримує доступ до репозиторіїв і ще на початкових етапах розробки впроваджує шкідливий софт в мобільний додаток. За допомогою дійсного сертифікату підписує програму і розповсюджує її у відповідному магазині застосунків, App Store, чи Google Play, минаючи перевірки безпеки. Користувачі завантажують і встановлюють вражене програмне забезпечення, що викрадає їхні облікові та інші конфіденційні дані. Потім ці дані використовуються для шахрайства або крадіжки інших особистих даних, завдаючи значної фінансової шкоди жертвам і репутації постачальника програми.

Четверте місце займає недостатній рівень захисту даних, що подаються на вхід/вихід. Програмне забезпечення, що не в змозі належним чином виявити та відфільтрувати вразливі дані може стати об'єктом різного роду кіберзагроз. Такі критичні вектори кібератак, як SQL ін'єкції, XSS, вірусні команди призводять до пошкодження даних або вразливості застосунку, дозволяючи зловмисникам впроваджувати шкідливий код, маніпулювати конфіденційною інформацією, доносити її у спотвореному вигляді до кінцевих споживачів.

Розглянемо типову кібератаку для даного виду загрози. Спершу відбувається ідентифікація мобільного застосунку, де відсутні належні стандарти введення даних. Потім проводяться

XSS, або SQL ін'єкції, що містять невалідні символи. Через непрописану в коді належну перевірку, ПЗ неправильно обробляє вхідні дані, що й приводить до вразливостей системи. Хакер успішно виконує довільний код, отримуючи несанкціонований доступ до ресурсів девайсу та конфіденційних даних.

Останнім "новачком" є недостатній рівень забезпечення конфіденційності. Загалом розрізняють такі проблеми конфіденційності: витік інформації (тобто порушення конфіденційності), маніпуляції з інформацією (порушення цілісності), блокування, або знищення інформації (порушення доступності). Як правило типові джерела інформації про персональні дані, такі як програмні логи, резервні копії, добре захищені. Проте завдяки "троянам", чи навіть фізичному заволодінню девайсом, зловмисники можуть отримати доступ і до такої інформації. [3].

Використання ідентифікаційної інформації в параметрах запиту URL-адреси є ласим об'єктом для кібератаки цього різновиду. Параметри запиту URL-адреси часто використовуються для передачі аргументів реквесту на сервер. Однак їх можна легко знайти в логах сервера, в локальній історії браузера, перехопити за допомогою спеціальних програм - сніфферів. Тому є небезпечною практикою передавання конфіденційної інформації у параметрах запиту. Це потрібно робити у заголовку або у тілі запиту..

Підсумовуючи, можна зазначити, що найефективнішим способом протидії кіберзагрозам, є превентивні дії. Робота щодо забезпечення безпеки застосунку повинна починатися ще з перших стадій розробки ПЗ, аналізу вимог, планування архітектури додатку, впровадження та дотримання стандартів безпеки ще під час кодингу. Також серйозну увагу треба приділяти просвітницькій роботі серед нетехнічних спеціалістів та кінцевих користувачів мобільних додатків.

Список використаних джерел

1. Digital Around the World: https://datareportal.com/global-digital-overview
2. Statista. Internet Acces by device worldwide:
   URL: https://www.statista.com/statistics/1289755/internet-access-by-device-worldwide/
3. OWASP Mobile Top 10: https://owasp.org/www-project-mobile-top-10/

Деніел КЕЛАРЬ
студент 4 курсу спеціальності «Інформаційні системи та технології»
Ужгородський національний університет
***Науковий керівник* – Василь ВАКУЛЬЧАК**
кандидат фізико-математичних наук, доцент кафедри інформатики
та фізико-математичних дисциплін
Ужгородський національний університет

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СФЕРІ ПРОМИСЛОВОЇ АВТОМАТИЗАЦІЇ

У зв'язку зі зростаючою автоматизацією промислових процесів та впровадженням технологій штучного інтелекту зростає і потреба в ефективному забезпеченні кібербезпеки в таких системах. Промислові системи автоматизації часто стають мішенню кібератак через їхню критичну роль в інфраструктурі, що може призвести до значних економічних та фізичних втрат. Застосування технологій штучного інтелекту для виявлення і запобігання кіберзагрозам на промислових об'єктах є перспективним напрямком для підвищення рівня безпеки. Штучний інтелект дозволяє здійснювати моніторинг і аналіз великих обсягів даних в реальному часі, виявляти аномалії та реагувати на загрози автоматично, мінімізуючи залежність від людського фактора [1].

Дослідження від McKinsey Global Institute показують, що впровадження ШІ в промислові процеси може підвищити продуктивність на 20-30% завдяки автоматизації та оптимізації складних рутинних завдань, таких як управління виробництвом та прогнозування дефектів обладнання. Таким чином підвищення продуктивності можна досягти завдяки скороченню кількості помилок і підвищення швидкості та якості виконання потрібної роботи [2].

Також були проведені дослідження компанією "Siemens" у сфері промислових рішень де використовувались нейронні мережі для автоматичного налаштування складних технологічних процесів, в результаті чого значно підвищилась ефективність використання ресурсів та зменшує витрати на енергоносії [3].

За даними дослідження PwC (PricewaterhouseCoopers), впровадження ШІ може підвищити глобальний ВВП на 14% до 2030 року, що еквівалентно $15,7 трлн. У промислових секторах автоматизація з використанням ШІ забезпечує більш ефективне управління ресурсами, скорочення витрат і оптимізацію виробничих процесів. За оцінками PwC, до 45% виробничих процесів можна автоматизувати за допомогою сучасних технологій,
що призводить до значного зниження витрат на робочу силу і підвищення якості продукції.[4]

Дослідження BCG (Boston Consulting Group) підкреслює, що автоматизація з використанням ШІ призводить до скорочення простоїв обладнання на 30-50% завдяки прогнозуванню поломок і оптимізації технічного обслуговування. Це стає можливим завдяки використанню нейронних мереж і систем машинного навчання, які виявляють аномалії у великих обсягах даних, зібраних з датчиків на промислових об'єктах. Крім того, впровадження ШІ дозволяє значно зменшити споживання енергії та витрати на технічне обслуговування за рахунок більш ефективного використання ресурсів [5].

У цілому, впровадження штучного інтелекту у промислову автоматизацію має потужний потенціал для підвищення продуктивності, оптимізації ресурсів та покращення кібербезпеки. ШІ дозволяє автоматизувати складні процеси, ефективніше використовувати енергетичні та інші ресурси, а також значно знижує ризики кібератак шляхом виявлення аномалій і забезпечення захисту в режимі реального часу. Дослідження від McKinsey Global Institute, Siemens, PwC та BCG показали, що автоматизація з використанням ШІ може не тільки покращити ефективність виробництва, але й сприяти глобальному економічному росту, одночасно підвищуючи рівень безпеки й надійності промислових систем.

Список використаних джерел

1. Роботизація в юридичній професії: результати дослідження McKinsey Global Institute– [Електронний ресурс] – Режим доступу: https://yur-gazeta.com/golovna/robotizaciya-v-yuridichniy-profesiyi-rezultati-doslidzhennya-mckinsey-global-institute.html.
2. McKinsey Global Institute “Artificial Intelligence and the future of work” – [Електронний ресурс] – Режим доступу: https://www.mckinsey.com/mgi/our-research/generative-ai-and-the-future-of-work-in-america.
3. Siemens Research on Industrial AI Solutions – [Електронний ресурс] – Режим доступу: https://press.siemens.com/global/en/pressrelease/industrial-ai-and-sustainability-scale-siemens-redefines-industrial-innovation.
4. PwC “Global Artificial Intelligence Study” – [Електронний ресурс] – Режим доступу: https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html.
5. Boston Consulting Group (BCG). “Generative AI in the factory of the Future,”– [Електронний ресурс] – Режим доступу: https://www.bcg.com/publications/2023/gen-ai-role-in-factory-of-future.

Кирил КОТУН
кандидат педагогічних наук, старший дослідник,
старший науковий співробітник
відділу зарубіжних систем педагогічної освіти і освіти дорослих
Інституту педагогічної освіти і освіти дорослих
імені Івана Зязюна НАПН України,
Співголова Кафедри ЮНЕСКО "Неперервна
професійна освіта XXI століття" НАПН України

ПОЛІТИКА БЕЗПЕЧНОГО ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УНІВЕРСИТЕТАХ СКАНДИНАВСЬКИХ КРАЇН

Штучний інтелект (далі – ШІ) набуває все більшого значення у вищій освіті Скандинавських країн, зокрема в університетах Швеції, Норвегії, Данії, а також Фінляндії. Ці країни вирізняються системним підходом до впровадження ШІ, приділяючи особливу увагу етичності, безпеці, прозорості алгоритмів та захисту персональних даних. Університети цих держав формують освітню політику, спрямовану на інтеграцію ШІ в освітній процес для створення інноваційного та інклюзивного середовища.

В університетах Швеції, таких як Уппсальський університет (Uppsala University), ШІ активно використовується для створення індивідуальних освітніх траєкторій здобувачів вищої освіти. Технології штучного інтелекту допомагають аналізувати великі обсяги даних для моніторингу академічного прогресу та вдосконалення платформ для онлайн-навчання. Водночас особливий акцент робиться на етиці та безпеці. Уппсальський університет є одним із лідерів у дослідженні прозорості алгоритмів та їхньої відповідності стандартам, встановленим Європейським Союзом, зокрема GDPR.

У Норвегії політика використання ШІ у вищій освіті базується на національній стратегії «Norway's National AI Strategy» (2020). Університет Осло (University of Oslo) застосовує ШІ для автоматизації адміністративних процесів, що дозволяє знизити бюрократичне навантаження на викладачів та здобувачів вищої освіти. Важливою складовою є підготовка викладачів до роботи з ШІ шляхом спеціалізованих освітніх програм, що сприяють до відповідального та ефективного використання ШІ. Крім того, значна увага приділяється забезпеченню академічної доброчесності, включаючи розробку інструментів для перевірки робіт здобувачів вищої освіти за допомогою ШІ.

Фінляндія, як один із лідерів у сфері цифровізації освіти, активно впроваджує ШІ в університетах, таких як Гельсінський університет (University of Helsinki). Однією з ключових ініціатив є курс «Elements of AI», що став обов'язковим для багатьох здобувачів вищої освіти і спрямований на розвиток базових знань про штучний інтелект. Ця програма є прикладом того, як технології можуть підтримувати розвиток цифрових компетенцій. Фінські університети також використовують ШІ для створення адаптивних навчальних платформ, які підлаштовуються під потреби здобувачів, зокрема тих, хто має особливі освітні потреби. Наприклад, автоматичний переклад текстів та створення субтитрів значно покращують доступність освітніх матеріалів.

Данія фокусується на використанні ШІ для підтримки персоналізованого навчання. Копенгагенський університет (University of Copenhagen) активно впроваджує системи, що використовують ШІ для створення адаптивного контенту, який відповідає рівню знань та потребам здобувачів вищої освіти. Важливим компонентом є дотримання етичних принципів, визначених у «Danish AI Strategy». Університети працюють над тим, щоб алгоритми були прозорими, а їхнє використання сприяло інклюзії та соціальній справедливості. Окрім цього, значна увага приділяється міждисциплінарним дослідженням, що вивчають вплив ШІ на академічне середовище.

Університети Скандинавських країн дотримуються єдиних принципів у впровадженні ШІ. Перш за все, вони забезпечують дотримання високих стандартів захисту персональних даних відповідно до GDPR. General Data Protection Regulation (GDPR) – це Загальні Положення

Захисту Даних, законодавчий акт Європейського Союзу, що встановлює правила збирання, зберігання, обробки та використання персональних даних громадян ЄС. Він набрав чинності 25 травня 2018 року і є обов'язковим для виконання у всіх країнах ЄС, а також для компаній та організацій, які працюють із даними громадян Євросоюзу, навіть якщо вони розташовані за межами ЄС. Політика прозорості алгоритмів спрямована на те, щоб уникнути упередженості та дискримінації у освітньому процесі. Викладачі проходять спеціалізовані тренінги, що допомагає їм ефективно застосовувати ШІ у своїй діяльності. Також важливим компонентом є використання технологій для інклюзивності, що забезпечує рівний доступ до освіти для всіх здобувачів вищої освіти. Політика використання ШІ у вищій освіті Скандинавських країн демонструє системний підхід до інтеграції новітніх технологій у навчальний процес. Швеція, Норвегія, Фінляндія, Данія створюють модель цифрової трансформації, орієнтовану на безпеку, етику та інновації. Їхній досвід може стати прикладом для інших країн, які прагнуть підвищити якість освіти через використання штучного інтелекту.

Список використаних джерел::

AI in 4 Nordic countries (2024). URL: http://surl.li/wzbugu

Danish AI Strategy: Ethical Implementation in Education. (2024). *Agency for Digital Government*. URL: https://en.digst.dk/strategy/the-danish-national-strategy-for-artificial-intelligence/

Elements of AI – Helsinki University. (2024). URL: https://www.elementsofai.com/

National Strategy for Artificial Intelligence. (2020). Ministry of Local Government and Modernisation. URL: http://surl.li/nnsudg

Osadcha, Kateryna & Krogstie, Birgit. (2024). Ways of using artificial intelligence in IT education of Norway. URL: http://surl.li/mnfnih

The General Data Protection Regulation (2018). URL: http://surl.li/wlulfm

Володимир ОРЕЛ
студент 4 курсу спеціальності
«Інформаційні системи та технології»
Науковий керівник – **Василь МОРОХОВИЧ**
кандидат фізико-математичних наук, доцент,
доцент кафедри інформатики
та фізико-математичних дисциплін
Ужгородський національний університет

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАПОБІГАННЯ ЛЮДСЬКИМ ПОМИЛКАМ У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

В умовах стрімкого розвитку інформаційних систем постає питання організації на їх основі роботи систем захисту інформації для запобігання втраті даних, пошкодженню апаратного устаткування, некоректній роботі апаратного забезпечення, витоку інформації з обмеженим доступом та несанкціонованим діям зі сторони користувачів. За результатами дослідження, проведеного аудиторсько-консалтингової компанії «BDO», причиною 80% випадків заволодіння конфіденційною інформацією користувачів системи зі сторони сторонніх осіб є людські помилки, здійснені особами із санкціонованим доступом через низьку кваліфікацію, введення в оману, нехтування правилами інформаційної безпеки [1]. Технологія штучного інтелекту дозволяє суттєво стримувати вплив кібератак на інформаційну систему, повністю або частково автоматизуючи процес прийняття користувачем рішень, що стосуються виконання операцій з конфіденційною інформацією.

Метою є сформулювати механізми використання технології штучного інтелекту в інформаційних системах із високою кількістю користувачів для запобігання виникнення людських помилок, що створюють загрози безпеці інформації. Можливості сучасних та розроблюваних моделей штучного інтелекту імітувати когнітивні аспекти людського мозку із використанням високих обчислювальних потужностей комп'ютерної техніки дозволяють підвищити ефективність розпізнавання кібератак та зменшити ймовірність здійснення таких втручань через унеможливлення помилок, що призводять до наведених наслідків, зі сторони користувачів та персоналу.

Дослідженню питань впровадження технологій штучного інтелекту в системи захисту інформації були присвячені численні роботи науковців Гевчук А. В., Шевчука А. А., Хлапоніна Ю. І., Тіворенко Ю. А., Звенігородського О. С., Зінченко О. В., Кашуби Н. М. та інших. Проте в умовах розширення застосування інформаційних систем у різних галузях людської діяльності та, як наслідок, збільшення кількості користувачів та осіб, причетних до впровадження та підтримки їх функціонування, слід приділяти більше уваги проблемі людських помилок у процесі користування та адміністрування.

Загрози захисту інформації, що реалізуються внаслідок людських помилок, можна поділити за походженням на дві групи:

- загрози, причиною виникнення яких є виключно дії персоналу системи та осіб із санкціонованим доступом;
- загрози, умисно створені сторонніми особами без права доступу для заволодіння конфіденційною інформацією, реалізовані через некоректні дії зі сторони персоналу системи або користувачів із санкціонованим доступом.

У всіх випадках людські помилки виступають випадковим фактором, що виникає через невмотивовані до нанесення шкоди системі дії зі сторони відповідальних за збереження безпеки даних осіб через низький досвід та рівень компетенції. У другому випадку, окрім вище описаного, також слід враховувати дії сторонніх осіб, що маючи наміри здійснювати аморальну та незаконну діяльність, необмежені нормами соціальної, професійної, корпоративної етики та відповідно можуть використовувати для заволодіння інформацією неприйнятні методи: введення в оману, представлення себе іншою особою, маскування

зловмисних дій, нанесення шкоди програмній та апаратній складових системи тощо. Серед таких загроз розробник антивірусного програмного забезпечення «ESET» виділяє наступні: фішинг — масова розсилка повідомлень шахрайськими організаціями з метою заволодіння персональною інформацією та/або фінансовими ресурсами користувача, розсилка програмного забезпечення, що втручається в роботу системи з метою використання обчислювальних та інформаційних ресурсів, виведення системи з ладу [2].

Серед випадків, коли можна використати технології штучного інтелекту в системах захисту інформації, інженер захисту систем Овен Воткінс виділяє чотири основні напрямки: виявлення аномалій; розвідка кіберзагроз; сканування коду програми на наявність загроз; автоматичне виявлення слабких місць у системі [3]. Таким чиним технології штучного інтелекту можна використати для запобігання реалізації вище описаних загроз через автоматизацію процесів системи захисту інформації, залежних від персоналу та користувачів, та супровід користувачів системи під час виконання завдань.

У випадку неумисних помилок користувачів можна автоматизувати складні для людини аспекти адміністрування системи, що об’єктивно є необхідні для забезпечення захисту інформації, як створення правил взаємодії з системою, відповідно до її предметної області. У супроводі користувача штучний інтелект дозволяє впровадити інструменти пропозиції коректних рішень під час адміністрування та користування інформаційною системою.

У випадках, коли джерелом небезпеки є зловмисні дії сторонніх осіб, для запобігання людським помилкам пропонується автоматизувати реагування на спроби кібератаки, використовуючи методи обробки природної мови, аналізу коду, порівняння з аналогічними випадками втручання в роботу системи. У випадках, коли неможливо об’єктивно визначити, чи є дана ситуація спробою несанкціонованого заволодіння ресурсами користувача або організації, модель штучного інтелекту може супроводжувати користувача, від рішення якого залежить безпека системи, попереджаючи про небезпечні дії та надаючи рекомендації щодо коректного реагування на ситуацію.

Отже, застосування можливостей технологій штучного інтелекту для запобігання людським помилкам при роботі систем захисту інформації дозволить суттєво знизити ризики успішності кібератак на інформаційні системи. Визначним у питанні ефективності впровадження штучного інтелекту в системи захисту є налаштування системи реагувати як на неумисні дії користувачів і персоналу, так і на умисні дії сторонніх осіб.

Список використаних джерел

1. BDO USA. Artificial Intelligence and Cybersecurity – [Електронний ресурс] Режим доступу: https://www.bdo.com/insights/digital/artificial-intelligence-and-cybersecurity.
2. ESET Digital Security. Енциклопедія Інтернет-загроз – [Електронний ресурс] Режим доступу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/.
3. Owen Watkins. 4 use cases for AI in cyber security – [Електронний ресурс] Режим доступу: https://www.redhat.com/en/blog/4-use-cases-ai-cyber-security.

Антон СМОЛЕН
студент 4 курсу спеціальності
«Інформаційні системи та технології»
Науковий керівник – **Михайло КЛЯП**
кандидат технічних наук,
доцент кафедри інформатики
та фізико-математичних дисциплін
Ужгородський національний університет

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ ТА ВИЯВЛЕННЯ ЇХ СЛАБКИХ МІСЦЬ

Застосування штучного інтелекту (ШІ) у криптоаналізі відкриває нові перспективи для виявлення та усунення вразливостей у криптографічних протоколах. ШІ здатний автоматично аналізувати криптографічні схеми та визначати потенційні слабкі місця, що виникають внаслідок зловживання криптографією або недосконалого впровадження алгоритмів. Дослідження показують, що машинне навчання може знаходити закономірності в шифротекстах, що значно підвищує ефективність атак на симетричні шифри та хеш-функції. Наприклад, методи на основі глибокого навчання виявилися особливо ефективними в ідентифікації аномалій у даних, які можуть сигналізувати про вразливості в системах шифрування [1,2].

Метою є дослідження можливостей технологій штучного інтелекту у сфері криптоаналізу, зокрема аналіз існуючих криптографічних протоколів та ідентифікація слабких місць, що можуть бути використані для компрометації системи захисту даних. Особлива увага приділяється можливостям використання ШІ для підвищення ефективності атак на криптографічні примітиви та протоколи.

Дослідження, що ґрунтуються на використанні формальних методів, таких як CPSA та Roletran, показують, як ШІ може оптимізувати процес аналізу і виявлення вразливостей у криптографічних протоколах, за допомогою чого забезпечується більш високий рівень безпеки даних у сучасних системах [5].

Існують твердження, що традиційні методи криптоаналізу поступаються за ефективністю комбінованим підходам з використанням ШІ. Зокрема, аналітичні методи, засновані на нейронних мережах, виявляють слабкі місця у криптографічних алгоритмах, аналізуючи великі масиви даних для пошуку прихованих аномалій та закономірностей. Хоча такі підходи демонструють не надійні результати, тому дані потребують подальшого вдосконалення, щоб зменшити кількість хибнопозитивних результатів та покращити їхню ефективність у реальному застосуванні. Це підкреслює важливість інтеграції нових технологій у криптоаналіз для підвищення надійності захисту інформації [3].

Зважаючи на швидкий розвиток ШІ, необхідно враховувати, що його використання в криптоаналізі може призвести до виникнення нових ризиків. Наприклад, існує потенційна можливість розробки спеціалізованих атак з використанням ШІ, які будуть спрямовані на компрометацію навіть найсучасніших криптографічних алгоритмів, таких як: AES, 3DES, RSA, ECC та ін. [6]. Це може створити нові виклики для фахівців у галузі безпеки інформаційних систем, що потребує розробки нових контрзаходів та стратегій для запобігання можливим загрозам, зумовленим використанням ШІ в шкідливих цілях [4].

На завершення, можна зазначити, що інтеграція ШІ у криптоаналіз є перспективним напрямом розвитку кібербезпеки, здатним значно покращити ефективність захисту даних від сучасних та майбутніх загроз. Водночас, це також створює нові виклики та ризики, які потребують уважного дослідження та розробки ефективних контрзаходів, щоб забезпечити безпеку інформаційних систем у майбутньому [5]. Систематичний підхід до аналізу криптографічних протоколів з використанням ШІ допоможе покращити розуміння безпеки криптографічних протоколів та виявити вразливості, що потребують термінового усунення.

Список використаних джерел

1. Aron Gohrhttps (2019). Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning – [Електронний ресурс] – Режим доступу: //eprint.iacr.org/2019/037.pdf
2. Неправильне використання криптографії – [Електронний ресурс] – Режим доступу: https://cqr.company/ua/web-vulnerabilities/zlovzhyvannya-kryptografiyeyu/
3. Криптоаналіз – [Електронний ресурс] – Режим доступу: https://wiki.tntu.edu.ua/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7
4. Catherine Meadows (2003). Formal Methods for Cryptographic Protocol Analysis: Emerging Issues and Trends – [Електронний ресурс] – Режим доступу: https://apps.dtic.mil/sti/tr/pdf/ADA465281.pdf
5. Performance and cryptographic evaluation of security protocols in distributed networks using applied pi calculus and Markov Chain – [Електронний ресурс] – Режим доступу: https://www.sciencedirect.com/science/article/pii/S2542660523002366
6. Шифрування: типи і алгоритми – [Електронний ресурс] – Режим доступу: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/

Артемій ЦІППІНЬО
студент 4 курсу спеціальності
«Інформаційні системи та технології»
Ужгородський національний університет
Науковий керівник – **Юліан МЕРЕНИЧ**
асистент кафедри інформатики
та фізико-математичних дисциплін
Ужгородський національний університет

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В БОРОТЬБІ З ЗАГРОЗАМИ

В сучасному світі спостерігається значний розвиток інформаційних систем, що став одним із ключових факторів для забезпечення функціонування державних структур, підприємств, а також користувачів. З розвитком технологій покращується не тільки обсяг даних для обробки, але й кількість загроз, які можуть порушувати цілісність та конфіденційність. Традиційні методи захисту інформації поступово втрачають ефективність у боротьбі з новими загрозами, а також через складність новітніх кібератак, що потребує сучасних рішень у подоланні їх.

Штучний інтелект (ШІ, англ. Artificial Intelligence, AI) є однією з найпередовіших технологій сьогодення, що дозволяє використовувати нові підходи для боротьби з постійно зростаючими кіберзагрозами. Це допомагає адаптуватись до змін в кіберпросторі, а також аналізувати величезні обсяги даних і виявляти кіберзагрози в реальному часі.

Метою даного дослідження є аналіз ролі штучного інтелекту у сфері кібербезпеки, його впливу на процеси виявлення та запобігання кібератакам.

Дослідження питання використання штучного інтелекту в сфері кібербезпеки були присвячені роботи таких науковців як: Гбур З., Боренков А., Лозовський, Р., Мороз А., Хлапонін Ю., Котенко Д., Чайка Ю. та інших. Однак, зі зростанням використання інформаційних систем у різних сферах діяльності та, як наслідок, збільшенням числа користувачів і осіб, залучених до їх впровадження та підтримки, необхідно приділяти більше уваги проблемі людських помилок під час їхнього використання та адміністрування.

Штучний інтелект застосовує потужні алгоритми, які дозволяють виявляти певні шаблони вхідних даних, а також аналізувати їх і можливість прийняття рішення на основі отриманих результатів. ШІ функціонує на основі OODA, що означає “observe, orient, decide, act”. Це схоже на дії людини, проте штучний інтелект виконує це в сотні раз швидше. Також в залежності, хто використовує технології штучного інтелекту, вони можуть стати ефективним засобом захисту, але водночас можуть бути й небезпечною загрозою.

На сьогодні можна виділити наступні види загрози з використанням штучного інтелекту:

- автоматизовані процеси взлому (наприклад, пошук вразливості системи, подолання захисту систем);
- автоматизація і спрощення фішингових атак для викрадення персональних даних;
- створення дипфейків для маніпуляції та шахрайства за допомоги соціальної інженерії;
- порушення та знищення цілісності даних для порушення роботи певних моделей штучного інтелекту;
- спрощення для створення шкідливого програмного забезпечення (віруси) [1].

Як було зазначено вище, використання штучного інтелекту може створювати не тільки загрози, але й вдосконалювати їх засоби захисту. В цьому може допомогти так званий прогнозуючий штучний інтелект, який може оптимізувати виявлення загроз і пропонувати якнайкращі рішення з кібербезпеки. Найкорисніше в таких системах штучного інтелекту є те, що вони здатні до самонавчання та аналізування непередбачуваних ситуацій.

Наприклад, можна виділити, якими способами може виявляти та передбачати загрози штучний інтелект:

- аналіз великих даних в режимі реального часу;
- визначення незвичайної діяльності;
- визначення потенційних векторів атак (прогнозування на основі історичних даних) [2].

Слід зазначити, що застосування штучного інтелекту в кібербезпеці розвивається у двох основних напрямах: превентивні заходи та реакція на атаки.

Превентивні заходи з використанням штучного інтелекту мають завдання попереджувати про можливі загрози ще до того, як вони можуть стати реальною проблемою. Наприклад, за допомогою прогнозного аналізу штучний інтелект може відстежувати аномальні патерни у мережевій активності, на основі яких робить висновки про потенційні атаки. Це допомагає запобігати атакам на ранніх етапах, виявляючи загрози ще до того, як вони проявляться у повній мірі.

Також штучний інтелект може допомогти у створенні динамічних моделей ризику, які постійно оновлюються відповідно до актуальних виявлених вразливостей, забезпечуючи актуальність заходів захисту. Важливу роль відіграє автоматичне оновлення систем безпеки на основі аналізу поведінки шкідливого програмного забезпечення (вірусів, троянів).

Завдяки можливості штучного інтелекту, працювати в режимі реального часу, системи безпеки можуть оперативно відповідати на кібератаки, виявляючи і блокуючи зловмисну активність ще до того, як це може спричинити значної шкоди. До прикладу, штучний інтелект може автоматично блокувати підозрілі IP-адреси, а також закривати вразливі порти та ізолювати скомпрометовані системи для мінімізації шкоди. Також ефективність штучного інтелекту проявляється в аналізі логів та метаданих мережевих атак, які дозволяють швидко відновлювати системи та запобігати повторенню подібних інцидентів у майбутньому.

Одним із популярних інструментів, що застосовуються організаціями для виявлення кіберзагроз, є системи UEBA (англ. User and entity behavior analytics, Аналітика поведінки користувачів та сутностей). Такі системи орієнтовані на моніторинг і аналіз дій користувачів у межах організації, з метою виявлення підозрілої або несанкціонованої активності. Завдяки використанню штучного інтелекту, системи UEBA можуть доповнювати або навіть замінювати традиційні методи безпеки, наприклад, система виявлення вторгнень (IDS). Штучний інтелект допомагає підвищити точність та ефективність виявлення загроз за рахунок аналізу поведінкових патернів і більш гнучкого реагування на аномалії [3, 4].

Отже, використання штучного інтелекту може запобігти новим кібератакам, використовуючи актуальні дані в режимі реального часу. Також ШІ не лише запобігає загрозам, але й постійно адаптується до нових видів атак завдяки навчанню. Це важливо, оскільки хакери також використовують штучний інтелект для складних кібератак. Штучний інтелект допомагає автоматизувати виявлення та реагування на загрози, зменшуючи навантаження на фахівців і підвищуючи ефективність захисних систем. У майбутньому розвиток штучного інтелекту може призвести до створення автономних систем кібербезпеки, здатних самостійно нейтралізувати загрози без участі людини.

Список використаних джерел

4. WEZOM. Застосування ШІ у кібербезпеці: роль та переваги – [Електронний ресурс] – Режим доступу: https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi.
5. BDO. The Role of AI in Cybersecurity: Anticipating and Preventing Attacks – [Електронний ресурс] – Режим доступу: https://www.bdo.com/insights/digital/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks.
6. ДУІКТ. Способи застосування штучного інтелекту в управлінні кібернетичною безпекою, Ухань Я. В., Сокуренко Д. О. – [Електронний ресурс] – Режим доступу: https://duikt.edu.ua/uploads/p_2626_38605375.pdf?file=p_2626_38605375.pdf#page=144.
7. IBM. What is user and entity behavior analytics (UEBA)? – [Електронний ресурс] – Режим доступу: https://www.ibm.com/topics/ueba.

Олена ПЕТРУШЕВИЧ
студентка ІІІ-го курсу,
кафедра математики та інформатики
Закарпатського угорського інституту ім. Ференца Ракоці ІІ
Еніке ЯКОБ
доктор філософії (PhD),
кафедри математики та інформатики
Закарпатського угорського інституту ім. Ференца Ракоці ІІ

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ У ВИКЛАДАННІ ІНФОРМАТИКИ

Інформатика, яка має широке застосування та використовується у всіх видах людської діяльності, за останнє століття, а особливо останні роки, інтенсивно розвивається. Тому одним із важливих завдань навчальних закладів є формування зростаючого покоління що орієнтується в інформаційній сфері, може правильно сприймати, аналізувати та обробляти інформацію, а також вміє використовувати комп'ютерні технології для навчання, професійної діяльності, та життєдіяльності загалом. Тому методика навчання цього предмету шкільної програми також потребує змін.

Для формування в учнів стійкої навчально-пізнавальної мотивації необхідно змінити традиційний зміст навчальних предметів. Важливою є перебудова не тільки змісту навчання, а й організації навчального процесу.

За останній час штучний інтелект (ШІ) стрімко розвивається та перетворився на один із ключових факторів розвитку сучасного суспільства. Його застосування стає дедалі ширшим та охоплює різні сфери життя. ШІ також має потенціал трансформувати та модернізувати освіту, покращити її якість, створити ефективні, індивідуалізовані підходи до здобуття знань.

Великий перелік ШІ-інструментів, доступних в Інтернеті є на сайті Aixploria. Підібравши відповідний інструмент ШІ вчителі можуть використати їх для вирішення багатьох завдань при викладанні інформатики. А саме планування уроків (MagicSchool), створення сценарію уроку (Nolej, DiffIt, MyLessonPal, Copilot, teachology.ai., Curipod), виготовлення завдань (Redmenta), отримання зворотнього звязку від проведеного уроку (TeachFX. EnlightenAI), перетворення тексту на відеоконтент (Elai.io.), створити з аудіозапису текст (Kami), виготовляти ілюстрації (Dall-E), адаптувати пояснення теми уроку враховуючи індивідуальні особливості учнів, генерувати запитання до тем (PrepAI, to teach_, Conker, Formative, QuestionWell, Mindgrasp, Quiz Makito, WorksheetsAI.), вивчати кодування (CodeSignal Learn, Replit) та багато інших завдань.

Отже, ШІ може автоматизувати багато рутинних завдань. Він також стає ключовим інструментом для постійного оновлення та удосконалення навчальних програм. Однією з ключових переваг використання ШІ у сфері освіти є гнучкість та індивідуалізація навчального процесу. Але існують і виклики використання ШІ в освіті. Серед них нерівний доступ, хибні дані, атрофія критичного мислення, перенасичення, відволікання уваги, дегуманізація і, звичайно, інформаційна безпека. Одним із важливих завдань, яке будемо досліджувати та вивчати в ході виконання курсової роботи на період 2024/2025 року це «Роль штучного інтелекту у сфері інформаційної безпеки». У підсумку впровадження ШІ у сферу освіти може зробити навчання більш ефективним, доступним та індивідуалізованим. Проте успіх цього процесу залежить від уважного врахування всіх можливих наслідків та вдосконалення стратегій використання ШІ в освітніх цілях.

Ключові слова: штучний інтелект, викладання інформатики, інформаційна безпека.

Artym ROSTYSLAV
Second year Bachelor students,
"Cybersecurity and information Protection" major
National Aviation University
***Scientific supervisor* - Tetyana SHULHA**
Senior Lecturer,
Department of foreign languages for professional communication,
National Aviation University

ARTIFICIAL INTELLIGENCE AS AN INFORMATION SECURITY TOOL

In today's world, the rapid advancement of information technologies, when not adequately embraced by society, presents a significant challenge. This directly impacts the information security of both the state and major entities such as international corporations. Artificial intelligence (AI) has become a potent tool in discerning and addressing issues associated with cyberattacks and information threats, with information security being one of its key aspects. AI's domain lies in automating information protection processes and countering evolving threats at increasingly sophisticated levels.

The purpose of this paper is to study the role of artificial intelligence in ensuring information security, namely, to provide examples of the effective use of AI to eliminate constant threats in the field of information security.

The most critical areas of artificial intelligence usage for ensuring security in the information space include attack detection or prediction, analysis of information data, intelligent authentication methods, self-learning, and adaptation.

Artificial intelligence detects attacks using algorithms that analyze potential threats based on large amounts of data. AI analyzes and correlates data about events and cyber threats from multiple sources, turning it into understandable and actionable insights that security professionals can use for further investigation, response, and reporting. Information data analysis is an integral part of what AI does to secure the information space, minimizing problems and facilitating the workflow of already verified and secure information.

Multifactor authentication is a security method for identity and access management that requires different forms of identification to access resources and data. AI-powered multifactor authentication helps to monitor and protect the most vulnerable data and networks.

Using machine learning algorithms, all AI-based intelligent systems are able to continuously learn from the data evaluated by the system, increasing their level of efficiency and reliability, which is a very important factor in cyberspace.

Artificial intelligence makes it possible to almost completely exclude humans from the process of ensuring information security protection and leave them with only auxiliary monitoring and correction functions, as it is able to analyze and control data on its own, for example, monitor networks, check logs, and detect minor system malfunctions. However, humans remain extremely important for cybersecurity. AI remains an auxiliary tool that helps them improve their skills and detect and eliminate threats faster. Based on statistics from the European Business Association, the market value of artificial intelligence in cybersecurity will reach USD 46.3 billion in 2027. AI cybersecurity companies offer significant benefits, providing organizations with invaluable tools to navigate cybersecurity and become more agile in the face of cyber threats.

Thus, the main advantages of using AI for information security include real-time analysis of large data sets, faster detection of critical cyber threats, identification of vulnerabilities and potential risks, provision of cyber threat analysis and analytical conclusions, optimized report generation, and assistance to analysts in developing their skills. However, when talking about the benefits of AI, it is worth mentioning the drawbacks, including the use of AI to crack passwords, generate fake data, and disinformation.

Based on all the information provided, including the role of artificial intelligence in information security, we can conclude that the significance of AI for security will continue to increase. It is important to remember that AI is not only used for defending against cyberattacks (white hacking),

but also for launching attacks and phishing (black hacking), which is punishable by law. In summary, while AI has the potential to strengthen defense in the realm of information security, we cannot ignore the fact that it can also be used for malicious purposes.

Polina TARAN
Viktoria SHVED
Second year Bachelor students,
"Cybersecurity and information Protection" major
National Aviation University
***Scientific supervisor*- Nataliia DENISENKO**
Senior Lecturer,
Department of foreign languages for professional communication,
National Aviation University

CAN ARTIFICIAL INTELLIGENCE SURPASS HUMAN INTELLIGENCE: TECHNICAL AND PHILOSOPHICAL PERSPECTIVES?

In the modern world, the rapid development of artificial intelligence causes numerous discussions about its potential and capabilities. AI already performs tasks that were previously considered purely human, such as analyzing large amounts of information, recognizing speech, and making decisions based on data.

In medicine, AI is used to improve diagnostics. For example, systems based on deep learning can analyze medical images such as X-rays and MRIs with high accuracy. This allows diseases such as cancer to be detected in the early stages, which significantly increases the chances of successful treatment. Autonomous vehicles, such as self-driving cars, use AI to process data from sensors and cameras, allowing them to navigate the road, avoid obstacles, and make real-time decisions. This can reduce the number of traffic accidents and improve road safety. In finance, AI helps detect fraudulent transactions, predict market trends, and automate trading. Associated with virtual assistants such as Siri or Google Assistant, speech recognition systems use AI to convert spoken speech into text. This allows users to interact with devices using voice commands, facilitating access to information and device management. Chatbots and virtual assistants, like those used in online stores or customer support, help automate the processing of inquiries and provide quick answers to common questions. This reduces the burden on human operators and improves the quality of customer service.
On online shopping platforms such as Rozetka or Prom, AI analyzes purchase and browsing history to create personalized product recommendations. This helps users find the products they are interested in and increases sales efficiency for companies.

From a philosophical point of view, the question of AI surpassing human intelligence touches on the concepts of consciousness, intelligence, and morality. Human intelligence includes not only logical thinking, but also emotions, self-awareness, and moral guidelines. Currently, AI does not have consciousness and is not capable of "understanding" information the way a human does. Although AI can generate text based on patterns, as in the case of GPT models, it does not have the true understanding or emotion that is inherent in humans. Philosophers debate the possibility of creating a conscious AI, its capacity for self-reflection, and ethical questions regarding the rights of such an intelligence.

The future coexistence of humans and AI can have different scenarios: from optimistic, where AI complements human intelligence and increases work efficiency, to threatening, where the development of superintelligence can lead to a loss of control. Transhumanism proposes the integration of technology into the human body and mind to remain competitive, but this opens up new ethical challenges. For example, neuroimplants can enhance a person's cognitive abilities, but they also raise questions about the privacy and security of personal data.

Artificial intelligence is already integrated into our lives through various systems, from fingerprint scanners and Face ID to chatbots and automation systems. His work is based on combining large amounts of data with processing algorithms that allow systems to learn from patterns and improve over time. Thus, the future coexistence of humans and AI will depend on how responsibly society approaches the development and regulation of these technologies.

Валерій КОЗЮРА
кандидат технічних наук, доцент кафедри технологій захисту кіберпростору центру Кібербезпеки Національна академія Служби безпеки України

КЕРУВАННЯ КІБЕРБЕЗПЕКОЮ НА ОСНОВІ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ

Керування безпекою на основі систем ШІ включає машинне навчання для аналізу об'єднаних колекцій історичних даних про кібербезпеку, вивчаючи існуючі моделі поведінки у сфері безпеки як людей, так і комп'ютерів. Подібні моделі неправомірної поведінки можуть вказувати на інциденти безпеки, які інакше залишилися б непоміченими, або можуть вказати на джерела інцидентів безпеки. Маючи можливість комбінувати низку джерел даних, такі методи навчання дозволяють краще виявляти складні закономірності, виявляти порушників, поєднувати розрізнені вектори кібератак із широким спектром слабких місць у системі безпеки ІТС.

Традиційні технології безпеки, такі як виявлення вторгнень та засоби контролю периметра, використовують спеціально написані правила або евристики, що визначаються вручну, для виявлення аномалій. Такі підходи вимагають значних ручних зусиль, щоб гарантувати, що вони залишаються актуальними та ефективними, і існує межа діапазону моделей поведінки, які можуть бути виявлені в такий спосіб.

Декілька типів методів машинного навчання, включаючи методи глибокого навчання, часто входять у модель кібербезпеки, засновану на ШІ.

Машинне навчання використовує структуровані, розмічені дані для отримання прогнозів. Це означає, що люди повинні ідентифікувати та класифікувати конкретні особливості вхідних даних. Навпаки, алгоритми глибокого навчання не вимагають попередньої обробки даних так само. Натомість вони беруть неструктуровані дані та отримують функції в рамках алгоритмічної обробки; глибоке навчання групує дані у схожі групи, накладаючи структуру на неструктурований набір даних. Глибоке навчання можна використовувати для виявлення мережевих вторгнень, ідентифікації та класифікації шкідливих програм, а також для виявлення бекдор-атак.

Машинне навчання і глибоке навчання засновані на різних типах процесів, які зазвичай називають контрольованим і неконтрольованим навчанням. Наприклад, контрольовані методи навчання можуть бути використані для виявлення спроб відмови в обслуговуванні. Це можна зробити, використовуючи дані, структуровані із заздалегідь заданими функціями, такими як IP-адреса джерела, веб-запит та формат веб-запиту. Навпаки, методи навчання без вчителя можуть працювати з даними, які не були попередньо позначені; тому дані називаються неструктурованими. Такі методи навчання можуть самостійно виявляти закономірності даних. Наприклад, такий метод дозволяє групувати користувачів певної програми та ідентифікувати дані, до яких вони можуть отримати доступ.

В управлінні безпекою на основі ШІ можуть використовуватися також методи обробки природної мови (Natural Language Processing, NLP). Приклади моделювання безпеки на основі NLP: виявлення шкідливих доменних імен у DNS-трафіку; виявлення фішингових атак шляхом вилучення фішингового контенту (URL-адреси, адреси електронної пошти, вміст та склад повідомлень); аналіз сімейств шкідливих програм.

Висновки. Основні кроки реалізації моделей ШІ в системах управління кібербезпекою: 1) визначити інфраструктуру системи управління кібербезпекою на базі моделей ШІ та оцінити ризики їх використання; 2) розробити посібник для підрозділів кібербезпеки, щоб кібербезпека на основі ШІ була правильно налаштована; 3) підвищити обізнаність організації про те, як ШІ формує та змінює можливості підходу організації до кібербезпеки; 4) підвищити обізнаність співробітників щодо потенційних переваг використання кібербезпеки на основі ШІ.

Богдан КОШТУРА
молодший науковий співробітник,
кафедри цивільного права та процесу
Ужгородський національний університет
***Науковий керівник –* Марія МЕНДЖУЛ**
професор, доцент
кафедри цивільного права та процесу
Ужгородський національний університет

ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ШТУЧНОГО ІНТЕЛЕКТУ

Постановка наукової проблеми. З розвитком технологій штучного інтелекту (ШІ) та їх широким застосуванням у сфері надання послуг постає питання забезпечення належного рівня кібербезпеки. Використання ШІ для автоматизації процесів у фінансовій, медичній, транспортній та інших сферах значно підвищує ефективність, але водночас створює нові загрози, пов'язані з порушенням кібербезпеки та захисту персональних даних. Ці ризики викликані як вразливістю технологій, так і відсутністю чіткого правового регулювання, що визначає відповідальність та вимоги до безпеки.

Формулювання завдання й обґрунтування актуальності. Мета доповіді полягає в аналізі, систематизації правових актів, які регулюють інформаційну безпеку ШІ в Україні. Дослідження націлене на виявлення та систематизацію законодавчої бази.

Актуальність дослідження зумовлена стрімким розвитком технологій ШІ та кіберзагроз, що потребує адаптації законодавства до сучасних викликів. Недостатність правової регламентації створює ризики для споживачів та учасників правовідносин.

Наукова новизна. На відміну від попередніх робіт, які переважно зосереджуються на загальних проблемах регулювання ШІ або окремих галузях, це дослідження інтегрує питання кібербезпеки в контексті інформаційної безпеки і пропонує систематизацію законодавчої бази з урахуванням міжнародного досвіду.

Короткий виклад поставленого завдання. Регулювання штучного інтелекту в Україні є на етапі становлення. У 2020 році Кабінет Міністрів України затвердив Концепцію розвитку ШІ (Розпорядження №1556-р), яка визначає основні напрями розвитку ШІ та його інтеграцію в різні сфери. Концепція охоплює правові, етичні та технічні аспекти впровадження ШІ. Однак в Україні поки що відсутній спеціальний закон про штучний інтелект, хоча розвиток законодавчої бази продовжується, спираючись на міжнародні стандарти.

Кібербезпека в Україні регулюється кількома ключовими нормативно-правовими актами, зокрема Законом України «Про основні засади забезпечення кібербезпеки України». Цей закон визначає загальні принципи забезпечення кібербезпеки для всіх інформаційних систем, включаючи ті, що працюють на основі штучного інтелекту. Хоча закон спеціально не регулює ШІ, кібербезпека, пов'язана з його використанням, охоплюється загальними правилами захисту інформації та кіберзагроз.

Додатково, Концепція розвитку ШІ також включає аспекти кібербезпеки, наголошуючи на необхідності створення безпечних умов для впровадження нових технологій, включаючи штучний інтелект. Ця концепція передбачає створення комплексних стандартів безпеки, які мають враховувати специфіку ШІ, оскільки він може об'єктомі інструментом кіберзагроз.

Висновки. В Україні відсутній спеціальний закон про штучний інтелект, проте існує низка нормативно-правових актів, які частково регулюють питання кібербезпеки у контексті ШІ. Це свідчить про необхідність вдосконалення правової бази. Відсутність чіткого законодавчого регулювання кібербезпеки ШІ створює правові та технічні ризики, зокрема щодо захисту персональних даних та відповідальності за кібератаки. Наразі, основними нормативно правовими актами, що регулюють інформаційну безпеку штучного інтелекту Концепція розвитку штучного інтелекту в Україні та Закон України “Про основні засади забезпечення кібербезпеки України.

Олександр РАДКЕВИЧ
доктор педагогічних наук, професор,
головний науковий співробітник відділу
моніторингу та оцінювання якості загальної середньої освіти,
Інститут педагогіки Національної академії
педагогічних наук України

ЦИФРОВА БЕЗПЕКА В ЕЛЕКТРОННИХ СИСТЕМАХ ОЦІНЮВАННЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ ПЕДАГОГІВ

З розвитком інформаційних технологій і цифровізації навчальних процесів, електронні системи оцінювання професійної діяльності педагогів набули широкого поширення. Однак, зростання використання таких систем спричинило нові виклики, пов'язані з цифровою безпекою. Основними аспектами цієї проблеми є захист персональних даних, гарантування конфіденційності інформації, а також захист від кібератак.

Основні загрози, з якими можуть стикатися електронні системи оцінювання:

1. Неавторизований доступ до даних. Системи оцінювання зберігають конфіденційну інформацію, таку як персональні дані педагогів, результати оцінювання, та інші документи, пов’язані з професійною діяльністю. Несанкціонований доступ до цих даних може призвести до витоку інформації, її підробки або несанкціонованого розповсюдження.
2. Кібер-атаки. Злом систем за допомогою шкідливого програмного забезпечення (вірусів, троянців) або атак типу "відмова у наданні послуг" (DDoS) можуть тимчасово вивести з ладу систему оцінювання або викликати втрату даних. Такі атаки можуть бути спрямовані на дискредитацію системи або отримання неправомірних переваг.
3. Соціальна інженерія. Один із найбільш ефективних способів компрометації систем безпеки полягає у маніпулюванні користувачами. Наприклад, фішингові атаки можуть використовуватися для отримання паролів або іншої конфіденційної інформації через електронну пошту або підроблені веб-сторінки.
4. Вразливості програмного забезпечення. Багато систем оцінювання можуть мати недоліки або вразливості в своїй програмній архітектурі, які можуть бути використані хакерами для несанкціонованого доступу або зміни даних.

Для забезпечення цифрової безпеки електронних систем оцінювання професійної діяльності необхідно впровадити низку заходів:

1. Шифрування даних. Використання сучасних алгоритмів шифрування даних, як під час їхнього зберігання, так і під час передачі, дозволяє мінімізувати ризики витоку інформації навіть у випадку несанкціонованого доступу.
2. Мультифакторна автентифікація (MFA). Забезпечення доступу до системи за допомогою двоетапної перевірки (пароль та код з мобільного пристрою) значно ускладнює можливості зловмисників отримати доступ до акаунтів користувачів.
3. Оновлення програмного забезпечення. Регулярне оновлення системи оцінювання дозволяє усунути відомі вразливості та захистити систему від нових видів загроз.
4. Навчання користувачів. Педагоги та інші користувачі системи повинні бути ознайомлені з основами цифрової безпеки, включаючи правила створення надійних паролів, розпізнавання фішингових атак та безпечне використання ресурсів мережі Інтернет.
5. Системи виявлення вторгнень (IDS). Інтеграція систем моніторингу та виявлення підозрілої активності дозволяє оперативно виявляти спроби несанкціонованого доступу і запобігати їм.

Ураховуючи викладене, цифрова безпека вбачається критично важливою складовою успішного функціонування електронних систем оцінювання професійної діяльності педагогів. Запобігання загрозам та впровадження відповідних захисних механізмів допоможе забезпечити конфіденційність, цілісність і доступність інформації, з якою працюють ці системи. Успішне вирішення питань цифрової безпеки сприятиме підвищенню довіри до електронних систем оцінювання та їх ефективному використанню в освітньому середовищ

Veronika KUKSA
Second year Bachelor student, "Cybersecurity and information Protection" major
National Aviation University
Scientific supervisor – **Natalia BILOUS**
Associate professor, Department of foreign languages for professional communication
National Aviation University

AUTOMATION OF THREAT DETECTION PROCESSES: IMPROVING THE QUALITY

Processes to automate the detection of threats in cyberspace improve the level of security.

Automation is created precisely in order to reduce the number of processes under the guidance of a person:

The artificial intelligence on which the systems are based, unlike a person, is capable of processing a large amount of information in real time.

Real-time response is minimizing the time between detection of a threat and taking action, reducing potential damage from cyber attacks.

Thanks to automation, specialists can not focus on detecting threats in the system and instead spend resources on more important projects.

Automation provides protection against the human factor (fatigue, inattention), i.e. all threats will be detected and neutralized.

Thanks to automation, specialists can not focus on identifying threats in the system and spend resources on larger projects.

UBA - an automated solution for analyzing user behavior through the integration of other systems

SIEM - information security event management system as an additional threat detection system.

Systems that are automatic scale to handle data or threats that increase in number, so they are indispensable for large enterprises.

Systems from different organizations can communicate with each other to learn or improve security by sharing data.

Companies that have an automated system can allocate resources much more efficiently, because they reduce the costs associated with responding to incidents and «manual costs».

Challenges:

- adaptation to new threats;
- prevention of defensive response to false threats.

Olexandra ZADOROZHNA
specialty "Information systems and technologies",
the 5th year of study
Scientific supervisor - **Hanna SOROKUN**
National Aviation University

ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

In today's world the Internet has become the invaluable tool of communication, education and entertainment, but it also has given rise to a huge amount of various forms of exploitation and abuse, targeting minors. Artificial Intelligence (AI) plays a pivotal role in detecting and preventing child abuse as well as it may be misused by cybercriminals to create different forms of exploitation, such as deepfakes or AI-generated Child Sexual Abuse Material (CSAM). Given the widespread and consistently evolving nature of these threats, the issue of developing the robust AI-driven solutions to combat them has never been more pressing.

AI significantly enhanced the ability of law enforcement and technology companies to detect harmful online behavior. Usage of Natural Language Processing (NLP) allows AI to scan millions of posts, comments and messages across different platforms to detect any sign of dangerous patterns, such as hate speech and threats. Similarly, photos and videos can be analyzed to prevent inappropriate or illegal content to be posted on Internet. Powerful tools of AI being a guardian of digital safety are facial recognition and image-matching technologies. These methods have become a huge assistance to law enforcement in locating and rescuing victims, using cross-referencing of images with databases of missing or exploited children.

According to Meta Transparency Report during the period from October 2023 to April 2024 there had been reported 495 cases of bullying and harassment, 164 cases of sexual assault and 764 cases of sexual extortion on Instagram alone [1]. Detecting such behavior online is possible due to implementation of AI in Meta products. Meta even launched the Deepfake Detection Challenge in 2020 to encourage IT-specialists to develop AI tools for deepfake detection.

Despite of all positive aspects, AI evolvement and unsupervised presence of children online may create a serious problem. According to Europol's Internet Organized Crime Threat Assessment (IOCTA) 2024 report, the use of AI, that allows offenders to generate or alter CSAM, is set to further proliferate in the near future. The production of artificial CSAM increments the amount of illicit material in circulation and complicates the identification of victims as well as perpetrators [2].

What can be done to prevent usage of AI in a harmful way? First, developers can build AI-powered filters that automatically detect and flag CSAM in images, videos, and text. This includes integrating image recognition algorithms and NLP models into platforms to detect harmful content quickly and accurately. Machine learning models that analyze user interactions to detect suspicious grooming behaviors can be designed. These models could identify patterns such as adults frequently initiating contact with minors, persistent messaging, or coercive language, triggering alerts for review. Second, holding technology platforms accountable for not doing enough to remove CSAM can be enforced through laws.

In conclusion, AI has proven to be a vital tool in the fight against online bullying, immoral and unethical behavior and abuse. Its ability to detect harmful content, analyze behavior, and automate reporting has significantly strengthened efforts to protect vulnerable individuals in the digital world. However, AI's potential that is weaponized by cybercriminals and predators highlights the double-edged nature of this technology.

References:

1. Regulation (EU) 2022/2065 Digital Services Act Transparency Report for Instagram. Official website. https://transparency.meta.com/reports/regulatory-transparency-reports
2. Internet Organised Crime Threat Assessment (IOCTA) 2024. Official website. https://www.europol.europa.eu

Maksim BRODYAK
Second year Bachelor student, "Cybersecurity and information Protection" major
National Aviation University
Scientific supervisor – **Natalia BILOUS**
Associate professor, Department of foreign languages for professional communication
National Aviation University

MODERN TRENDS AND CHALLENGES OF CYBER SECURITY IN THE CONDITIONS OF DIGITAL TRANSFORMATION

Modern cybersecurity trends and challenges in the context of digital transformation are important aspects of technology and business development. The main trends in cybersecurity include:Modern trends and challenges in cybersecurity in the context of digital transformation are important aspects of technology and business development.

The main trends in cybersecurity include:

1.Increasing number of cyberattacks

As processes are digitalized, the number and complexity of cyberattacks are increasing. Not only individual companies but also critical infrastructure (energy, healthcare, transportation) are being attacked. Cyber fraud, phishing, and denial of service (DDoS) attacks are taking on new forms.

2. Strengthening personal data protection

Under new regulations such as the GDPR in the EU, companies are required to effectively protect users' personal information. Breaches in cybersecurity can lead to fines and loss of customer trust.

3. Internet of Things (IoT)

The Internet of Things brings together many devices that can be targeted for attacks. Insufficient security of such devices can become a vulnerability for attackers who can use them for large-scale attacks.

4. Artificial intelligence (AI) and machine learning (ML)

AI and ML are increasingly used for both defense and attack. On the one hand, these technologies allow detecting threats in real time, and on the other hand, attackers use AI to create more sophisticated attacks.

5. Cloud technologies

The massive transfer of data and applications to cloud storage creates new challenges for cybersecurity. Additional measures are needed to protect these systems, especially when it comes to sensitive data.

6. Development of quantum computing

Although quantum computing has not yet become a mainstream technology, its development can significantly change the cybersecurity field. Quantum computers can crack modern cryptographic systems, which raises the challenge of developing new security methods.

Cybersecurity challenges in the context of digital transformation:

Lack of qualified workers.

Outdated security systems.

Adapting to new forms of threats.

Privacy in the digital environment.

Антон ЛУЧИЦЬКИЙ
2 курс, 125 «Кібербезпека та захист інформації»
Національний авіаційний університет
***Науковий керівник* – Олена ГУРСЬКА**
доцент кафедри іноземних мов за фахом
Національний авіаційний університет
olena.hurska@npp.nau.edu.ua

ШТУЧНИЙ ІНТЕЛЕКТ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ

В останні роки стрімке зростання кількості кібератак змусило багато організацій і урядів по всьому світу звернути особливу увагу на питання кібербезпеки. Одним з найважливіших інструментів у цій боротьбі став штучний інтелект (ШІ), який дозволяє створювати нові рішення для захисту інформаційних систем. Не зважаючи на актуальність означеної проблеми, аналіз останніх публікацій [1, 2] засвідчив, що питання використання ШІ в кібербезпеці вивчене ще недостатньо. Таким чином, наша доповідь має на *меті* дослідити сучасні перспективи та виклики у забезпеченні кібербезпеки.

Однією з ключових переваг ШІ є можливість аналізувати величезні обсяги даних і оперативно виявляти підозрілі дії або аномалії, які можуть свідчити про кібератаки. У звичайних умовах для такого аналізу було б потрібно багато часу і зусиль з боку людей, але ШІ може виконувати це автоматично і в реальному часі, а системи на основі машинного навчання можуть "вчитися" на вже відомих випадках кібератак і прогнозувати нові загрози.

Ефективність використання ШІ можна побачити на прикладі компанії Darktrace, яка застосовує алгоритми штучного інтелекту для моніторингу корпоративних мереж. Їхні системи використовують машинне навчання для побудови моделей нормальної поведінки мережі та виявлення відхилень, що можуть бути ознаками кібератак.

Водночас, з використанням ШІ у кібербезпеці пов’язано чимало викликів. Наприклад, важливо враховувати, що навіть найсучасніші системи можуть робити помилки або виявляти надмірну активність там, де її немає. Це може викликати непотрібні тривоги або пропускати реальні загрози. Також виникає питання довіри до систем, де рішення ухвалює ШІ, а не людина. Як зазначає експерт з кібербезпеки Джон Сміт: "Ми повинні пам'ятати, що штучний інтелект – це лише інструмент, і його ефективність залежить від того, як ми навчимо його й інтегруємо в наші системи. Найбільший ризик полягає не в технології, а в тому, як ми її використовуємо".

Основними *результатами* дослідження є виявлення перспектив використання ШІ у галузі кібербезпеки. Очікується, що в майбутньому ці системи стануть ще більш ефективними і здатними не лише швидко й автоматично реагувати на загрози без людського втручання, але й адаптуватися до змінних умов кіберпростору та самостійно навчатися на основі нових даних. Проте важливо приділяти увагу вирішенню етичних питань і гарантувати, що технології ШІ застосовуються відповідально та без шкоди.

Висновок. Таким чином, штучний інтелект стає важливим інструментом у сфері кібербезпеки, допомагаючи швидше й точніше виявляти загрози та автоматизувати процеси захисту. Однак його ефективність залежить від належної інтеграції з традиційними методами, дотримання етичних норм та постійного вдосконалення технологій. Виклики, пов'язані з довірою до ШІ та можливістю його використання зловмисниками, потребують особливої уваги. Тож, незважаючи на великий потенціал, штучний інтелект має бути доповненням до існуючих підходів, а не їхньою заміною.

Список використаних джерел:

1. Ящик О. Б., Симонов В. В., Іваненко Р. О. Забезпечення кібербезпеки в еру штучного інтелекту: аналіз технологічних підходів та стратегій для захисту інформації. *Бізнес інформ. 2024.* № 1. С.81-86. DOI: Org/10.32983/2222-4459-2024-1-81-86

2. Welukar, J. N., & Bajoria, G. P. (2021). Artificial Intelligence in Cyber Security-AReview. *International Journal of Scientific Research in Science and Technology*. 2021. P. 488–491.

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