Міністерство освіти і науки
Український державний університет науки і технологій
Дніпровський державний технічний університет
Дніпровський національний університет імені Олеся Гончара
Національний технічний університет «Дніпровська політехніка»
Криворізький національний університет
Харківський національний університет радіоелектроніки
Херсонський національний технічний університет
Чорноморський державний університет імені П. Могили
Aalto University (Університет Аалто, Фінляндія)
American University of Central Asia (Бішкек, Киргизстан)
Tallinna Tehnikaülikool (Таллінн, Естонія)
AGH University of Science and Technology (Краків, Польща)
Politechnika Rzeszowska (Жешув, Польща)
Ariel University (Аріель, Ізраїль)
Michigan State University (Іст-Лансінґ, США)
Leibniz Universitat Hannover, Institute of Photogrammetry and Geoinformation
(Ганновер, Німеччина)

МАТЕРІАЛИ
Міжнародної науково-технічної конференції
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ в
МЕТАЛУРГІЇ та МАШИНОБУДУВАННІ

MATERIALS
of Scientific and Technical International Conference
INFORMATION TECHNOLOGY IN
METALLURGY AND MACHINE ENGINEERING

23 квітня 2025 року

м. Дніпро

СЕКЦІЯ 1

СИСТЕМНИЙ АНАЛІЗ І СИНТЕЗ ПРОЦЕСІВ У МЕТАЛУРГІЇ ТА МАШИНОБУДУВАННІ

SECTION 1

SYSTEM ANALYSIS AND SYNTHESIS OF PROCESSES IN METALLURGY AND MECHANICAL ENGINEERING

DOI: 10.34185/1991-7848.itmm.2025.01.117

ІНФОРМАЦІЙНА БЕЗПЕКА В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Шарова Т.М.

Таврійський державний агротехнологічний університет

імені Дмитра Моторного, доктор філологічних наук, професор, Україна

Анотація. *У статті досліджено актуальні виклики інформаційної безпеки в умовах цифрової трансформації, що охоплює всі сфери суспільного життя – від державного управління до освіти та бізнесу. Проаналізовано основні типи загроз, які виникають у процесі впровадження цифрових технологій, зокрема атаки на критичну інфраструктуру, витоки даних, шкідливе програмне забезпечення та соціальну інженерію. Розглянуто сучасні підходи до протидії загрозам, зокрема моніторингу інформаційного середовища та підвищення рівня цифрової культури користувачів. Особливу увагу приділено українському контексту, зокрема досвіду реагування на кібератаки в умовах війни та інтеграції європейських стандартів інформаційної безпеки. Зроблено висновки щодо необхідності міждисциплінарного підходу та розвитку кіберстійкості на всіх рівнях цифрової взаємодії.*

Ключові слова: *цифрова трансформація, інформаційна безпека, кіберзагрози, інтелектуальні системи, штучний інтелект, кіберстійкість.*

Вступ. Сучасний етап розвитку суспільства характеризується стрімкою цифровою трансформацією, яка охоплює всі сфери людської діяльності – від державного управління та освіти до промисловості, охорони здоров’я й побуту. Водночас із розширенням цифрового простору зростає і спектр інформаційних загроз, що ставить під сумнів безпеку як окремих користувачів, так і цілих держав. Поширення технологій Інтернету речей, хмарних обчислень, великих даних і штучного інтелекту створює нові можливості, але й відкриває нові вектори атак для кіберзлочинців. Сучасні дослідники Василенко В., Буряк А. переконують, що «…недостатня захищеність даних може призвести до серйозних наслідків, як-от втрата конфіденційності, втрата довіри клієнтів і партнерів, фінансові втрати та репутаційні проблеми» [1, с. 103].

Особливої актуальності ця проблема набуває в умовах воєнного стану в Україні, коли інформаційна безпека є критично важливою складовою національної безпеки. Масовані кібератаки на державні установи, інфраструктуру та громадянський сектор підкреслюють потребу в системному, інтелектуальному та прогнозованому підході до забезпечення кіберзахисту. У

цьому контексті постає необхідність вивчення не лише сучасних кіберзагроз, а й інструментів і стратегій протидії їм. Саме тому дослідження питань інформаційної безпеки в умовах цифрової трансформації є своєчасним, соціально значущим та має практичну цінність для розроблення ефективних рішень на рівні державної політики, бізнесу та освіти [3, с. 479].

У статті досліджено актуальні виклики інформаційної безпеки в умовах цифрової трансформації суспільства.

Основний матеріал. Цифрова трансформація відкриває широкі можливості для модернізації управлінських процесів, покращення якості послуг, автоматизації виробництва, впровадження інновацій у сфері освіти та охорони здоров'я. Однак вона також супроводжується значним зростанням ризиків, пов'язаних з інформаційною безпекою. Зміна традиційної архітектури ІТ-систем, активне використання віддалених підключень, мобільних пристроїв, хмарних сервісів, систем IoT – усе це розширює потенційні точки вразливості.

До основних викликів інформаційній безпеці на сучасному етапі належать:

1. кіберзагрози нового покоління спрямовані на довготривале проникнення до системи, збирання конфіденційних даних та її виведення з ладу;
2. фішинг і соціальна інженерія, що спрямовані на маніпуляцію поведінкою користувачів з метою отримання доступу до інформації;
3. атаки на критичну інфраструктуру, що можуть спричинити значні збитки не лише економічного, а й гуманітарного характеру;
4. витоки персональних і комерційних даних внаслідок недосконалості систем зберігання або недотримання стандартів безпеки.

У процесі цифрової трансформації організації стикаються з широким спектром загроз інформаційній безпеці, які можуть мати різну природу, складність і наслідки. Для формування ефективної стратегії кіберзахисту необхідно чітко ідентифікувати типи загроз, розуміти їхнє походження та характер впливу на інформаційні системи. З метою систематизації основних небезпек у сфері інформаційної безпеки доцільно здійснити їх класифікацію за різними критеріями, що представлено у таблиці нижче (табл. 1).

Таблиця 1

Класифікація основних загроз інформаційній безпеці

Категорія загрози	Опис	Приклади
Технічні загрози	Пов’язані з вразливостями апаратного чи програмного забезпечення	Віруси, трояни, вразливості ОС і мережевого обладнання
Програмні загрози	Зловмисне програмне забезпечення, яке виконує несанкціоновані дії	Ransomware, Spyware, Botnet, Backdoor
Мережеві загрози	Загрози, що виникають під час передачі даних мережею	DoS/DDoS-атаки, перехоплення трафіку (sniffing), підміна IP-адреси
Соціальна інженерія	Вплив на людину з метою отримання доступу до інформаційних ресурсів	Фішинг, вішинг (голосовий фішинг), baiting (приманка), pretexting (легенда)
Організаційні загрози	Недотримання внутрішніх політик безпеки або їх відсутність	Незахищені паролі, слабкі процедури автентифікації, відсутність резервного копіювання
Загрози з боку персоналу	Дії працівників, навмисні або випадкові, що загрожують безпеці	Витік інформації, шахрайство, порушення політик доступу
Фізичні загрози	Руйнування або пошкодження обладнання через зовнішні фактори	Пожежі, повені, крадіжка обладнання
Гібридні/воєнні кіберзагрози	Кіберінструменти як елемент гібридної війни чи терористичних дій	Кібератаки на державні ресурси, дезінформаційні кампанії

Аналіз поданих у таблиці загроз демонструє, що інформаційна безпека потребує комплексного підходу, який поєднує технічні, організаційні, правові та людські аспекти. Особливої уваги заслуговують загрози соціальної інженерії та внутрішні ризики, оскільки вони є найскладнішими для виявлення. На думку Головка О. «на рівень інформаційної культури людини… впливають численні фактори, серед яких окрему увагу варто приділяти питанням забезпечення цифрових прав людини» [2, с. 40]. У сучасних умовах протидія кожній із категорій загроз має включати використання інтелектуальних засобів виявлення, постійне оновлення систем захисту, розробку політик інформаційної безпеки та навчання персоналу з метою формування кіберкультури в організації. На думку Шопіної І. «ключовим впливом кіберзагроз на освіту є порушення процесів навчання» [4, с. 33]. Ефективна

система кіберзахисту має будуватися на поєднанні технічних, організаційних, правових і освітніх заходів, а також бути гнучкою до змін середовища та здатною до самонавчання.

Висновки. Отже, ефективне забезпечення інформаційної безпеки в епоху цифрової трансформації потребує не лише впровадження сучасних технічних рішень, але й формування комплексної стратегії управління ризиками, що включає правові, організаційні та освітні компоненти. Особливу увагу слід приділяти питанням кібергігієни та розвитку цифрової культури серед працівників. У результаті дослідження встановлено, що загрози соціальної інженерії та внутрішні ризики, спричинені людським фактором, залишаються найменш контрольованими, а отже – найнебезпечнішими.

ЛІТЕРАТУРА

1. Василенко В. Ю., Буряк А. М. Безпека даних в епоху цифрової трансформації: проблеми та виклики. Інформація та соціум. 2024. №1. С. 103 – 106.
2. Головко О. М. Цифрова культура та інформаційна культура: права людини в епоху цифрових трансформацій. Інформація і право. 2019. №4 (31). С. 37 – 44.
3. Шарова Т. М., Землянський А. М. Освіта в інформаційному просторі: цифрове суспільство. Наука і техніка сьогодні. 2023. №14(28). С. 479 – 492.
4. Шопіна І. М. Інформаційна безпека цифрової трансформації. Науковий вісник Львівського державного університету внутрішніх справ (серія юридична). 2023. №1. С. 28 – 35.

INFORMATION SECURITY IN THE ERA OF DIGITAL TRANSFORMATION

Sharova T.

Abstract. *The article explores the current challenges of information security in the context of digital transformation, which affects all areas of public life—from government administration to education and business. The main types of threats arising during the implementation of digital technologies are analyzed, including attacks on critical infrastructure, data breaches, malicious software, and social engineering. Modern approaches to countering these threats are considered, in particular monitoring of the information environment, and the promotion of users' digital literacy and culture. Special attention is given to the Ukrainian context, particularly the experience of responding to cyberattacks during wartime and the integration of European information security standards. The study concludes with the assertion that an interdisciplinary approach and the development of cyber resilience at all levels of digital interaction are essential.*

Keywords: *digital transformation, information security, cyber threats, intelligent systems, artificial intelligence, cyber resilience.*

REFERENCE

1. Vasylenko V. Iu., Buriak A. M. Bezpeka danykh v epokhu tsyfrovoi transformatsii: problemy ta vyklyky. Informatsiia ta sotsium. 2024. №1. S. 103 – 106. [in Ukrainian].
2. Holovko O. M. Tsyfrova kultura ta informatsiina kultura: prava liudyny v epokhu tsyfrovykh transformatsii. Informatsiia i pravo. 2019. №(31). S. 37 – 44. [in Ukrainian].
3. Sharova T. M., Zemlianskyi A. M. Osvita v informatsiinomu prostori: tsyfrove suspilstvo. Nauka i tekhnika sohodni. 2023. №14(28). S. 479 – 492. [in Ukrainian].
4. Shopina I. M. Informatsiina bezpeka tsyfrovoi transformatsii. Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav (seriia yurydychna). 2023. №1. S. 28 – 35. [in Ukrainian].