КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.951
УДК 004.056

Суський Георгій Валерійович
аспірант 3-го року навчання
Інститут програмних систем НАН України, Київ, Україна
ORCID: 0000-0001-8049-1687
nitaet@gmail.com

ВИКЛИКИ І РИЗИКИ ГЛОБАЛІЗАЦІЇ У ФОКУСІ КІБЕРБЕЗПЕКИ

Анотація. Стаття присвячена проблемам і ризикам глобалізації, що спричинила експансію комп'ютерних мереж. Ця експансія нагадує процес вестернізації в епоху пізнього модерну, коли за висловом А.Тойнбі, «всюдисуще» західне суспільство тримало в своїх руках долю всього людства, й поступово розкриває свої недоліки, зокрема, в галузі інформаційної безпеки. Крадіжка даних, незахищеність корпоративних мереж, несанкціонований доступ до інформації, спроби експлуатації вразливості та компроментації систем стали одними з найрозповсюдженіших загроз кібербезпеці інформаційних ресурсів і окремих корпорацій та компаній, і держав в цілому. Пропорційно розвитку можливостей та появі новітніх технологічних рішень, що удосконалюють користування мережами, розвивається і «винахідливість» кіберзловмисників: фішинг, сніфінг (процес перехоплення та аналізу мережевого трафіку за допомогою спеціальних пристроїв та програм), зараження шкідливим програмним забезпеченням тощо. Розширюється спектр та варіативність кіберінцидентів, мішенню атак стають ресурси та бази даних держустанов, об'єктів інфраструктури, корпоративні мережі. Зворотній бік глобалізації проглядається як система викликів та ризиків, що сьогодні мають передбачатись не тільки спеціалістами з кібербезпеки, але й фахівцями з цифровізації у всіх державних та комерційних структурах і компаніях. Комп'ютерні зловмисники використовують все більш витончені прийоми для проникнення в системи і бази даних, розробляють засоби для зараження та розповсюдження шкідливого програмного забезпечення. Назріла необхідність систематизації знань та формування окремих галузей з протидії шкідливим втручанням в мережу та убезпечення баз даних від кібератак.

Ключові слова: мкібербезпека; глобалізація; модернізація; кіберінциденти; інформаційні ресурси.

ВСТУП

Майже століття прагнення людства до глобалізації комунікацій та міжнародних зв'язків було дороговказом до розвитку. Підкріплене прискоренням науково-технічного прогресу, воно набуло апогею в кінці XX ст. – коли після появи глобального телебачення наступним кроком став Інтернет, який зробив можливим моментальне включення у будь-які події світу, що транслювались в мережах.

Здається лише нещодавно, а саме, на початку 2000-х глобалізація тлумачилась як комплексне і багатогранне явище, що сприяло пришвидшенню та суттєвій інтенсифікації транскордонного поширення потоків інформації, технологій, капіталів, товарів, послуг, робочої сили тощо, завдяки чому, як писав Ю. Щербак, «створюється нова світова фінансово-економічна і геополітична архітектура, поглиблюється взаємозалежність держав та національних економік, посилюються інтеграційні процеси і, водночас, загострюються світові суперечності» [1, с. 32].

Постановка проблеми. Глобалізація інформаційного простору висуває унікальні виклики щодо визначення стратегій протидії кіберзлочинності, зокрема через її транскордонний характер та мінливість технологій. Постійне поширення можливостей

та зростання залежності від цифрових технологій, паралельно супроводжується різноманітними векторами атак та швидкими інноваційними циклами у сфері кібербезпеки [2]. Це висуває перед спеціалістами з кібербезпеки, правоохоронними та наглядовими органами вимогу постійно адаптуватися і розвивати свої можливості протидії, щоб ефективно протистояти новим формам кіберзлочинності.

Аналіз останніх досліджень і публікацій. Згадуючи позиції М. Вебера, який заклав візію бачення «нормальності» незахідного світу, наполягаючи, у той же час, на унікальності західного, можна уявити та зрозуміти, чому уніфікаційні підходи до будь-яких проблем глобалізованого світу зазнають концептуальної і практичної поразки. Його думку продовжив Р. Робертсон, вказуючи на процес «розгалуження» модернізації відповідно до локальних можливостей окремих країн та регіонів; він зауважує: «Із моєї власної аналітичної та інтерпретаційної позиції поняття глобалізації передбачало одночасність і взаємопроникнення того, що ми зазвичай називаємо глобальним і локальним, або ж говорячи в абстрактнішому дусі – універсальним і партикулярним»[3, с. 55], вбачаючи одним з основних завдань дослідників глобалізації – осягнути форму структурування нинішнього зсуву в напрямку взаємозалежного світу, акцентуючи при цьому, що «ця форма зосереджується на чотирьохосновних елементах глобально-людського становища: суспільствах, індивідах, міжнародній системі суспільств і людстві» [3, с. 60]. Тим самим Р. Робертсон вказує на сучасні найбільш вразливі щодо «стиснення» інформаційного простору елементи суспільства, у якому в результаті «міжнародних переговорів і технологічних нововведень відбулася стандартизація часопростору, яка неминуче була водночас універсальною і партикулярною» [3, с. 62].

При цьому, всупереч універсалістським прагненням покластися на переваги глобалізації, розходження з західними зразками вже не розцінюється зараз як незавершена форма модернізації. Але саме Ю. Ґабермас (як автор ідеї «незавершеності модерну») протиставив свого часу інструментальній дії (сфера праці, що оперує критеріями ефективності) – дію комунікативну, тобто таку взаємодію двох сторін, що упорядкована згідно обов'язковим нормам. Інструментальна дія орієнтована на успіх, комунікативна – на взаєморозуміння діючих осіб («акторів» комунікативної дії), їх консенсус. Відповідно, Ю. Ґабермас розрізняв раціональність інструментальну (поняття запозичене у М. Вебера) і комунікативну [4, p.184]. Основною відмінністю у розвитку людства на перетині XX і XXI ст. Ю. Габермас вважає те, що певне полегшення експлуатації та перетворення в економічній сфері супроводжуються деформацією (зокрема завдяки засобам масової інформації та розповсюдженню масової культури) усталених структур життєвого світу (сім'ї, добробуту, формам відпочинку, трансформаціям світу думок і почуттів індивіда), що поступово перетворюються на «чужі» форми координації комунікативних дій. На думку теоретика процесів глобалізації та одночасно її критика Ульріха Бека, глобалізація просувається вперед завдяки парадоксальному братанню її супротивників, а з точки зору «переможців глобалізації за все слід дякувати неолібералізму; з точки зору потерпілих від неї через неї розпалюються фобії до чужинців і дозовано вливається отрута реетнізації. Одначе навіть в цьому разі стає зрозумілим, що модернізований фашизм, …йому також довелося б плисти в потоці глобалізації і осмислювати це так, що він прагне не перешкоджати глобалізації, а за можливості прискорювати її. Саме так поводився класичний фашизм, оскільки він також був модернізаційним рухом, який, з одного боку, проповідував кров і землю, а з другого – просував модернізацію тоталітарними методами» [5, с. 356-357]. Передбачення ризиків глобалізації сфокусовані також в комунікаційному ключі й Г. Бехманном, який називає сучасне суспільство «суспільством ризику»; його висновок, що

«всі небезпеки, що загрожують нам, у принципі породжені прийнятими або не прийнятими рішеннями. Ризик як рішення веде до нестабільного стану у майбутньому» [6, p. 69].

Метою статті є висвітлення проблеми зниження інформаційної безпеки як ризику глобалізації, адже безпека даних є однією з найголовніших проблем у мережі Інтернет.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Перебуваючи на передньому краї зіткнення уявлень про багато в чому ідеалізований «глобальний світ», Україна опинилась перед викликами глобалізації в прямому сенсі: з початком повномасштабної російської агресії стало очевидним, що інформаційний простір стає не тільки полем гібридної війни, але й багато постулатів «уніфікації» глобального світу руйнуються під натиском кіберзагроз і кібератак, що множились з самих перших днів російсько-української війни.

Одразу з початком повномасштабного вторгнення країни-агресорки на територію України, а саме: 25 лютого 2022 року, відбулась потужна кібератака з метою перешкоджання виїзду біженців до Румунії на пункті прикордонного контролю. Також відбувались в перші дні (а саме: 28 лютого 2022 року) російської агресії, зафіксовані EEAS, атаки на цифрову інфраструктуру України, з метою блокування доступу до фінансових послуг та енергетичних ресурсів [7]. Вже 10 травня 2022 року верховний представник ЄС засудив атаку проти KA-SAT, яка призвела до перебоїв зі зв'язком для приватних осіб та державних і комерційних структур України. Верховний представник ЄС назвав це «ще одним черговим прикладом безвідповідальної поведінки Росії в кіберпросторі», додавши, що кібератаки, націлені на Україну, «можуть поширитися на інші країни та спричинити системні наслідки, загрожуючи безпеці європейських громадян»[8].

Найбільше, як і раніше, атакують Уряд і місцеві органи влади, оборонний, фінансовий, енергетичний сектори. Залишаються у полі зору кіберзловмисників також транспортна інфраструктура та галузь телекомунікацій[9].

Таблиця 1

Основні сектори, що стають об'єктом кібератак (станом на червень 2022р.)

Сектор	Кількість кібератак
Уряд і місцеві органи влади	179
Сектор безпеки та оборони	104
Фінансовий сектор	55
Комерційні організації	54
Енергетичний сектор	54
Інше	350

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», прийнятого Верховною Радою України 05.10.2017р.[10], центральні повноваження з дотримання безпеки у кіберпросторі (відповідно до статті 5 Закону) забезпечує сам гарант Конституції через очолювану ним Раду національної безпеки і оборони України; Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України; Кабінет Міністрів України та міністерства; центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування; Національний банк України; підприємства, установи та

організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом, авторизованими електронними майданчиками.

Таблиця 2

Найпоширеніші методи кібератак

Методи кібератак	Кількість кібератак
Збір інформації зловмисниками	242
Шкідливий програмний код	192
Втручання в роботу ІКС	92
Спроби втручання	82
Порушення доступності сервісів	56
Інше	132

Останні події в світі, що демонструють розбіжності між країнами «старого» і «нового світу» стосовно завершення російсько-української війни суттєво підривають уявлення теоретиків політики та міжнародних відносин щодо «реконфігурації» союзу демократій навколо основного ядра – США та Європейського Союзу [11]. Довготривале уявлення, що тісне партнерство США та ЄС стане «головною засадою глобалізованого світового порядку у XXI столітті» [12], було зруйноване агресивними діями росії щодо України та намаганням затягування російсько-української війни за рахунок маніпулювання ресурсами західної допомоги Україні протягом цієї війни.

Саме передбаченням ризиків зумовлюється змагальний характер у розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо, забезпечує швидке удосконалення цих засобів і систем. Також на актуальний розвиток систем кібербезпеки України повпливали:

а) мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;

б) вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинив стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;

в) впровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що потребує удосконалення в частині заходів з кібербезпеки та без належної оцінки ризиків.

Привертає увагу, проаналізоване А.О. Твердохлібом, використання блокчейн-технологій у кібербезпеці. Автор підкреслює, що «однією з найвагоміших переваг блокчейн-технології є її децентралізований характер. На відміну від традиційних централізованих систем управління даними, що містять єдину точку відмови, блокчейн розподіляє інформацію між усіма вузлами мережі, що істотно ускладнює можливість компрометації системи шляхом атак на окремий сервер» [13, с. 210]. Також, наводячи порівняльну таблицю (див. табл.3) методів кібербезпеки [Ibid], автор класифікує їх за певними аспектами безпеки, порівнюючи традиційні методи та блокчейн-рішення, що можна вважати надзвичайно актуальним.

Таблиця 3

Порівняльна таблиця методів безпеки

Аспект безпеки	Традиційні методи	Блокчейн-рішення
Централізація	Централізований сервер	Децентралізована мережа
Захист даних	Може бути змінений адміністратором	Неможливо змінити запис без консенсусу
Аутентифікація	Логін/пароль, двофакторна аутентифікація	Криптографічні ключі, смарт-контакти
Контроль доступу	ACL, рольові моделі	Автоматизовані смарт-контакти
Стійкість до атак	Слабка стійкість до DDOS-атак	Висока стійкість до DDOS-атак
Прозорість та аудит	Закриті журнали подій	Публічний незмінний реєстр
Автоматизація безпеки	Потребує людського втручання	Автоматичне виконання правил безпеки

Одними з найбільших загроз для стійкості країни та розвитку у період її відновлення, очевидно, є кібератаки на економіку та інфраструктуру, що забезпечує безперешкодну реалізації економічних зв'язків, фінансових трансакцій, контрактів тощо. Треба згадати, що найбільш активними послідовними критиками глобалізації були саме американські економісти Д. Барбер, П. Бьюкеннен, Дж. Голдсміт, Г. Дейлі, Д. Кортон, ін. У цьому контексті, необхідно згадати також праці Е. Гідденса [14], В. Гаттона [15] та Е. Тофлера [16], де «глобалізація розглядається як потужна трансформуюча сила, відповідальна за усестороннє «перетряхування» суспільств, економіки, інститутів та світового порядку. Але напрямок такого «перетряхування» розуміється як випадковий, оскільки глобалізація за своєю сутністю - випадковий історичний процес, повний суперечностей» [17, с. 3].

У цьому зв'язку можна згадати й цивілізаційну теорію С. Ґантінгтона, який запропонував власну типологію модернізації. Згідно думки С. Ґантінгтона [18], руйнація традиційного суспільства, яка йде шляхом вестернізації без модернізації не має перспектив (наприклад, Філіппіни Єгипет, ін.). Однак, не має успіху й зворотній процес – модернізація без «вестернізації», тобто така модернізація, яка відбувається на ґрунті власної ідентичності; наприклад, модернізація Японії та низки інших країн Південно-Східної Азії. С. Ґантінгтон передбачав, що цей спосіб перетворень перебуває у кризовому періоді також через ті обставини, що зразок для наслідування, а саме – Захід, наразі сам зазнає суттєвих змін [18]. Основним типом розвитку, на його думку була так звана «наздогоняюча модернізація» (Мексика, Росія, Турція, ін). Результати реалізації політики «наздоганяючої модернізації», згідно з думкою А.С. Гальчинського, є очевидними: «світосистема, яка заснована на принципах індустріального капіталізму, на засадах євроцентризму, пройшла пік свого розвитку і вочевидь наблизилась до своїх логічних меж»[19, с.66]. Про це свідчать не лише економічні суперечності, а й глибокий світоглядний вакуум, який спричинений, щонайперше, тим що рух прогресу уперед відповідно завчасно заданій траєкторії, за моделями, що нав'язуються суспільству ззовні, призводить найчастіше до інтелектуальної деградації, спустошення свідомості особистості; «не глобальний (насамперед економічний) розвиток глобалізує особистість, а навпаки – енергія самозбагачення особистості породжує енергію глобалізаційного процесу» [19, с. 64].

Інтернет-мережі, які слугували колись виключно дослідницьким та навчальним цілям, науковцям, чиї інтереси «тягнулись» аж до доступу до суперкомп'ютерів, стали найбільш популярними саме в ділових колах. Компанії в усьому світі цінують швидкість, дешевий глобальний зв'язок, зручність для проведення спільних робіт, доступні програми, унікальні бази даних. Деякі компанії розглядають глобальну мережу як

доповнення до своїх власних локальних мереж. Проте, не слід забувати, що Інтернет та інформаційна безпека несумісні за самою своєю природою. Глобальна мережа народилась спочатку як чисто корпоративна, проте, на даний час, за допомогою єдиного стека протоколів TCP/IP та єдиного адресного простору, вона об'єднує не лише корпоративні та відомчі мережі установ, корпорацій і цілих соціальних інститутів (державні, військові, освітні, комерційні тощо), які мають бути, за визначенням, мережами з обмеженим доступом. Це також стосується і пересічних користувачів, які мають можливість отримати прямий доступ в мережу Інтернет зі своїх робочих або домашніх комп'ютерів чи зі смартфонів. Проте, чим легший та простіший доступ в мережу, тим гірша її інформаційна безпека, стійкість до кібератак, адже користувач може й не дізнатися, що у нього були скопійовані файли чи програми, не кажучи про можливість шкідливих підключень, псування програмного забезпечення, фішингу, несанкціонованої модифікації, зараження шкідливим програмним забезпеченням тощо. Отже, безпека даних є однією з найголовніших проблем здійснення мережевого пошуку, доступу до розподілених ресурсів, електронних архівів, баз документообігу, ін. Таким чином, запорукою розвитку глобалізаційних процесів та інтеграції економічних, соціополітичних та культурних зв'язків є кібербезпека.

На думку фахівців з міжнародного права О. Панасюка, С. Олійник та В. Литовченка, «поширене розуміння глобалізації передбачає три її головні аспекти: економіку, культуру та політику»[20, с. 4]. Проте, крім позитивних аспектів, глобалізація має ще й негативні, наприклад, О. Євтушенко та Ю. Горенко виділяють такі: зростання розриву між багатими і бідними прошарками населення (як в межах одного суспільства, так і між різними країнами); цифровий та інформаційно-технічний розрив (між тими, хто має постійний доступ до Інтернету, і тими, хто його не має); нерівність у розподілі доходів; підрив національного суверенітету; виникнення суперечностей, конфліктів, воєн між державами; нераціональне використання природних ресурсів; постійне зростання тіньового бізнесу, корупції; прояви тероризму, екстремізму [21, с. 209]. Особливо останнє тісно пов'язане з питаннями кібербезпеки, адже саме через комп'ютерні мережі проходять найбільші масиви інформації, що створює небезпеку втручання як в ідеологічну сферу та свідомість громадян різних країн, так і спрямовується на руйнування та дестабілізацію роботи важливих промислових та інфраструктурних об'єктів. На думку О.В. Саган, «активізацію інформаційного тероризму зумовили три чинники: масовізація інформаційних технологій, що призвела до зміни сенсу інформації, від якої залежить повсякденне життя людини; демасифікація суспільного буття, що перебуває в залежності від медіа; глобальна система комунікації, що відкрила кожну націю для зовнішнього впливу» [22, с.14-15].

Згідно даних, опублікованих в Інформаційному бюлетені Генштабу Збройних Сил України «Стан кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури» (за 17.08.2025 р.) [23, с. 3], найбільше кіберінцидентів припадає на такі їх різновиди: а) сканування – 3628454 випадків; б) спроби експлуатації вразливості – 80344; в) спам – 33065; г) шкідливі підключення – 3201; д) спроби авторизації/входу в систему – 2234; е) несанкціонований доступ до інформації – 818; є) розповсюдження шкідливого програмного забезпечення – 748; а також ще 1088 невизначених інцидентів (табл.4):

Таблиця 4

Статистична інформація щодо стану кіберзахисту ДІР (кіберінциденти). (Дані на 17.08.2025).

№	Тип інциденту	Кількість атак
1	Спам	33065
2	Зараження шкідливим програмним забезпеченням	35
3	Розповсюдження шкідливого програмного забезпечення	748
4	Шкідливе підключення	3201
5	Сканування	3628454
6	Сніфінг	0
7	Фішинг	326
8	Спроба експлуатації вразливості	80344
9	Спроба авторизації/входу в систему	2234
10	Компроментація облікового запису	0
11	Компроментація системи	90
12	Атака на відмову в обслуговуванні	24
13	Саботаж /шкідливі дії	0
14	Збій	0
15	Несанкціонований доступ до інформації	818
16	Несанкціонована модифікація	0
17	Шахрайський сайт	0
18	Вразливість	6
19	Некоректна конфігурація	7
20	Невизначений інцидент	1088
	Всього	3750440

Джерело: Інформаційний бюлетень Генштабу Збройних Сил України «Стан кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури» (за 17.08.2025 р.), с.3.

В результаті осмислення ролі глобалізаційних процесів, можна дійти до висновку, що хоч «глобалізація» є одним з ключових слів нашого часу й визначає розуміння нашого «взаємопов'язаного світу», як зауважують Манфред Штегер та Пауль Джеймс (Manfred Steger & Paul James), проте «цей термін неоднозначний, а поняття, що має багато значень, зазвичай використовується для позначення розширення та посилення соціальних відносин у всьому світі. Було написано багато робіт, присвячених різним аспектам глобалізації. Однак дивно, що жодна критична історія цієї концепції досі не надала історичного відображення її концептуального походження, еволюції та генеалогічних ліній»[24, p.1]. Події останніх років першої чверті XXI ст. підтверджують, що глобалізації властиві не лише позитивні аспекти, адже вона несе з собою й безліч викликів і ризиків. Особливо важливими постають тут виклики безпеки мереж та захисту інформаційного простору України, коли кібератаки стають інструментом гібридного впливу та прямого втручання в суверенний простір держави.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Критичні зауваги щодо процесів глобалізації, її викликів і ризиків не тільки ставлять запитання, на які не завжди можливо знайти однозначні відповіді, а й розкривають парадокси протікання цих процесів на різних рівнях. Увагу науковців привертає й те, що теоретичні розвідки і практичні платформи сучасних трансформацій в галузі кібербезпеки багато в чому не збігаються. Саме тому сьогодні вже можна говорити про оформлення напряму не тільки структурованої критики глобалізації, але й

про розгортання доказового теоретизування на предмет наявності та нейтралізації парадоксів глобалізації, незважаючи на активність протікання й незавершеність – з одного боку, та інтеграційну значущість процесів інформаційного обміну в усьому світі та технологічне всезагальне охоплення глобалізаційними змінами – з іншого.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shcherbak, Yu. (2003). *Ukraina: vyklyk i vybir. Perspektyvy Ukrainy u hlobalizovanomu sviti XXI stolittia* [Ukraine: Challenge and Choice. Ukraine's Prospects in the Globalized World of the 21st Century]. Kyiv: Dukh i Litera.
2. Koziura, V. D., Khoroshko, V. O., Shelest, M. Ye., Tkach, Yu. M., & Baliunov, O. O. (2020). *Zakhyst informatsii v komp'iuternykh systemakh: pidruchnyk* [Information Protection in Computer Systems: Textbook]. Nizhyn: TPK "Orkhideia."
3. Robertson, R. (2008). Glocalization: Time–Space and Homogeneity–Heterogeneity. In M. Featherstone, S. Lash, & R. Robertson (Eds.), *Global Modernities* (pp. 48–73). Kyiv: Nika-Center.
4. Habermas, J. (1981). *Theorie des kommunikativen Handelns* (Vol. 2). Frankfurt am Main: Suhrkamp.
5. Beck, U. (2015). *Vlada i kontrvlada u dobu hlobalizatsii. Nova svitova politychna ekonomiia* [Power and Counterpower in the Age of Globalization. The New World Political Economy]. Kyiv: Nika-Center.
6. Bechmann, G. (2005). Risk and rationality in a future-oriented society. In *Rationality in an Uncertain World* (Vol. 1, pp. 60–75). Series: Gesellschaft – Technik – Umwelt.
7. European External Action Service (EEAS). (2022, March 21). *A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security*. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf
8. Menn, J. (2022, May 1). Hacking Russia was off-limits. The Ukraine war made it a free-for-all. *The Washington Post.* https://www.washingtonpost.com/technology/2022/05/01/russia-cyber-attacks-hacking/
9. Derzhspetszviazok. (2022, June). *Statystyka kiberatak za chotyry misyatsi viiny* [Statistics of Cyberattacks During Four Months of the War]. The Unified Web Portal of the Executive Authorities of Ukraine. https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni
10. Verkhovna Rada of Ukraine. (2017). *Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy"* [Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine"]. https://zakon.rada.gov.ua/laws/show/2163-19#Text
11. Modelski, G., Devezas, T., & Thompson, W. R. (Eds.). (2008). *Globalization as Evolutionary Process: Modeling Global Change.* Routledge.
12. Modelski, G. (2005). Long-term trends in world politics. *Journal of World-Systems Research, 11*(2), 195–206.
13. Tverdokhlib, A. O. (2025). Methods for ensuring cybersecurity in high-load computer systems using smart contracts. *Cybersecurity: Education, Science, Technique, 4*(28), 206–216.
14. Giddens, A. (2000). *Runaway World: How Globalization is Reshaping Our Lives.* New York: Routledge.
15. Hutton, W., & Giddens, A. (Eds.). (2000). *On the Edge: Living with Global Capitalism.* London: Jonathan Cape.
16. Toffler, A. (1981). *The Third Wave: The Classic Study of Tomorrow.* New York: Random House Publishing Group.
17. Palii, K. S. (2014). *Hlobalizatsiia yak superechlyva realnist isnuvannia suchasnoho svitu* [Globalization as a Contradictory Reality of the Modern World's Existence]. *Visnyk Kharkivskoho Natsionalnoho Universytetu im. V. N. Karazina. Seriia "Teoriia kultury i filosofiia nauky," 50*(1092). Kharkiv.
18. Huntington, S. P. (1996). *The Clash of Civilizations and the Remaking of World Order*. New York: Simon & Schuster.
19. Halchynskyi, A. S. (2015). *Stanovlennia hlobalnoho suspilstva ta perspektyvy hlobalnoho informatsiino-merezhevoho suspilstva* [Formation of the Global Society and Prospects of the Global Information-Network Society]. *Naukovyi Visnyk Dyplomatychnoi Akademii Ukrainy, 22*(3), 62–72. http://nbuv.gov.ua/UJRN/Nvdau_2015_22%283%29__8
20. Panasiuk, O. P., Oliinyk, S. M., & Lytovchenko, V. P. (2024). Globalization and its challenges to national sovereignties: Analysis of the impact of globalization processes on modern international law. *Akademichni Vizii, 33*, 1–12. https://doi.org/10.5281/zenodo.12625395 https://www.academy-vision.org/index.php/av/article/view/1238

21. Yevtushenko, O., & Horenko, Yu. (2024). The nation-state under globalization and global democracy. *Public Administration and Regional Development, 23*, 199–224.
22. Sahan, O. V. (2021). *Protydiia media-informatsiinomu teroryzmu yak pytannia natsionalnoi bezpeky Ukrainy* [Countering Media-Information Terrorism as a National Security Issue of Ukraine] (Doctoral dissertation, National Academy of Public Administration). Kyiv.
23. General Staff of the Armed Forces of Ukraine. (2025, August 17). *Stan kiberzakhystu derzhavnykh informatsiinykh resursiv ta obiektiv krytychnoi infrastruktury* [The State of Cyber Defense of State Information Resources and Critical Infrastructure Objects]. Information Bulletin. Kyiv.
24. Steger, M., & James, P. (Eds.). (2015). *Globalization: The Career of a Concept.* Routledge.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

Heorhii Suskiy
аспірант 3-го року навчання
Інститут програмних систем НАН України, Київ, Україна
ORCID: 0000-0001-8049-1687
nitaet@gmail.com

DEVELOPMENT OF A TEST ENVIRONMENT FOR EVALUATING THE EFFECTIVENESS OF IMPLEMENTED APPLICATION-LEVEL SECURITY MEASURES

Abstract: The article is devoted to the problems and risks of globalization, which caused the expansion of computer networks. This expansion resembles the process of Westernization in the era of late modernity, when, according to A. Toynbee, the "ubiquitous" Western society held the fate of all humanity in its hands, and is gradually revealing its shortcomings, in particular, in the field of information security. Data theft, insecurity of corporate networks, unauthorized access to information, attempts to exploit vulnerabilities and compromise systems have become one of the most common threats to the cybersecurity of information resources and individual corporations and companies, and states as a whole. In proportion to the development of capabilities and the emergence of new technological solutions that improve the use of networks, the "ingenuity" of cybercriminals is also developing: phishing, sniffing (the process of intercepting and analyzing network traffic using special devices and programs), infection with malicious software, etc. The spectrum and variability of cyber incidents is expanding, the targets of attacks are resources and databases of state institutions, infrastructure facilities, corporate networks. The reverse side of globalization is seen as a system of challenges and risks, which today must be foreseen not only by cybersecurity specialists, but also by digitalization specialists in all state and commercial structures and companies. Computer attackers use increasingly sophisticated methods to penetrate systems and databases, develop tools for infection and distribution of malicious software. There is a need to systematize knowledge and form separate branches to counteract malicious interference in the network and secure databases from cyberattacks.

Keywords: cybersecurity; globalization; modernization; cyber incidents; information resources.

REFERENCES

1. Shcherbak, Yu. (2003). *Ukraina: vyklyk i vybir. Perspektyvy Ukrainy u hlobalizovanomu sviti XXI stolittia* [Ukraine: Challenge and Choice. Ukraine's Prospects in the Globalized World of the 21st Century]. Kyiv: Dukh i Litera.
2. Koziura, V. D., Khoroshko, V. O., Shelest, M. Ye., Tkach, Yu. M., & Baliunov, O. O. (2020). *Zakhyst informatsii v komp'iuternykh systemakh: pidruchnyk* [Information Protection in Computer Systems: Textbook]. Nizhyn: TPK "Orkhideia."
3. Robertson, R. (2008). Glocalization: Time–Space and Homogeneity–Heterogeneity. In M. Featherstone, S. Lash, & R. Robertson (Eds.), *Global Modernities* (pp. 48–73). Kyiv: Nika-Center.
4. Habermas, J. (1981). *Theorie des kommunikativen Handelns* (Vol. 2). Frankfurt am Main: Suhrkamp.
5. Beck, U. (2015). *Vlada i kontrvlada u dobu hlobalizatsii. Nova svitova politychna ekonomiia* [Power and Counterpower in the Age of Globalization. The New World Political Economy]. Kyiv: Nika-Center.
6. Bechmann, G. (2005). Risk and rationality in a future-oriented society. In *Rationality in an Uncertain World* (Vol. 1, pp. 60–75). Series: Gesellschaft – Technik – Umwelt.
7. European External Action Service (EEAS). (2022, March 21). *A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security*. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf
8. Menn, J. (2022, May 1). Hacking Russia was off-limits. The Ukraine war made it a free-for-all. *The Washington Post*. https://www.washingtonpost.com/technology/2022/05/01/russia-cyber-attacks-hacking/
9. Derzhspetszviazok. (2022, June). *Statystyka kiberatak za chotyry misyatsi viiny* [Statistics of Cyberattacks During Four Months of the War]. The Unified Web Portal of the Executive Authorities of Ukraine. https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni

10. Verkhovna Rada of Ukraine. (2017). *Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy"* [Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine"]. https://zakon.rada.gov.ua/laws/show/2163-19#Text
11. Modelski, G., Devezas, T., & Thompson, W. R. (Eds.). (2008). *Globalization as Evolutionary Process: Modeling Global Change.* Routledge.
12. Modelski, G. (2005). Long-term trends in world politics. *Journal of World-Systems Research, 11*(2), 195–206.
13. Tverdokhlib, A. O. (2025). Methods for ensuring cybersecurity in high-load computer systems using smart contracts. *Cybersecurity: Education, Science, Technique, 4*(28), 206–216.
14. Giddens, A. (2000). *Runaway World: How Globalization is Reshaping Our Lives.* New York: Routledge.
15. Hutton, W., & Giddens, A. (Eds.). (2000). *On the Edge: Living with Global Capitalism.* London: Jonathan Cape.
16. Toffler, A. (1981). *The Third Wave: The Classic Study of Tomorrow.* New York: Random House Publishing Group.
17. Palii, K. S. (2014). *Hlobalizatsiia yak superechlyva realnist isnuvannia suchasnoho svitu* [Globalization as a Contradictory Reality of the Modern World's Existence]. *Visnyk Kharkivskoho Natsionalnoho Universytetu im. V. N. Karazina. Seriia "Teoriia kultury i filosofiia nauky," 50*(1092). Kharkiv.
18. Huntington, S. P. (1996). *The Clash of Civilizations and the Remaking of World Order.* New York: Simon & Schuster.
19. Halchynskyi, A. S. (2015). *Stanovlennia hlobalnoho suspilstva ta perspektyvy hlobalnoho informatsiino-merezhevoho suspilstva* [Formation of the Global Society and Prospects of the Global Information-Network Society]. *Naukovyi Visnyk Dyplomatychnoi Akademii Ukrainy, 22*(3), 62–72. http://nbuv.gov.ua/UJRN/Nvdau_2015_22%283%29__8
20. Panasiuk, O. P., Oliinyk, S. M., & Lytovchenko, V. P. (2024). Globalization and its challenges to national sovereignties: Analysis of the impact of globalization processes on modern international law. *Akademichni Vizii, 33*, 1–12. https://doi.org/10.5281/zenodo.12625395 https://www.academy-vision.org/index.php/av/article/view/1238
21. Yevtushenko, O., & Horenko, Yu. (2024). The nation-state under globalization and global democracy. *Public Administration and Regional Development, 23*, 199–224.
22. Sahan, O. V. (2021). *Protydiia media-informatsiinomu teroryzmu yak pytannia natsionalnoi bezpeky Ukrainy* [Countering Media-Information Terrorism as a National Security Issue of Ukraine] (Doctoral dissertation, National Academy of Public Administration). Kyiv.
23. General Staff of the Armed Forces of Ukraine. (2025, August 17). *Stan kiberzakhystu derzhavnykh informatsiinykh resursiv ta obiektiv krytychnoi infrastruktury* [The State of Cyber Defense of State Information Resources and Critical Infrastructure Objects]. Information Bulletin. Kyiv.
24. Steger, M., & James, P. (Eds.). (2015). *Globalization: The Career of a Concept.* Routledge.