DOI: https://doi.org/10.32782/2524-0072/2026-85-174

УДК 330.43:338.2

ЕКОНОМІКО-МАТЕМАТИЧНА МОДЕЛЬ ВПЛИВУ ЦИФРОВОЇ ГРАМОТНОСТІ НА ФІНАНСОВІ РИЗИКИ КІБЕРПРОСТОРУ: ПОРІВНЯЛЬНИЙ АНАЛІЗ КРАЇН ЄС ТА УКРАЇНИ

ECONOMIC-MATHEMATICAL MODEL OF THE IMPACT OF DIGITAL LITERACY ON CYBERSECURITY FINANCIAL RISKS: A COMPARATIVE ANALYSIS OF EU COUNTRIES AND UKRAINE

Лінгур Любов Миколаївна
кандидат економічних наук, доцент,
Національний університет «Одеська політехніка»
ORCID: https://orcid.org/0000-0002-0730-2381

Lingur Liubov
Odessa Polytechnic National University

Досліджене взаємозв'язок між цифровими навичками з кібербезпеки та обсягом фінансових втрат від кіберзлочинів у країнах ЄС та України. Актуальність підтверджується даними ENISA, Europol IOCTA 2025 та НКЦК. На основі індексів DSI за 2021–2025 роки побудовано регресійну модель залежності фінансового ризику від цифрових навичок з кібербезпеки та ринкової вартості витоку даних з показниками якості R^2=0,90; F=32,03. Підтверджено існування критичного порогу цифрових навичок, досягнення якого знижує ефективність атак соціальної інженерії. Виявлено три зони стійкості по країнах: з низькими навичками (Румунія, Болгарія), перехідним рівнем (Німеччина, Франція, Україна) та цифрові фортеці (Нідерланди, Данія, Естонія). Зростання навичок на 1% знижує ризик на 1,93 бали, а підвищення вартості даних на 1 пункт збільшує на 16,52 бали, що обґрунтовує необхідність поєднання освітніх та технологічних інструментів захисту.

Ключові слова: кібербезпека, соціальна інженерія, фінансові втрати від кіберзлочинів, цифрові навички, кібергігієна, регресійна модель, індекс фінансового ризику.

The relationship between the level of digital literacy of the population in the field of cybersecurity and the volume of financial losses from cybercrime in the Member States of the European Union and in Ukraine has been studied. The relevance of the study is driven by the rapid and accelerating growth of damages caused by cyber fraud, as consistently documented in regular reports by ENISA, Europol (IOCTA 2025), and NCCC. The study is grounded in the premise that the human factor remains the most critical vulnerability in the cybersecurity chain, with over 60% of successful cyber incidents relying on social engineering techniques. Despite significant advances in technical protection systems, the behavioral and educational dimensions of cybersecurity continue to be underexplored in quantitative research, particularly with respect to their direct financial impact at the national level. Using data from the Digital Economy and Society Index (DESI), the Digital Skills Indicator (DSI) covering the period 2021–2025, and findings from Europol IOCTA 2023, 2025 and ENISA 2025 reports, a multivariate regression model was constructed to quantify the dependence of the Financial Risk Index on two key variables: the level of cybersecurity digital skills among the population and the market value of data breaches. The model demonstrates high statistical reliability, with a coefficient of determination R^2=0.90, and Fisher's criterion F=32.03, confirming its validity and practical applicability. The findings confirm the hypothesis that a critical threshold of digital competence exists, above which the effectiveness of social engineering attacks is substantially reduced and mass cyber fraud becomes economically unviable for perpetrators. Three distinct zones of digital resilience were identified: low-skill (Romania, Bulgaria), transitional-level (Germany, France, Ukraine), and "digital fortresses" (Netherlands, Denmark, Estonia). The analysis established that a 1% increase in cybersecurity skills reduces the Financial Risk Index by 1.93 points, while a one-point rise in data value increases the risk index by 16.52 points. This asymmetry highlights the need to combine broad-based educational initiatives with advanced technological protection measures. The case of Ukraine is

highlighted as particularly instructive: despite lower living standards, the country has achieved a transitional level of cyber resilience through intensive awareness programs, real-world exposure to threats, and national digital literacy platforms, demonstrating that education-driven cybersecurity can be a powerful instrument of economic protection.

Keywords: cybersecurity, social engineering, cybercrime financial losses, digital skills indicator, cyber hygiene, regression model, financial risk index.

Постановка проблеми. Стрімке впровадження цифрових технологій в архітектуру державного управління та фінансовий сектор країн Європейського Союзу та України створило нову парадигму соціо-технічних ризиків. Попри технологічну досконаліть сучасних систем кіберзахисту, «людський фактор» залишається найбільш критичною ланкою в ланцюгу забезпечення інформаційної безпеки. За даними ENISA (2025), понад 60% успішних кіберінцидентів базуються на методах соціальної інженерії, що призводить до мільярдних прямих фінансових втрат. Так, по оцінках ENISA глобальні світові збитки лише від інвестиційного шахрайства у 2024 році оцінюються від 9,1 до 11,4 млрд євро, демонструючи річне зростання на 40%.

Розгляд окремих методів та технології соціальної інженерії наводить на гіпотезу, що основної причиною успішності шахрайських схем є недостатня усвідомленість населення та бізнесу о правилах кібербезпеки, дотримання їх, підвищення рівня цифрових навичок, особливо в галузі кібергігієни та кібербезпеки.

Аналіз останніх досліджень і публікації. Проблематика кібербезпеки у особистому житті та фінансовій сфері є предметом активних досліджень. Дослідження зарубіжних науковців показують, що персональна цифрова безпека залежить від суб'єктивного сприйняття загроз та впевненості у ефективності особистих дій по захисту інформації як підкреслює О. Шульга [15]; вік, знання та навички також впливають на рівень обізнаності про кіберзагрози, особливо для старшого покоління стверджується у М. Бучі та інш. [2]; а Л. Богнар та Л. Боттиан [1] виокремлюють структурні умови – наприклад UX-налаштування за замовчуванням, політика, регулювання сприймаються молоддю як додаткові обмеження. Українські науковці ставлять на перше місто поширення заходів кібербезпеки за ініціативою та відповідальністю держави. Так, у роботах О. Гиляки [14] та О. Шульги [15] надані рекомендації починати зі створення ефективного нагляду за захистом персональних даних, просування безпечних інтернет-технологій і відмову від заборони шифрування на законодавчому рівні. Автори Ю. Кокарча та А. Лалуєва [5] навпаки пропонують користувачам турбуватися про свою кібербезпеку самостійне: підвищувати цифрову грамотність, усвідомити цінність персональних даних, приділяти увагу політикам конфіденційності, реалізації прав на доступ, редагування, видалення. У роботі І. Гончаренко [3] наведена інформація з фінансових втрат у 2022 році від незаконних операцій у банківської сфері в 481 млн грн. Обґрунтування залежності між рівнем навичок цифрової безпеки населення та його фінансової стійкості та опис системи практичних рекомендацій щодо зменшення кіберризиків надається С. Кучеренко [6]. Автори Маслій О., Буряк А., Науменко О. [7] систематизують детермінанти економічної безпеки держави та підкреслюють багатовимірність впливу цифровізації на національну економіку. Висновком роботи є концепція стратегії економічної безпеки в умовах Індустрії 4.0, яка включає підвищення показників цифрових навичок.

Нерозглянутими у роботах українських та зарубіжних авторів залишаються питання визначення достовірної моделі залежності між фінансовими втратами країн та населення від рівня цифрових навичок саме з питань кібербезпеки та гігієни.

Мета дослідження. Метою статті є виявлення та математичне обґрунтування кореляційної залежності між індексом цифрової грамотності населення, частиною якого є рівень навичок з кібербезпеки, та обсягом фінансових збитків від кіберзлочинів з побудовою регресійної моделі парадоксу цифровізації. У роботі перевіряється гіпотеза про наявність критичного порогу цифрової компетентності, досягнення якого дозволяє радикально знизити ефективність кібератак, що базуються на соціальній інженерії.

Наукова новизна дослідження полягає у розробці моделі ефективності цифрової гігієни та аналізі прогнозних загроз в умовах індустріалізації фішингу за допомогою технологій штучного інтелекту.

Виклад основного матеріалу дослідження. З 2014 року Європейська Комісія

визначає та публікує Індекс DESI (Digital Economy and Society Index). У 2023 році Кабінет Міністрів України в якості кроку до євроінтеграції цифрового простору, затвердив перелік показників DESI для розрахунку в країні. Одним з важливих показників індексу DESI виступають цифрові навички населення. Однак, визначення індексу ніяк не пов'язане з фінансовими показниками втрат з-за недотримання правил кібербезпеки.

Щорічний звіт Europol IOCTA 2025 підкреслює, що збитки з-за кіберзлочинів підвищуються особливо в країнах з високим рівнем життя. Хоча високий рівень ВВП не завжди означає високий рівень обізнаності до цифрової гігієни. Тут значну роль відіграє вартість інформації на тіньових ринках. Відмічається також чітка залежність для країн з середнім рівнем ВВП між цифровими навичками та патернами поведінки [18].

В цілому, данні по втратах фізичних осіб від шахрайських дії не розповсюджуються з різних причин. Але, фахівці з кібербезпеки холдингу SHERIFF наполягають, що для українського бізнесу втрати можуть сягати від 100 до 500 тис. доларів за один виток даних [19].

Виявлені тенденції свідчать про виникнення явної кореляційної залежності: країни з високим рівнем проникнення цифрових послуг, але недостатньою динамікою зростання цифрової грамотності населення (Франція, Німеччина, Італія), демонструють вищу вразливість порівняно з «цифровими фортецями» (Данія, Естонія, Фінляндія). Україна збирає інформацію для DESI, тому її досвід також можна врахувати в моделі. За роки повномасштабного вторгнення інтенсивність кібератак на критичну інфраструктуру та логістику тільки збільшується, але цифрові навички населення зростають щорічно, демонструючи високий рівень адаптивності бізнесу та населення як ключового фактору національної кіберстійкості.

Як свідчить звіт Europol IOCTA 2025, формування фінансових втрат відбувається за циклічною моделлю «Steal, Deal, Repeat». Успішність таких механізмів ґрунтується на низькому рівні цифрової гігієни користувачів. Часто використовується неліцензійне ПЗ, паролі зберігаються у браузерах, паролі не надійні, ставлення до кібергігієни по остаточному принципу, що призводить до масового зараження пристроїв інфостілерами. Завдяки чому, викрадені облікові записи стають товаром на підпільних маркетплейсах, де ціна за доступ до одного європейського домогосподарства або компанії корелює з рівнем добробуту країни. Чим вище вартість життя, особистої інформації, тим вище вартість викрадених даних, що в цілому стимулює професіоналізацію кіберзлочинності, створення методів соціальної інженерії та використання генеративного ШІ для обходу базових навичок цифрової грамотності населення. Таким чином, країни ЄС з потужною економікою мають високий Індекс фінансового ризику [18].

Цифрові навички є частиною індексу DESI та визначаються за допомогою Індикатора цифрових навичок (DSI). Цей показник розраховується на основі опитувань за допомогою платформи DigComp 3.0 [12] та враховує знання, навички та підходи користувачів у п'яти сферах компетенцій:

– комп'ютерна та інформаційна грамотність;
– комунікація та співпраця;
– створення цифрового контенту;
– вирішення проблем;
– навички безпеки.

Тобто, знання та вміння хоча б одного інструмента у перелічених сферах надає базовий рівень цифрової грамотності; наявність 1-2 компетентностей у кожної сфері надає рівень «вище базового».

Результати узагальнення показника DSI за 2021, 2023, 2025 роки (оцінка проводиться раз на 2 роки) наведені на рисунку 1.

На діаграмі представлені усереднені данні за 3 опитування.

Насиченість кольору відображає рівень досягнутих цифрових навичок. Тільки Нідерланди та Фінляндія перетнули 80% ціль Цифрового десятиліття 2030. Наблизилися до неї Ірландія та Данія (75 та 73 %). Найменші значення демонструють Румунія та Болгарія. Україна (56,43%) не є членом ЄС, але також збирає данні щодо визначення індексу DESI. Такій поділ слугує підґрунтям до подальшого формулювання гіпотези – чим вище рівень цифрових навичок населення, тим менш фінансова вразливість особистості та країни в цілому від кібезшахрайства та кіберзагроз. Але, для перевірки гіпотези необхідне оцінити загальні втрати як населення так і країн суто від кіберзагроз та недотримання кібергігієни.

Окремого виділення по сфері кібербезпеки DSI не розраховує. Але, для формулювання цільової моделі залежності такі данні представляють найбільший інтерес. Тому, для подальшого дослідження, були використані деталізовані набори даних по розрахунках

Рис. 1. Індикатор цифрових навичок країн ЄС за 2021-25 роки

Джерело: сформовано на основі [10]

базових навичок з кібербезпеки за 2021, 2023, 2025 роки та проведене їх узагальнення, що представлене на рисунку 2 [11]. На рисунку представлені показники країн, які виступають типовими представниками отриманого рівня навичок.

Загальні висновки зі звітів Europol IOCTA 2023, 2025 та оприлюдненої інформації по розкритих шахрайських схемах у звітах [9, 120-142] та ENISA 2025 [13], дозволяють визначити рівень фінансових втрат деяких країн, що стає підґрунтям для формування індексу фінансового ризику населення країн Європи. Відповідне до мети аналізу, та враховуючи підвищений рівень кібератак на Україні впродовж повномасштабного вторгнення, данні по цифровим навичкам та розкритим шахрайським схемам також додані до моделі залежності.

Значення Індексу фінансового ризику напряму залежать від економічної доцільності атаки. Так для країн з високим ВВП (Німеччина, Франція, Італія) вартість викраденого доступу до банківського рахунку або корпоративної пошти у рази вище ніж в країнах низького рівня добробуту населення (Румунія, Болгарія). Навіть висока грамотність не рятує заможні країни від кібератак, оскільки злочинці готові інвестувати в AI-дипфейки та складне шпигунське ПЗ, щоб здобути «дорогу» жертву. Ризик високий там, де дані коштують дорого, а рівень цифрової кібергігієни та грамотності не є достатньо повним, щоб зробити атаку збитковою для хакера. Однак, країни, що досягли високого рівня цифрових навичок з кібергігієни та в цілому (Нідерланди, Данія, Естонія), мають значно нижчий ризик. Причина не в тому, що вартість інформації нижча, а в досвідченості населення та бізнесу з принципів організації масових атак та протидії їм. В таких країнах високий рівень базової кібербезпеки робить масові атаки (фішінг, вішінг, SMS-шахрайство) економічно нерентабельними для злочинців – витрати значні, прибуток їх не покриває. Україна протягом понад 4 років є об’єктом масованих кібератак та має значний досвід ознайомлення та навчання, наприклад на платформі Дія-освіта, бізнесу, освітян, населення протидії шахраям через щоденне зіткнення з реальними загрозами.

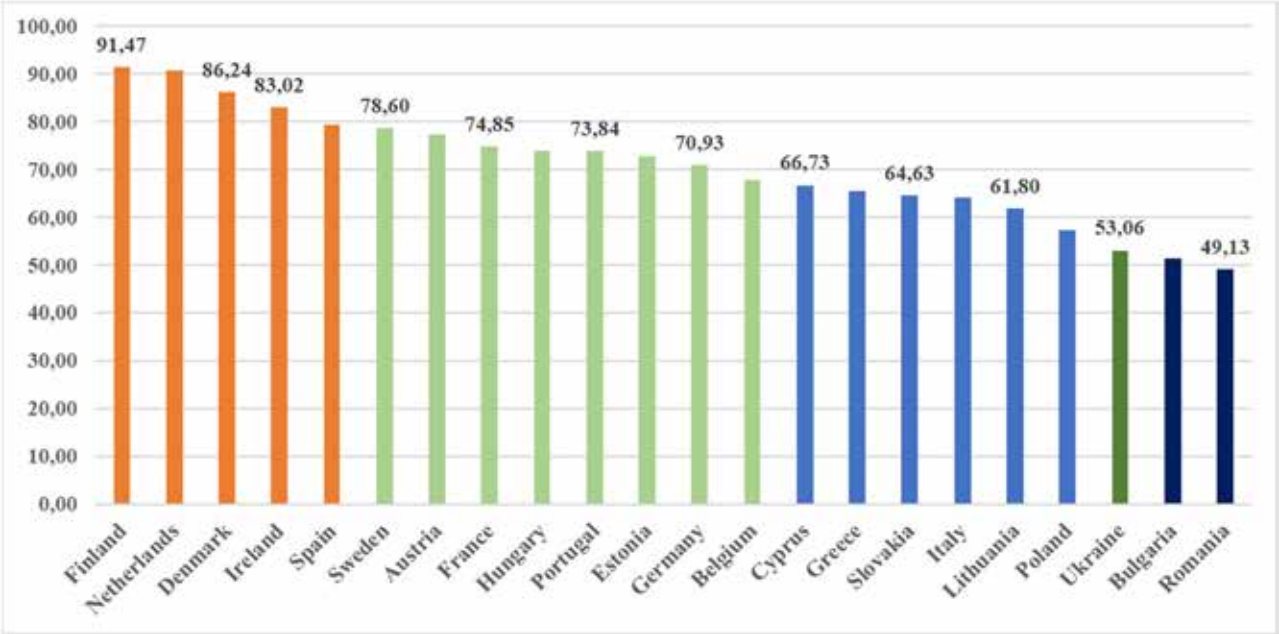

Рис. 2. Цифрові навички з безпеки в інтернеті

Джерело: сформовано на основі [11]

Тому середня вартість втрат даних нижча, а навички кібербезпеки досягають рівня німців.

Всі сформульовані передумови дозволили висунити гіпотезу моделі залежності індексу фінансового ризику від навичок цифрової безпеки та вартості витоку даних в наступному вигляді:

$$Y=\beta_0+\beta_1 G+\beta_2 V+\varepsilon$$

де:

Y – індекс фінансового ризику, характеризує вартість втрат від кібершахрайства;

G – рівень цифрових навичок з кібербезпеки та гігієни;

V – вартість підтверджених витоків даних;

β_0 – константа, яка враховує «білий шум»;

β_1 – параметр моделі, що оцінює вплив цифрових навичок на вартість втрати даних;

β_2 – параметр моделі, що показує привабливість зламу даних;

ε – константа моделі, що включає не враховані в моделі фактори.

Регресійний аналіз фактичних даних дозволів визначити наступні параметри моделі та показники якості:

$$Y=123,63-1,93G+16,52V$$

Коефіцієнт кореляції R^2 =0,90; скорегований R^2 = 0,87; критерій Фішера для моделі F = 32,03 при $F_{табл}$= 4,1, що підтверджує статистичну значущість та надійність моделі. Значення t-критерію для параметрів рівняння (10,03; -7,98; 5,02) значно більше табличного (2,28) значення, що підтверджує їх статистичну значущість.

По отриманих результатах розрахунків побудована діаграма розсіювання, яка представлена на рис. 3.

Інтерпретацію отриманих результатів можна розглянути використовуючи різні підходи. Звичайна інтерпретація отриманої моделі показує, що підвищення цифрових навичок кібербезпеки та кібергігієни на 1% знижує індекс фінансового ризику країни на 1,93 бали при тому самому рівні вартості інформації (добробуту, рівні втрат, вимог від шахраїв). Таким чином підтверджується ведуча роль освіти як захисного інструмента проти кіберзлочинів. При цьому, збільшення вартості даних, особистої інформації, комерційної таємниці на 1 пункт призведе до підвищення індексу на 16,52 бали при тому самому рівні цифрових навичок. Тобто, кібершахраї оцінюють в першу чергу цінність та повноту інформації та пов'язаних з нею інших даних. Збільшення вартості втрачених даних буде спонукати злочинців шукати або більш цікаві, дороговартісни об'єкти, або розробляти більш складні схеми шахрайства. Тому більш привабливими для них будуть довготривалі занурення у системи підприємств та організації за допомогою шпигунського ПЗ з метою зламу всієї системи, ніж фішингові листи на особисту пошту.

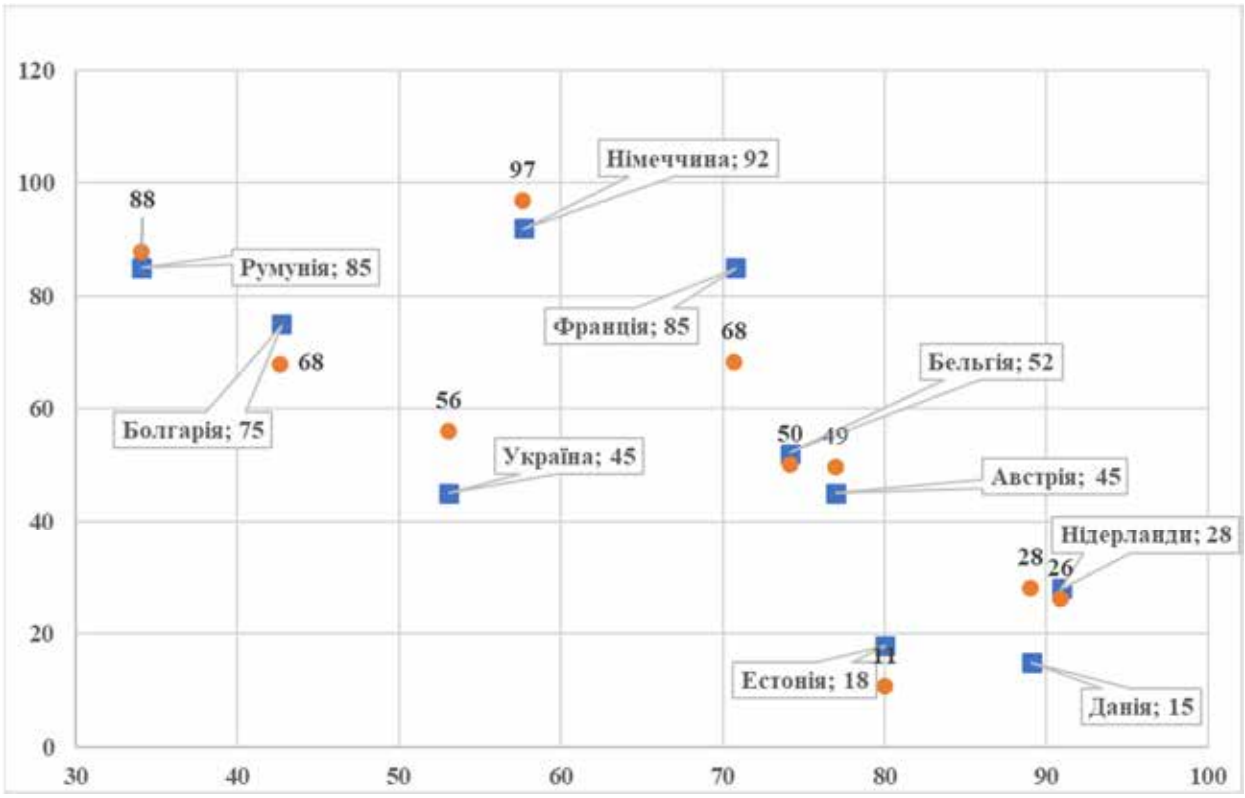

Рис. 3. Фактичні та змодельовані значення індексу фінансового ризику

Джерело: сформовано автором

З іншого боку можна чітко розділити отримані результати на три сегменти по рівнях навичок.

В країнах, які демонструють слабкі навички цифрової кібербезпеки (Румунія, Болгарія), втрати від кібершахрайства зростають майже пропорційне до рівня навичок. По наведеної у звітах інформації, найчастіше використовується різноманітна соціальна інженерія – «нігерійська» афера, злам месенджерів, пропозиція романтичних стосунків або цікавої роботи. Доволі часто, ті хто потрапив під такі дії, соромляться звертатися до поліції, якщо понесені втрати невеликі. Тому загальна інформація по таких випадках обмежена, з'являється тільки при опитуваннях у вигляді збільшення відсотків випадків. Для таких країн ознайомлення з методами соціальної інженерії, поширення прикладів та навчання протидії призведе до підвищення цифрових навичок. Згідно з моделлю, підвищення з 34% (Румунія) до 42% (Болгарія) знижує рівень втрат на декілька пунктів.

Друга зона графіку це країни зі стійкими навичками – Німеччина, Франція, Австрія, Швеція, Бельгія. Тут цифрові навички з кібербезпеки вже перейшли поріг масової вразливості від соціальної інженерії, але залишається критичним вплив таргетованих атак. Вартість особистої інформації достатньо висока, але досвідченість та ставлення до методів та способів протидії кібершахрайству використовується у відношенні до будь-якої інформації. На практиці це виражається у обережному відношенні до розголошення будь-чого. Тому німці, бельгійці та інші можуть говорити на різні теми окрім грошей.

В цьому секторі знаходиться й Україна. Цей момент є парадоксальним, тому що вартість життя значно нижча, але цифрові навички особливо з кібербезпеки, в Україні сформувалися під впливом поширення інформаційних проєктів від Дія-освіта, UGEN, EY та інших IT-проєктів, постійного обміну випадками та досвідом від постраждалих в соціальних мережах. Важливим є і вплив кібератак на державні та суспільні портали, які значно поширилися з 2022 року під час повномасштабного вторгнення. Українці швидко вчяться розпізнавати вішинг, смішинг та кетфішинг, слідкують за своїми банківськими рахунками, навчаються OSINT-технологіям. Рівень цифрових навичок з кібербезпеки та кібергігієни значно підвищується серед молоді та

груп працівників, які пов'язані з медициною та освітою в першу чергу за рахунок цифровізації в цих галузях, про що свідчить звіт Дослідження Цифрової та ШІ-грамотності в Україні [4].

Третя зона графіку, на якої знаходяться Нідерланди, Данія, Естонія, Фінляндія демонструє значний імунітет до методів соціальної інженерії та інших способів кібершахрайства. Рівень цифрових навичок в цих країнах >=80%, а по навичках кібербезпеки перевищує це значення. Будь які підозрілі сповіщення, або збої у роботі систем відстежуються автоматичне, а населення та працівники мають чіткі інструкції. Для цих країн головним є підтримка досягнутого рівня навичок, відпрацювання дій по нових загрозах.

Висновки. Проведений регресійний аналіз підтвердив гіпотезу, що рівень фінансових втрат у кіберпросторі залежить від двох основних факторів: рівня цифрової грамотності населення, особливо у галузі кібербезпеки, але стимулюється підвищенням ринкової вартості інформації, яка є основним об'єктом атаки. Моделювання підтвердило, що в умовах сучасної кіберзлочинності цифрові навички є необхідним, але недостатнім інструментом захисту для заможних економік. Для країн з високою вартістю даних навчання населення має доповнюватися складними технологічними засобами захисту, тоді як для країн у стані трансформації (Румунія, Болгарія, Україна), підвищення грамотності залишається найефективнішим методом боротьби з масовими втратами.

Уповільнене зростання навичок цифрової грамотності знижує ризики з меншою швидкістю ніж зростає вартість цифрових активів. Тому важливо працювати на випередження дії шахраїв, поширюючи інформацію про наявні приклади кібершахрайства, ознайомлювати населення з принципами кібергігієни та захисту особистої інформації. Такий підхід необхідне включити у стратегію цифрового розвитку держави, як підґрунтя до загальної економічної безпеки. Фінансова стійкість кожного громадянина сприяє підвищенню добробуту суспільства та напряму залежіть від цифрової грамотності та захищеності споживачів у цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Bognár L., Bottyán L. Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students. *Education Sciences*. Вип. 14, № 6. С. 588. DOI:10.3390/educsci14060588

2. Büchi M., Festic N., Just N. та ін. Digital inequalities in online privacy protection: effects of Age, education, and gender. ред. Eszter Hargittai. Edward Elgar Publishing, 2021. DOI:10.5167/UZH-210668

3. Гончаренко І. КІБЕРЗАГРОЗИ ФІНАНСОВОГО СЕКТОРА В УМОВАХ ВІЙНИ. *Економіка та суспільство*. Issue 50. DOI:10.32782/2524-0072/2023-50-82

4. Дослідження Цифрової та ШІ-грамотності в Україні. URL: https://osvita.diia.gov.ua/uploads/3/16241-doslidzenna_cifrovoi_ta_si_gramotnosti_v_ukraini_2025_pptx_pptx.pdf (дата звернення 15.03.2026).

5. Кокарча, Ю., Лалуєва, А. Особливості захисту персональних даних в соціальних мережах: вплив воєнного стану. *2022*. P. 70–74. URL: https://previous.scientia.report/index.php/archive/article/view/579

6. Кучеренко С. Як втратити мільярд: чому фінансові шахраї почуваються безкарно в Україні? 09.06.2025. URL: https://mind.ua/publications/20290333-yak-vtratiti-milyard-chomu-finansovi-shahrayi-pochuvayutsya-bezkarno-v-ukrayini

7. Маслій О., Буряк А., Науменко О. ДЕТЕРМІНАНТИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ІНДУСТРІЇ 4.0. *Scientific Journal of Yuriy Fedkovich Chernivtsi National University Economics*. Issue 3. P. 53–60. DOI:10.32782/ecovis/2025-3-8

8. Яровенко, Г. М., Койбічук, В. В., Боженко, В. В., & Пахненко, О. М. Програми підвищення фінансової грамотності споживачів фінансових послуг в країнах ЄС як напрям боротьби з кібершахрайствами. *Протидія кібершахрайству у фінансовому секторі: практика ЄС*. P. 143. URL: https://essuir.sumdu.edu.ua/server/api/core/bitstreams/dca3b00e-7897-4c85-a653-75788f85deb0/content

9. Bondarenko O. C., Dumchykov M. O. PROTECTION OF DIGITAL PERSONHOOD: STUDYING THE EXPERIENCE OF THE EUROPEAN UNION AND UKRAINE. *Juridical scientific and electronic journal*. Issue 1. P. 334–338. DOI:10.32782/2524-0374/2024-1/75

10. Cost of a cyber data breach averaged $4.35 mln. URL: https://beinsure.com/news/cost-cyber-data-breach/ (дата звернення 16.02.2026).

11. Database Eurostat. URL: https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21__custom_20793271/default/table (дата звернення 16.02.2026).

12. DigComp 3.0. URL: https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-digcomp/digcomp-30_en (дата звернення 20.02.2026).

13. ENISA Threat Landscape 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (дата звернення 25.02.2026).

14. Hyliaka O. S. Right to privacy and protection personal data in digitalization conditions. *JOURNAL OF THE NATIONAL ACADEMY OF LEGAL SCIENCES OF UKRAINE*. Vol. 30, Issue 1. P. 15–30. DOI: 10.31359/1993-0909-2023-30-1-15

15. Шульга О. А. Конфіденційність та шахрайство в інтернет-сфері *Економічний вісник університету*. Випуск 48. P. 76–91. DOI:https://doi.org/10.31470/2306-546X-2021-48

16. Skills for the digital age. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Skills_for_the_digital_age#Data_sources (дата звернення 06.03.2026).

17. Sophie C. Boerman, Sanne Kruikemeier, Frederik J. Zuiderveen Borgesius. Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. DOI:https://doi.org/10.1177/0093650218800915 (дата звернення 06.03.2026).

18. Steal, deal and repeat: How cybercriminals trade and exploit your data. URL: https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data (дата звернення 25.02.2026).

19. ЄГОРОВ Є. Україна 2026: як працюють сучасні кібератаки та як їх зупинити -. (26.03.2026). UGF, 2026. Duration: 1.46. (дата звернення 27.03.2026).

REFERENCES:

1. Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences, 14*(6), 588. https://doi.org/10.3390/educsci14060588

2. Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*. https://doi.org/10.1177/0093650218800915

3. Bondarenko, O. C., & Dumchykov, M. O. (2024). Protection of digital personhood: Studying the experience of the European Union and Ukraine. *Juridical Scientific and Electronic Journal, 1*, 334–338. https://doi.org/10.32782/2524-0374/2024-1/75. (in Ukrainian)

4. Büchi, M., Festic, N., & Just, N. (2021). Digital inequalities in online privacy protection: Effects of age, education, and gender. In E. Hargittai (Ed.), *Digital inequalities*. Edward Elgar Publishing. https://doi.org/10.5167/UZH-210668

5. Beinsure. (n.d.). *Cost of a cyber data breach averaged $4.35 mln*. https://beinsure.com/news/cost-cyber-data-breach/ (accessed February 16, 2026)

6. Diia Education. (2025). *Research on digital and AI literacy in Ukraine*. https://osvita.diia.gov.ua/uploads/3/16241-doslidzenna_cifrovoi_ta_si_gramotnosti_v_ukraini_2025_pptx_pptx.pdf (accessed March 15, 2026)

7. ENISA. (2025). *ENISA threat landscape 2025*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (accessed February 25, 2026)

8. European Commission, Joint Research Centre. (n.d.). *DigComp 3.0: The digital competence framework for citizens*. https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-digcomp/digcomp-30_en (accessed February 20, 2026)

9. Europol. (n.d.). *Steal, deal and repeat: How cybercriminals trade and exploit your data*. https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data (accessed February 25, 2026)

10. Eurostat. (n.d.). *Database Eurostat* [Data set]. European Commission. https://ec.europa.eu/eurostat/data-browser/view/isoc_sk_dskl_i21__custom_20793271/default/table (accessed February 25, 2026)

11. Eurostat. (n.d.). *Skills for the digital age*. European Commission. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Skills_for_the_digital_age#Data_sources (accessed March 06, 2026)

12. Goncharenko, I. (2023). Cyber threats of the financial sector in wartime conditions. *Economy and Society, 50*. https://doi.org/10.32782/2524-0072/2023-50-82. (in Ukrainian)

13. Hyliaka, O. S. (2023). Right to privacy and protection of personal data in digitalization conditions. *Journal of the National Academy of Legal Sciences of Ukraine, 30*(1), 15–30. https://doi.org/10.31359/1993-0909-2023-30-1-15. (in Ukrainian)

14. Kokarcha, Yu., & Laluyeva, A. (2022). Peculiarities of personal data protection in social networks: The impact of martial law (pp. 70–74). *Scientia*. https://previous.scientia.report/index.php/archive/article/view/579. (in Ukrainian)

15. Kucherenko, S. (2025, June 9). *How to lose a billion: Why financial fraudsters feel unpunished in Ukraine*. Mind.ua. https://mind.ua/publications/20290333-yak-vtratiti-milyard-chomu-finansovi-shahrayi-pochuvayutsya-bezkarno-v-ukrayini. (in Ukrainian)

16. Maslii, O., Buriak, A., & Naumenko, O. (2025). Determinants of state economic security under Industry 4.0 conditions. *Scientific Journal of Yuriy Fedkovich Chernivtsi National University Economics, 3*, 53–60. https://doi.org/10.32782/ecovis/2025-3-8. (in Ukrainian)

17. Shulga, O. (2021). Confidentiality and scam in the internet. *University Economic Bulletin, 48*, 76–91. https://doi.org/10.31470/2306-546X-2021-48. (in Ukrainian)

18. Yarovenko, H. M., Koibichuk, V. V., Bozhenko, V. V., & Pakhnenko, O. M. (n.d.). Financial literacy enhancement programmes for financial services consumers in EU countries as a means of combating cyber fraud. In *Countering cyber fraud in the financial sector: EU practice* (p. 143). Sumy State University. https://essuir.sumdu.edu.ua/server/api/core/bitstreams/dca3b00e-7897-4c85-a653-75788f85deb0/content. (in Ukrainian)

19. Yehorov, Ye. (2026, March 26). *Ukraine 2026: How modern cyberattacks work and how to stop them* [Video]. UGF. Duration: 1:46. (in Ukrainian)

Дата надходження статті: 17.04.2026
Дата прийняття статті: 08.05.2026
Дата публікації статті: 14.05.2026