



УДК 004:37

[https://doi.org/10.52058/2786-6165-2026-2\(44\)-1682-1694](https://doi.org/10.52058/2786-6165-2026-2(44)-1682-1694)

Гаркавий Сергій Федорович кандидат технічних наук, доцент кафедри військової підготовки ЧНУ ім.Б.Хмельницького м. Черкаси, <https://orcid.org/0009-0001-3443-4486>

Бардадим Олег Валерійович викладач кафедри освітнього, артменеджменту і соціальної роботи ЧНУ ім.Б.Хмельницького, <https://orcid.org/0000-0002-2777-6568>

ІНФОРМАЦІЙНА БЕЗПЕКА У СОЦІАЛЬНІЙ РОБОТІ ТА АРТМЕНЕДЖМЕНТІ: ТИПОЛОГІЯ ЗАГРОЗ, ЦИФРОВА КОМПЕТЕНТНІСТЬ, СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА ІНСТИТУЦІЙНІ СТРАТЕГІЇ ЗАХИСТУ

Анотація. У статті представлено розгорнутий аналіз сучасних викликів інформаційної безпеки у соціальній роботі та артменеджменті, що активно переходять до цифрових форматів діяльності й через це демонструють підвищену вразливість до кібератак. Фахівці цих сфер працюють із конфіденційними персональними даними, цифровими архівами, результатами творчої діяльності, фінансовими документами та транскордонними комунікаціями, що формує складну багаторівневу систему ризиків. У роботі представлено розширену типологію загроз, яка включає соціальну інженерію (фішинг, цільовий фішинг, претекстинг), шкідливе програмне забезпечення різних класів, мережеві та інфраструктурні атаки (DDoS, MITM, експлойти нульового дня), а також нові загрози, породжені штучним інтелектом, серед яких дипфейк-маніпуляції та автоматизовані схеми компрометації доступу. Для кожного типу визначено ключові індикатори, механізми реалізації та можливі наслідки, які можуть впливати на гуманітарні й культурні організації через витоки даних, фінансові втрати, порушення операційної діяльності й зниження довіри користувачів. У статті запропоновано цілісний комплекс правил цифрової гігієни, орієнтований на практичне застосування: використання менеджерів паролів, багатфакторної автентифікації, шифрування пристроїв, аудит доступу, контроль активності в хмарних сервісах, безпечна робота з публічними мережами, резервне копіювання та моніторинг аномалій. Розроблено чотирирівневу модель цифрової компетентності, яка охоплює базове усвідомлення загроз, операційні навички, аналітичні спроможності та інституційне лідерство в



питаннях кібербезпеки. Для кожного рівня подано типові навчальні завдання, адаптовані до професійних сценаріїв соціальних працівників і артменеджерів. Показано, що поєднання індивідуальної компетентності з організаційною політикою безпеки формує стійку модель кіберзахисту, необхідну для підтримання надійності, етичності та безперервності роботи соціальних і культурних інституцій.

Ключові слова: кібербезпека, соціальна робота, артменеджмент, цифрова компетентність, фішинг, програми–вимагачі, дипфейки, соціальна інженерія, захист персональних даних, інформаційна безпека.

Serhii Harkavyi, Candidate of Technical Sciences, Associate Professor, Department of Military Training, B. Khmelnytskyi National University, Cherkasy, <https://orcid.org/0009-0001-3443-4486>

Oleg Bardadym Lecturer, Department of Education, Art Management, and Social Work, B. Khmelnytskyi National University, <https://orcid.org/0000-0002-2777-6568>

INFORMATION SECURITY IN SOCIAL WORK AND ART MANAGEMENT: TYPOLOGY OF THREATS, DIGITAL COMPETENCE, SOCIAL ENGINEERING, AND INSTITUTIONAL PROTECTION STRATEGIES

Abstract. The article presents an extended analysis of current information security challenges in social work and art management, two sectors undergoing rapid digital transformation and therefore exhibiting heightened vulnerability to cyberattacks. Professionals in these fields operate with sensitive personal data, digital archives, intellectual property, financial documentation, and cross-border communication, creating a complex and multilayered risk environment. The study proposes an expanded typology of cyberthreats encompassing social engineering (phishing, spear-phishing, pretexting), various categories of malicious software, network and infrastructural attacks (DDoS, MITM, zero-day exploits), as well as emerging threats driven by artificial intelligence, such as deepfake manipulation and automated credential-compromise schemes. For each threat type, the article identifies key indicators, operational mechanisms, and potential consequences, which may include data breaches, financial losses, workflow disruptions, and erosion of institutional trust within humanitarian and cultural organizations.

The study offers a comprehensive set of cyber hygiene practices tailored to practical implementation: the use of password managers, multi-factor authentication, device encryption, access auditing, monitoring activity in cloud



environments, safe interaction with public networks, systematic data backup, and anomaly detection. A four-level model of digital competence is introduced, covering basic threat awareness, operational skills, analytical capabilities, and institutional leadership in cybersecurity governance. Each level includes practical training tasks adapted to the professional contexts of social workers and art managers. The findings demonstrate that the integration of individual digital competence with organizational security policies enables the creation of a resilient, multi-layered cybersecurity system essential for maintaining reliability, ethical standards, and continuity of services across social and cultural institutions.

Keywords: cybersecurity, social work, art management, digital competence, phishing, ransomware, deepfakes, social engineering, personal data protection, information security.

Постановка проблеми. Кібербезпека стала фундаментальною передумовою професійної діяльності у всіх наукоємних секторах. У соціальній роботі фахівці оперують надзвичайно чутливими персональними даними, включаючи інформацію про вразливі групи населення, стан здоров'я, економічні умови, міграційну історію та психологічні профілі. В артменеджменті професіонали працюють з цифровими архівами, авторськими правами, міжнародними грантовими контрактами, мистецькими портфоліо та фінансовими транзакціями.

Цілісність та конфіденційність інформації є не лише технічним питанням, а етичною вимогою, яка впливає на права людини, довіру. Численні звіти підтверджують, що гуманітарні, освітні та культурні організації стали пріоритетними мішенями для атак через низький рівень захисних заходів та залежність від електронної комунікації. Ключова суперечність полягає в зростаючій цифровізації соціальних та культурних послуг на тлі недостатньої цифрової та інформаційної безпекової компетентності серед професіоналів. Соціальні працівники активно використовують хмарні сервіси, месенджери та цифрові системи управління справами, тоді як арт-менеджери покладаються на транскордонну комунікацію, платформи цифрового маркетингу, онлайн-фінансові системи та репозиторії для творчих робіт.

Аналіз останніх досліджень і публікацій. Попри критичність безпечної цифрової поведінки, жоден із секторів повністю не інтегрував кібербезпеку у свої професійні стандарти. Як зазначається в українських рамках цифрової компетентності, інформаційна та цифрова грамотність є необхідними для сучасних фахівців, зокрема викладачів природничих наук, де цифрові технології трансформують роль педагога, стимулюючи інтерес та залученість студентів [1]. Аналогічно наголошується на важливості



класифікації веб-ресурсів, верифікації інформації та розуміння інформаційних систем, що безпосередньо корелює зі стійкістю до кіберзагроз [2; 3; 4; 5].

Проблема посилюється глобальними факторами: гібридною війною, масовою дезінформацією, стрімким розвитком штучного інтелекту та зростаючою складністю стратегій кіберзлочинців. Сучасні дослідження кібербезпеки для нетехнічних професій виокремлюють кілька ключових напрямків: моніторинг кіберзагроз [6; 7], еволюція програм-вимагачів [8], аналітика витоків даних [9], освітні рамки цифрової компетентності [10; 15], загрози, генеровані штучним інтелектом, включно з імпровізацією дипфейків [11], та класифікації веб-вразливостей [12]. Українські дослідники підкреслюють діяльнісну складову формування цифрової компетентності, включаючи здатність управляти, оцінювати та створювати цифровий контент відповідально [1]. Цей підхід поширюється на оцінювання надійності інформаційних ресурсів, класифікацію освітніх платформ та дослідження інформаційних систем для інституційного управління - знання, безпосередньо застосовне до цифрової безпеки [2; 3; 4]. Водночас, небагато досліджень безпосередньо адресують виклики кібербезпеки, специфічні для соціальної роботи та арт-менеджменту, що робить актуальним інтегрування загального знання з галузево-специфічними ризиками. Цифрова компетентність визначається як сукупність знань, навичок та ставлень, що забезпечують ефективно та безпечно використання цифрових технологій [15]. Інформаційна та цифрова компетентність включає здатність отримувати доступ до інформації та управляти нею, оцінювати достовірність, інтегрувати та створювати цифрові ресурси, застосовувати цифрові інструменти для розв'язання практичних проблем, комунікувати безпечно та етично [1].

Ці принципи узгоджуються з потребами цифрової компетентності соціальних працівників та арт-менеджерів. Українська рамка наголошує на конкурентоспроможності на ринку праці, здатності оперувати сучасними технологіями та безпечній онлайн-поведінці [10]. Роль цифрової компетентності змінюється від простого технічного користування до відповідального цифрового громадянства. На основі аналізу міжнародної аналітики виокремлюються шість основних категорій загроз: фішинг та цільовий фішинг, компрометація корпоративної електронної пошти, програми-вимагачі, маніпуляції дипфейками та загрози на базі штучного інтелекту, витoki даних та скомпрометоване хмарне сховище, вразливості вебсайтів та цифрових платформ. Кожна загроза має специфічні індикатори ризику та спричинила задокументовані інциденти в гуманітарних та культурних інституціях.



Мета статті. Розробити узагальнену концептуальну рамку кібербезпеки для фахівців соціальної роботи та арт-менеджменту шляхом інтеграції сучасних міжнародних стандартів, типологій кіберзагроз і моделей цифрової компетентності, адаптованих до специфіки цих професій. Для досягнення мети визначено такі завдання: систематизувати ключові категорії кіберзагроз, релевантні для соціальної роботи та артменеджменту; розробити практичний інструментарій ідентифікації кіберризиків через таблиці індикаторів загроз; структурувати правила цифрової гігієни у вигляді узагальнених таблиць із прикладами застосування; створити чотирирівневу модель розвитку цифрової компетентності з кібербезпеки; визначити інституційні механізми захисту та протоколи реагування на кіберінциденти; запропонувати практичні навчальні завдання та симуляційні вправи з формування компетентностей кібербезпеки.

Виклад основного матеріалу. Розглянемо типи інформаційних небезпек **1. Соціальна інженерія** є сукупністю методів психологічного маніпулювання, що використовуються зловмисниками для отримання доступу до даних та систем. **Фішинг** - масова розсилка шахрайських електронних листів, які намагаються виманити облікові дані або фінансову інформацію. Основними ознаками фішингу є несподівані повідомлення нібито від офіційних установ, загальні звернення («Шановний користувач»), вимога термінових дій, помилки у доменах, граматичні помилки та підозрілі вкладення.

Наслідками фішингових атак стають компрометація облікових записів, втрата доступу до організаційних систем, фінансові збитки й розкриття конфіденційних даних. **Цільовий фішинг** (spear phishing) - персоналізована атака, що імітує комунікацію конкретних осіб (керівників, донорів, партнерів), використовуючи реальні контексти та схожі домени. Його ознаками є високий ступінь персоналізації повідомлень, посилання на реальні події, майже ідентичні доменні імена та термінові запити на переказ коштів чи передачу інформації.

Наслідки включають втрату значних фінансових ресурсів, витік стратегічної інформації, компрометацію партнерських відносин і репутаційні ризики.

Претекстинг - маніпулятивна техніка створення вигаданого сценарію (наприклад, «техпідтримка», «аудит»), що спонукає жертву розкрити конфіденційні дані. Його ознаками є несподівані дзвінки, запити на паролі для «верифікації», вимоги надати доступ до внутрішніх документів та створення штучного відчуття кризи. Наслідками стають повний несанкціонований доступ до систем, маніпуляції базами даних, крадіжка інтелектуальної власності та підірив довіри між співробітниками.



2. Шкідливе програмне забезпечення становить другу групу ризиків. Трояни, черв'яки, шпигунське ПЗ та кейлоггери - це програми, що маскуються під легітимні застосунки, поширюються через мережі, відстежують активність та фіксують натискання клавіш. Їх ознаками є уповільнення роботи пристрою, збільшення трафіку, спливаючі вікна, зміна налаштувань браузера, вимкнення антивірусу, поява невідомих програм та зникнення файлів. Наслідки включають витік персональних і фінансових даних, викрадення інтелектуальної власності, втрату контролю над обліковими записами та довготривале перебування зловмисників у системі. **Криптоджекінг** - приховане використання обчислювальних ресурсів користувача для майнінгу криптовалюти. Його ознаками є надмірне навантаження процесора, перегрів пристрою, швидке розрядження батареї та зниження продуктивності. Наслідками виступають неможливість виконання ресурсомістких завдань, прискорене зношення обладнання та виявлення глибших системних вразливостей. Атаки на паролі - це брутфорс, словникові атаки та використання викрадених паролів для отримання доступу до систем. Їх ознаки включають численні невдалі спроби входу, блокування акаунтів, входи з незвичних локацій та неініційовані запити на скидання пароля. **Наслідки** - несанкціонований доступ до критичних систем, компрометація фінансових операцій, витік конфіденційної інформації та модифікація або видалення даних.

3. Мережеві, інфраструктурні та апаратні атаки становлять окремий вектор загроз. DDoS-атаки - перевантаження вебресурсів надмірною кількістю запитів з метою зробити їх недоступними. Ознаки включають повільне завантаження сторінок, помилки таймауту, раптову недоступність та аномальний трафік. Наслідками є зупинка онлайн-сервісів, фінансові й репутаційні втрати та потреба у додаткових витратах на кіберзахист. Атаки «людина посередині» (MITM) - перехоплення трафіку через підроблені Wi-Fi точки. Ознаки: попередження про сертифікати, незвичне перепідключення до мережі, входи з нових пристроїв та підозрілі точки доступу. Наслідки - перехоплення паролів, витік конфіденційної комунікації, доступ до сесійних токенів і компрометація транзакцій. **SQL-ін'єкції** - маніпулювання запитами до баз даних для доступу або зміни інформації. Ознаки: помилки бази, необґрунтований доступ до адмінпанелі, несанкціоновані зміни даних, підозрілі записи в логах. Наслідки: масові витоки персональних і фінансових даних, модифікація записів та створення фіктивних адмін-акаунтів. **Експлойти нульового дня** - використання невідомих розробникам вразливостей. Їх ознаками є обходи захисних механізмів, компрометація без видимої точки входу та відсутність реакції антивірусу. Наслідки включають повну компрометацію системи, масштабне



поширення атаки та необхідність екстрених оновлень. Апаратні імплантати - шкідливі пристрої, що маскуються під звичайні аксесуари. Ознаки: знайдені підозрілі USB, «подарункові» флешки, автоматичне виконання команд після підключення. Наслідки: миттєве викрадення файлів, встановлення бекдорів, компрометація мережі та обходи програмного захисту.

4.Окрему категорію становлять загрози, згенеровані штучним інтелектом. Дипфейк аудіо та відео – підроблені мультимедійні матеріали, що імітують голос чи зовнішність керівників для отримання доступу до ресурсів або примушення до термінових дій. Ознаками є неприродні рухи губ, нехарактерні інтонації, невідповідні фонові шуми, дивні тіні та низька якість відео. **Наслідки:** фінансові втрати, хибні управлінські рішення, репутаційні скандали, підрив довіри в команді, юридичні наслідки та психологічний стрес співробітників [11; 18]. На основі вище згаданих кібератак слід сформулювати правила користування Інтернет мережею

1. Сильні унікальні паролі (8+ символів, змішані символи) слід використовувати через менеджери паролів (Bitwarden, 1Password, KeePass), наприклад, для системи обліку клієнтів / для адмінпанелі сайту галереї. Недотримання цього правила сприяє легкому злому акаунтів і витоку конфіденційних даних. Ніколи не варто використовувати один і той самий пароль для різних сервісів, адже унікальні паролі для електронної пошти, CRM та хмарного сховища / для сайту галереї, онлайн-банкінгу, соцмереж запобігають загрозі, коли злом одного облікового запису ставить під загрозу всі сервіси.

2. Увімкнення багатфакторної автентифікації (MFA) із застосуванням Google Authenticator, Microsoft Authenticator або Authy дозволяє забезпечити додатковий рівень безпеки при доступі до бази даних клієнтів / до системи управління грантами та адміністрування сайту. Несанкціонований доступ до систем навіть при знанні пароля стає неможливим. Регулярне оновлення програмного забезпечення через автоматичне оновлення ОС, антивірусу та додатків забезпечує безпеку CRM-системи / системи бронювання квитків і вебсайту галереї, запобігаючи використанню відомих вразливостей зловмисниками та атакам ransomware.

3. Використання антивірусного та антишпигунського програмного забезпечення з регулярним скануванням захищає ПК соціальних працівників / ПК та сервери галереї від вірусів, троянів та шпигунських програм, які можуть вкрасти дані або пошкодити систему. Обережне використання електронної пошти та посилань, включаючи перевірку відправника та застосування фільтрів спаму, допомагає уникати відкриття підозрілих листів / переходів за сумнівними посиланнями, що зменшує ризик фішингу та зараження шкідливим ПЗ.



4. Безпечне використання хмарних сервісів із шифруванням файлів, обмеженням доступу та резервним копіюванням дозволяє захистити персональні дані клієнтів / зберігати фото та матеріали виставок, зменшуючи ймовірність витоку даних або доступу сторонніх. Обмеження доступу та прав користувачів через надання доступу лише за необхідністю та аудит прав забезпечує контроль доступу соціальних працівників лише до своїх клієнтів / працівників галереї до своїх систем, запобігаючи несанкціонованому доступу та внутрішнім загрозам.

5. Навчання та підвищення кіберобізнаності через регулярні тренінги та симуляції фішингових атак підвищує безпеку персоналу соціальних працівників / співробітників галереї, зменшуючи ризики, пов'язані з людським фактором. Безпечне використання публічних мереж із застосуванням VPN та униканням доступу до критичних систем у відкритих Wi-Fi забезпечує захист при підключенні до CRM / вебсайту галереї від перехоплення трафіку та крадіжки логінів і паролів.

6. Регулярне резервне копіювання даних за допомогою автоматичного створення бекапів захищає інформацію клієнтів / копії медіафайлів виставок від втрат через збій, атаки ransomware або випадкове видалення. Шифрування пристроїв та даних (BitLocker, FileVault, шифрування мобільних пристроїв) забезпечує захист ноутбуків соціальних працівників / планшетів та ПК галереї, зменшуючи ризик витоку даних у разі викрадення або втрати пристрою.

7. Контроль соціальних мереж через налаштування приватності, обмеження публікацій та двофакторну автентифікацію дозволяє закривати соціальні профілі / контролювати публікації галереї, мінімізуючи публікацію конфіденційної інформації та репутаційні втрати. Безпечне використання USB та зовнішніх носіїв через сканування перед підключенням та шифрування захищає документи / медіафайли виставок від шкідливого ПЗ та витоку даних.

8. Моніторинг підозрілої активності за допомогою систем моніторингу та сповіщення про аномалії дозволяє контролювати доступ до бази клієнтів / адмінпанелі сайту галереї, зменшуючи ризик непомічених несанкціонованих дій. Захист мобільних додатків із застосуванням антивірусу на смартфоні та блокування сторонніх додатків забезпечує безпечне використання офіційних мобільних CRM-додатків / управління продажами та квитками галереї, запобігаючи зараженню мобільних пристроїв, крадіжці даних та втручанню в роботу систем.

Розвиток цифрової компетентності для фахівців соціальної роботи та артменеджменту здійснюється через чотири послідовні рівні, що дозволяє поступово нарощувати навички від базового усвідомлення до інститу-



ційного лідерства, аналогічно до рамки компетентностей для громадянина, яка пропонує систему рівнів освоєння: від базового ознайомлення до повної самостійності та стратегічного впливу.

На рівні базового усвідомлення фокус спрямований на розпізнавання фішингу, увімкнення багатофакторної автентифікації та використання менеджера паролів, а також розуміння базових загроз. У соціальній роботі це реалізується через аналіз фішингових листів, виявлення ключових індикаторів (невідповідність домену, граматичні помилки, терміновість, підозрілі вкладення), створення складних паролів для систем обліку клієнтів та увімкнення MFA для робочої пошти. В артменеджменті практичні завдання включають налаштування менеджера паролів для облікових записів галереї, увімкнення двофакторної автентифікації для email та фінансових систем, перевірку налаштувань приватності хмарних сховищ та аналіз потенційно фішингових листів із пропозиціями грантів. Додаткове завдання: створити тестовий фішинговий лист і оцінити його як справжній або шахрайський; очікуваний результат: правильна ідентифікація всіх ознак фішингу.

На рівні операційної компетентності учасники опановують аудит хмарного сховища, оцінку достовірності ресурсів, ідентифікацію вразливостей та застосування принципів кібергігієни. Соціальні працівники виконують симуляції підозрілих входів у системи, відключають мережу, змінюють паролі, повідомляють IT-відділ та керівника, здійснюють самоаудит облікових записів і перевірку встановленого програмного забезпечення. В артменеджменті операційні завдання охоплюють аудит публічних посилань на хмарні сховища, обмеження доступу для колишніх співробітників, перевірку шифрування фінансових документів та налаштування безпеки соціальних мереж. Додаткове завдання: провести аудит власного Google Drive і видалити непотрібні публічні посилання; очікуваний результат: усі документи доступні лише для авторизованих користувачів.

Рівень аналітичної компетентності включає розробку моделей загроз, аналіз артефактів дипфейків, реагування на складні інциденти та оцінку ризиків проєктів. Соціальні працівники створюють карту загроз робочого дня, визначають ймовірність і наслідки ризиків на різних етапах взаємодії з клієнтами, аналізують витoki даних та розслідують компрометації. В артменеджменті практичні завдання передбачають детекцію дипфейків у відео та аудіо, розробку протоколів верифікації запитів на фінансові операції та оцінку ризиків міжнародних виставок із формуванням матриці ризиків і пріоритизацією загроз. Додаткове завдання: провести аналіз короткого відео на наявність ознак дипфейку; очікуваний



результат: точне визначення підроблених елементів та запропоновані заходи для верифікації[19; 20]..

На рівні інституційного лідерства учасники опановують написання внутрішніх регуляцій, навчання колег, впровадження GDPR-політик, управління інцидентами та стратегічне планування безпеки. Соціальні працівники розробляють політику кібербезпеки для організацій, що працюють із вразливими групами, створюють річні програми навчання персоналу та симуляції фішингу. В артменеджменті завдання включають навчання всіх ролей у культурному центрі та створення протоколів інцидент-менеджменту для сценаріїв компрометації сайтів, витоку контрактів або атак програм-вимагачів із призначенням ролей, ланцюгами комунікації, юридичними процедурами та PR-стратегіями. Додаткове завдання: розробити короткий внутрішній регламент реагування на кіберінциденти; очікуваний результат: документ, який чітко визначає дії персоналу при критичних інцидентах і забезпечує швидке реагування [16].

Додаткові активності включають використання детекторів дипфейків, симулятори фішингу та самоаудит цифрової гігієни, що охоплюють перевірку паролів, аналіз пристроїв, сканування хмарних сховищ і оцінку загального рівня цифрової безпеки. Карта загроз для соціальної справи або мистецького проєкту дозволяє системно візуалізувати потенційні кіберризики на різних етапах роботи, від первинного контакту з клієнтом чи партнером до архівування матеріалів після завершення проєкту, сприяючи інтеграції безпечних практик у повсякденні робочі процеси[17; 20].

Висновки. Інформаційна безпека у соціальній роботі та артменеджменті є не просто технічною функцією, а основною етичною відповідальністю професіоналів цих галузей. Інтеграція рамок цифрової компетентності, типологій загроз та практичних вправ дозволяє інституціям значно знизити вразливість перед кіберзагрозами. Багаторівнева модель компетентності підтримує професійний розвиток фахівців, тоді як організаційні політики забезпечують системний захист. Розширена типологія кібератак, адаптована до специфіки обох секторів, демонструє різноманітність та складність сучасних загроз, від соціальної інженерії до атак на бази штучного інтелекту.

Систематизація індикаторів кіберризиків у табличному форматі з конкретними прикладами для соціальної роботи та арт-менеджменту забезпечує практичний інструментарій для швидкої ідентифікації потенційних загроз у повсякденній діяльності. Правила кібергігієни, представлені у структурованому вигляді з технічною реалізацією та галузевими прикладами, дозволяють фахівцям негайно впроваджувати захисні практики без потреби у глибоких технічних знаннях.



Чотирирівнева модель розвитку цифрової компетентності з конкретними практичними завданнями для кожного рівня створює чіткий освітній трек від базового усвідомлення до інституційного лідерства, дозволяючи організаціям планувати довгострокові програми навчання персоналу. Інтеграція інституційних механізмів захисту з індивідуальним розвитком компетентностей забезпечує багаторівневий підхід до кібербезпеки, де технічні рішення підтримуються людським фактором та організаційною культурою.

Майбутні дослідження мають зосередитися на ризиках, пов'язаних із штучним інтелектом, порівняльних міжнародних практиках кібербезпеки в гуманітарному та культурному секторах, а також психологічних факторах, що впливають на дотримання правил кібербезпеки серед фахівців допоміжних професій. Особливу увагу варто приділити вивченню бар'єрів впровадження захисних механізмів у ресурсообмежених організаціях та розробці економічно доступних рішень для малих неурядових організацій та культурних ініціатив. Перспективним напрямком є також дослідження ефективності різних форматів навчання кібербезпеки для нетехнічних професіоналів та розробка галузево-специфічних сертифікаційних програм

Література

1. Шпак, В., & Бардадим, О. (2022). Формування інформаційно-цифрової компетентності викладачів природничих наук: діяльнісна складова. *Вища освіта України*, 1(90), 153–170. <https://doi.org/10.38014/osvita.2022.90.14>
2. Бардадим, О. В. (2022). Класифікація освітніх веб-ресурсів. *Наукові записки. Серія: Педагогічні науки*, 207, 89–99. <https://doi.org/10.36550/2415-7988-2022-1-207-89-99>
3. Бардадим, О. (2024). Сервіси для перевірки фактів. *Zenodo*. <https://doi.org/10.5281/zenodo.14832217>
4. Бардадим, О. (2025). Види інформаційних систем управління закладом освіти. *Матеріали IV Міжнародної конференції «Цифрові інновації та соціальні трансформації в освіті»*. *Zenodo*. <https://doi.org/10.5281/zenodo.14840251>
5. Бардадим, О. (2025). Статистика соціальних явищ. *Zenodo*. <https://doi.org/10.5281/zenodo.14837856>
6. CERT-UA. (2023). Звіти про кіберзагрози. <https://cert.gov.ua>
7. ENISA. (2023). *Threat Landscape Report 2023*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2023>
8. Sophos. (2023). *State of Ransomware Report*. <https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2023-wp.pdf>
9. Verizon. (2023). *Data Breach Investigations Report*. <https://www.verizon.com/business/resources/reports/dbir/>
10. Міністерство освіти і науки України. (2021). *Рамка цифрової компетентності для України*. <https://mon.gov.ua/ua/npa/ramka-cifrovoi-kompetentnosti>
11. Europol. (2024). *Facing Reality? Law Enforcement and Deepfakes*. <https://www.europol.europa.eu/publications-documents/facing-reality-law-enforcement-and-deepfakes>



12. OWASP Foundation. (2023). OWASP Top 10 Vulnerabilities. <https://owasp.org/Top10/>
13. NIST. (2020). Cybersecurity Framework. National Institute of Standards and Technology. <https://www.nist.gov/cyberframework>
14. European Commission. (2021). General Data Protection Regulation (GDPR). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
15. European Commission. (2021). DigComp 2.2: The European Digital Competence Framework. https://joint-research-centre.ec.europa.eu/digcomp/digcomp-2-2-2021_en
16. Microsoft Security. (2023). Phishing Trends Analysis. <https://www.microsoft.com/security/blog/phishing-trends-2023>
17. IBM Security. (2023). Cost of a Data Breach Report. <https://www.ibm.com/reports/data-breach-2023>
18. Google Security. (2023). Safe Browsing Transparency Report. <https://safebrowsing.google.com/transparency-report/>
19. Cisco. (2022). Cybersecurity Threat Trends. <https://www.cisco.com/c/en/us/products/security/security-reports.html>
20. McAfee Labs. (2023). Cyberthreat Report. <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2023.pdf>

Reference

1. Shpak, V., & Bardadym, O. (2022). Formuvannia informatsiyno-tsyfrovoyi kompetentnosti vykhovateliv pryrodnychkh nauk: diialnisna skladova [Formation of information-digital competence of natural science teachers: activity component]. Kyiv: Vyscha osvita Ukrainy [in Ukrainian]. <https://doi.org/10.38014/osvita.2022.90.14>
2. Bardadym, O. V. (2022). Klasyfikatsiia osvitnikh web-resursiv [Classification of educational web resources]. Kyiv: Naukovi zapysky. Seriya: Pedahohichni nauky [in Ukrainian]. <https://doi.org/10.36550/2415-7988-2022-1-207-89-99>
3. Bardadym, O. (2024). Servisy dlia perevirky faktiv [Fact-checking services]. Zenodo [in Ukrainian]. <https://doi.org/10.5281/zenodo.14832217>
4. Bardadym, O. (2025). Vydy informatsiynykh system upravlinnia zakladom osvity [Types of information management systems in educational institutions]. Materyaly IV Mizhnarodnoi konferentsii "Tsifrovi innovatsii ta sotsialni transformatsii v osviti" [in Ukrainian]. <https://doi.org/10.5281/zenodo.14840251>
5. Bardadym, O. (2025). Statystyka sotsialnykh iavysch [Statistics of social phenomena]. Zenodo [in Ukrainian]. <https://doi.org/10.5281/zenodo.14837856>
6. CERT-UA. (2023). Zvity pro kiberzahrozy [Reports on cyber threats]. Kyiv [in Ukrainian]. <https://cert.gov.ua>
7. ENISA. (2023). Threat Landscape Report 2023. European Union Agency for Cybersecurity [in English]. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2023>
8. Sophos. (2023). State of Ransomware Report [in English]. <https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2023-wp.pdf>
9. Verizon. (2023). Data Breach Investigations Report [in English]. <https://www.verizon.com/business/resources/reports/dbir/>
10. Ministerstvo osvity i nauky Ukrainy. (2021). Ramka tsyfrovoyi kompetentnosti dlia Ukrainy [Digital competence framework for Ukraine]. Kyiv [in Ukrainian]. <https://mon.gov.ua/ua/npa/ramka-cifrovoi-kompetentnosti>



11. Europol. (2024). Facing Reality? Law Enforcement and Deepfakes [in English]. <https://www.europol.europa.eu/publications-documents/facing-reality-law-enforcement-and-deepfakes>
12. OWASP Foundation. (2023). OWASP Top 10 Vulnerabilities [in English]. <https://owasp.org/Top10/>
13. NIST. (2020). Cybersecurity Framework. National Institute of Standards and Technology [in English]. <https://www.nist.gov/cyberframework>
14. European Commission. (2021). General Data Protection Regulation (GDPR) [in English]. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
15. European Commission. (2021). DigComp 2.2: The European Digital Competence Framework [in English]. https://joint-research-centre.ec.europa.eu/digcomp/digcomp-2-2-2021_en
16. Microsoft Security. (2023). Phishing Trends Analysis [in English]. <https://www.microsoft.com/security/blog/phishing-trends-2023>
17. IBM Security. (2023). Cost of a Data Breach Report [in English]. <https://www.ibm.com/reports/data-breach-2023>
18. Google Security. (2023). Safe Browsing Transparency Report [in English]. <https://safebrowsing.google.com/transparency-report/>
19. Cisco. (2022). Cybersecurity Threat Trends [in English]. <https://www.cisco.com/c/en/us/products/security/security-reports.html>
20. McAfee Labs. (2023). Cyberthreat Report [in English]. <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2023.pdf>

Дата першого надходження статті до видання: 14.02.2026

Дата прийняття статті до друку після рецензування: 28.02.2026



Наукові перспективи
Видавнича група



Bulletin of Science and Education

ВІСНИК науки та
освіти
ISSN 2786-6165 (ONLINE)



№ 2(44) 2026

Видавнича група «Наукові перспективи»
Християнська академія педагогічних наук України

«Вісник науки та освіти»

№ 1(43) 2026

Київ – 2026

Publishing Group «Scientific Perspectives»
Christian Academy of Pedagogical Sciences of Ukraine

"Bulletin of Science and Education"

№ 1(43) 2026

Kyiv – 2026

ISSN 2786-6165 Online

УДК 001.32:1 /3(477)(02)

Ідентифікатор медіа R40-05847

DOI: [https://doi.org/10.52058/2786-6165-2026-2\(44\)](https://doi.org/10.52058/2786-6165-2026-2(44))

«Вісник науки та освіти»: журнал. 2026. № 2(44) 2026. С. 3860

Рекомендовано до видавництва Всеукраїнською Асамблеєю докторів наук з державного управління
(Рішення від 02.03.2026, № 1/3-26)



Згідно наказу Міністерства освіти і науки України 10.10.2022 № 894 журналу присвоєні категорії "Б" із історії та археології (спеціальність - 032 Історія та археологія) та педагогіки (спеціальність - 011 Освітні, педагогічні науки)

Згідно наказу Міністерства освіти і науки України від 23.12.2022 № 1166 журналу присвоєна категорія Б з філології (спеціальність - 035 філологія)

Журнал видається за підтримки Інституту філософії та соціології Національної академії наук Азербайджану, Всеукраїнської асоціації педагогів і психологів з духовно-морального виховання та Всеукраїнської асамблеї докторів наук з державного управління

Журнал публікує наукові розвідки з теоретичних та прикладних аспектів гуманітарних наук та мистецтва

Цільова аудиторія: вчені, лінгвісти, літературознавці, перекладачі, мистецтвознавці, культурознавці, педагоги, соціологи, історики, археологи, а, також, інші фахівці з різних сфер життєдіяльності суспільства, де знаходить застосування тематика наукового журналу



Журнал включено до міжнародної наукометричної бази Index Copernicus (IC), Research Bible, міжнародної пошукової системи Google Scholar



Головний редактор: Котельницький Назар Анатолійович – член-кореспондент Української Академії Наук, кандидат історичних наук, доцент кафедри мовної підготовки та міжкультурних комунікацій, ЗВО Університет трансформації майбутнього (м. Чернігів, Україна)

Редакційна колегія:

- ✓ **Азарова Лариса Євстахіївна** - докт.філол.наук, професор, завідувач кафедри мовознавства Вінницького національного технічного університету (Україна)
- ✓ **Берест Ігор Романович** - доктор історичних наук, професор кафедри медійних технологій, інформаційної та книжкової справи, Національного університету «Львівська політехніка» (Україна)
- ✓ **Беррі, Стівен** доктор історичних наук, професор, професор епохи Громадянської війни Коледжу мистецтв і наук Франкліна Університету Джорджії (США)
- ✓ **Вуколова Катерина Володимирівна** – кандидат філологічних наук, доцент кафедри романо-германської філології та перекладу Білоцерківського національного аграрного університету (Біла Церква, Україна), доцент Дніпровського відділення центру наукових досліджень та викладання іноземних мов Національної академії наук України, Дніпро, Україна (Україна)
- ✓ **Гурко Олена Василівна** - доктор філологічних наук, професор, завідувач кафедри англійської мови для нефілологічних спеціальностей Дніпровського національного університету імені Олеся Гончара, (Дніпро, Україна)
- ✓ **Заур Алієв** доктор філософії з історії науки, доктор філософії з політичних наук, доцент, доцент Інституту філософії та соціології НАНА, Азербайджан (Азербайджан)
- ✓ **Оскар Чамоса** кандидат історичних наук, доцент, доцент кафедри історії Коледжу мистецтв і наук Франкліна Університету Джорджії, (США)

- √ **Островський Олександр Олександрович**, доктор філософії, доцент, доцент кафедри філології, Закарпатський угорський університет ім. Ф.Ракоці II (Україна)
- √ **Попа, Іоана** кандидат історичних наук, доцент, доцент кафедри історії Інституту соціальних наук про політику (Франція)
- √ **Робак Ігор Юрійович** - доктор історичних наук, професор, завідувач кафедри суспільних наук Харківського національного медичного університету (Україна)
- √ **Рубан Микола Юрійович** - доктор філософії з історії та археології, член правління Луганського обласного об'єднання ВУТ "Просвіта" імені Тараса Шевченка, голова правління громадської організації "Фонд відновлення залізничної спадщини України" (Україна)
- √ **Сайд М. Ісмаїл** доктор наук, професор, професор кафедри англійської мови, Коледж природничих наук і гуманітарних наук, Університет принца Саттама бін Абдулазіза, Аль-Хардж (Саудівська Аравія)
- √ **Синявська Олена Олександрівна** - кандидат історичних наук, доцент, доцент Одеського національного університету імені І. І. Мечникова (Україна)
- √ **Січкаренко Галина Геннадіївна** - доктор історичних наук, доцент, професор кафедри документознавства та інформаційної діяльності Державного університету телекомунікацій (Україна)
- √ **Скляр Ірина Олександрівна** - кандидат філологічних наук, доцент, доцент кафедри української філології, доцент кафедри світової літератури Горлівського інституту іноземних мов ДВНЗ Донбаський Державний педагогічний університет, постдокторант (Україна)
- √ **Супрун Володимир Миколайович** – доктор філологічних наук, доцент, професор кафедри журналістики та українознавства Національного університету водного господарства та природокористування (Україна)
- √ **Хитровська Юлія Валентинівна** - доктор історичних наук, професор, професор кафедри історії факультету соціології і права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» (Україна)
- √ **Юган Наталія Леонідівна** – доктор філологічних наук, доцент, професор кафедри літературознавства, східної філології і перекладу Луганського національного університету імені Тараса Шевченка, практичний психолог у закладах освіти, член Центру українсько-європейського наукового співробітництва, Української асоціації когнітивної лінгвістики та поетики, Міжнародної федерації арт-терапії та самореалізації особистості (Україна)

**Статті розміщені в авторській редакції.
Відповідальність за зміст та орфографію поданих матеріалів несуть автори.**

Шановні колеги, любі друзі!



Вийшов черговий випуск журналу категорії Б із історії, археології, педагогіки та філології «Вісник науки та освіти».

Видання відзначається багатогранністю відтворення змістового компоненту і значним інформаційним наповненням із питань: теоретичного обґрунтування академічної доброчесності як методологічної основи науково-педагогічних досліджень у системі професійної освіти та визначення її ролі у забезпеченні якості освіти, достовірності й наукової цінності дослідницьких результатів; дослідження функцій та педагогічної цінності формувального оцінювання в межах інтегрованого курсу «Природничі науки» для учнів 7–9 класів, що реалізується у контексті реформи Нової української школи; осмислення авторського бачення перекладацького процесу та його місця в міжкультурній комунікації, аналізуючи здебільшого матеріали інтерв'ю з О.Н. Мушкудіані; аналізу методологічного потенціалу цифрової демографії для вивчення змін етнічного складу населення, оцінки переваг та обмежень використання цифрових слідів у порівнянні з традиційними переписами та ін.

Щоденних перемог нам, друзі, задля спільної Перемоги!

Дякуємо ЗСУ за кожен день нашого життя!

**З повагою,
директор Видавничої групи
«Наукові перспективи»,
директор Європейського ліцею
«Наукові перспективи»**

Ірина Жукова



ЗМІСТ

СЕРІЯ «ФІЛОЛОГІЯ»

- Bilova A.H., Budilova O.V., Volkova M.Yu.** 40
*TEACHING INTERCULTURAL COMMUNICATIVE COMPE-
TENCE THROUGH AUTHENTIC VIDEO CONTENT IN TEFL*
- Derkach Yu. Ya.** 52
*FROM STORY TO STRUCTURE: INTEGRATING ENGLISH
CHILDREN'S LITERATURE INTO GRAMMAR INSTRUCTION
WHEN TEACHING ENGLISH IN PRIMARY SCHOOL*
- Dibrova V. A., Dukhanina N. M.** 64
*THE CATEGORY OF NEGATION IN MODERNd ENGLISH:
STRUCTURAL, SEMANTIC AND PRAGMATIC DIMENSIONS*
- Dolynskiy Ie. V., Boiko D. S.** 72
*TRANSLATION STRATEGIES FOR RENDERING COMMON LAW
TERMS IN UKRAINIAN LEGAL DISCOURSE*
- Hlazkova I. Ya., Khalabuzar O. A., Kharchenko T. I.** 85
*LANGUAGE STRATEGIES OF MANIPULATIVE INFLUENCE IN
THE MEDIA AND POLITICAL SPACE*
- Novakivska L. V., Osipenko N. S.** 99
*USING TECHNOLOGIES FOR DEVELOPING CRITICAL
THINKING IN UKRAINIAN LITERATURE CLASSES*
- Novakivska L. V., Yovenko L. I.** 111
*A GENDER APPROACH TO THE ANALYSIS OF A LITERARY
WORK*
- Nykyporets S.S., Kot S.O., Hadaichuk N.M., Ibrahimova L.V.,
Chopliak V.V.** 121
*ARGUMENTATION PATTERNS IN POWER ENGINEERING
STUDENT RESEARCH WRITING: HOW LEARNERS CONST-
RUCT CAUSALITY, EVIDENCE, AND GENERALIZATIONS*



- Pastukh I. V.** 140
MULTIMODALITY IN CONTEMPORARY ENGLISH SOCIAL ADVERTISING
- Popova I. S., Posudiiievska O. R.** 155
PECULIARITIES OF USING MEDICAL VOCABULARY IN THE DISCOURSE OF ENGLISH-SPEAKING MILITARY CAREGIVERS
- Pryshupa Yu. Yu.** 172
ENGLISH FOR SPECIFIC PURPOSES AS A LINGUISTIC SYSTEM IN THE DIGITAL COMMUNICATION SPACE OF A TECHNICAL UNIVERSITY
- Serhienko L. V., Shuhai A. Yu., Badior N. B.** 186
LEXICAL NON-EQUIVALENCE AS A KEY ISSUE IN LEGAL AND MILITARY TRANSLATION
- Shevchenko O. L., Sinitsyna N. M., Kapustina O. V.** 202
KNOWING, EXPECTING AND FEARING THE MARKET: EPISTEMIC OPERATORS IN CONTEMPORARY ENGLISH ECONOMIC JOURNALISM
- Shlikhtenko Yu. V., Martseniuk O. H.** 216
FROM SHAKESPEARE TO SOCIAL MEDIA: DIACHRONIC TRANSFORMATIONS OF ENGLISH STYLISTIC DEVICES
- Shylo A., Honsalies-Munis S.** 229
LINGUISTIC CONSTRUCTION OF VICTIM IDENTITY IN EDITH EVA EGER'S HOLOCAUST MEMOIR: FROM POWERLESSNESS TO AGENCY
- Tsyhanok O. O., Sanivskyi O. M., Honcharuk V. A., Kyrychenko V. G.** 242
THE IMAGE OF THE UKRAINIAN VILLAGE IN THE LITERATURE OF THE 1970s-1990s: FROM ETHNOGRAPHIC IDYLLY TO SOCIO-PSYCHOLOGICAL ANALYSIS
- Александрович Т. З., Малинка М. М.** 253
ІНТЕРАКТИВНІ ТЕХНОЛОГІЇ НАВЧАННЯ ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОСТІ ОСВІТНЬОГО ПРОЦЕСУ НА ЗАНЯТТЯХ З УКРАЇНСЬКОЇ ЛІТЕРАТУРИ В КОЛЕДЖІ



- Андрієвська Е. М.** 265
СТРАТЕГІЇ ВИРІШЕННЯ ПРОБЛЕМ В УСНОМУ ПЕРЕКЛАДІ
- Антонюк-Кириченко С. А.** 279
*ДЕРИВАЦІЙНІ СПРОМОЖНОСТІ ДОТИКОВИХ АД'ЕКТИВІВ
У ПОЕТИЧНІЙ СПАДЩИНІ ПУБЛІА ВЕРГІЛІЯ МАРОНА*
- Бахов І. С., Робакова К. А.** 293
*АМЕРИКАНСЬКИЙ ТА БРИТАНСЬКИЙ ГУМОР У МОВІ ТА
КУЛЬТУРИ: ПОРІВНЯЛЬНИЙ АНАЛІЗ*
- Білик О. О., Пуга О. О., Подоляк З. Р.** 302
*ЛЕКСИЧНІ, МОРФОЛОГІЧНІ, СИНТАКСИЧНІ ОСОБЛИ-
ВОСТІ РЕКЛАМНИХ ТЕКСТІВ В ЦИФРОВОМУ ПРОСТОРІ*
- Білічак О. І., Лашків Т. В.** 315
*ФОРМУВАННЯ МІЖКУЛЬТУРНОЇ ІНШОМОВНОЇ КОМПЕ-
ТЕНТНОСТІ НА ПРАКТИЧНИХ ЗАНЯТТЯХ З АНГЛІЙСЬКОЇ
ТА ФРАНЦУЗЬКОЇ МОВ*
- Бойчук В. М., Бойчук М. В.** 324
*ЛІНГВАЛЬНА ПРИРОДА НЕОЛОГІЗМІВ АНГЛІЙСЬКОЇ ТА
УКРАЇНСЬКОЇ МОВ: ЗІСТАВНІ СТУДІЇ*
- Ватченко С.О., Максютенко О.В.** 338
*«І ОТ ПИТАННЯ – БУТИ ЧИ НЕ БУТИ...» ПРО ЖИТТЯ І
СМЕРТЬ АВТОРА В ЛІТЕРАТУРІ*
- Венгринович А. А., Весоловський О. В.** 353
*ФУНКЦІОНАЛЬНО-СЕМАНТИЧНІ ТА СИНТАКСИЧНІ
МОДИФІКАЦІЇ СКЛАДНИХ КОНСТРУКЦІЙ У СУЧАСНОМУ
НІМЕЦЬКОМОВНОМУ МАСМЕДІЙНОМУ ДИСКУРСІ*
- Вергун Т. М., Романчева Ю. Ф., Барабашук Ю. В.** 366
*ГЕНДЕРНА НЕЙТРАЛЬНІСТЬ В АНГЛІЙСЬКІЙ МОВІ:
ТЕНДЕНЦІЇ ТА ВИКЛИКИ СУЧАСНОГО СУСПІЛЬСТВА*
- Вихованець (Іжевська) З.С.** 382
*МОВЛЕННЄВІ СТРАТЕГІЇ АНГЛОМОВНОГО ПРОФЕСІЙ-
НОГО ДИСКУРСУ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я*



- Возняк І. З.** 393
*МЕДІАГРАМОТНІСТЬ НА ЗАНЯТТЯХ ІНОЗЕМНОЇ МОВИ
ПРОФЕСІЙНОГО СПІЛКУВАННЯ У ВІЙСЬКОВОМУ ЗВО*
- Герман В. В., Шевченко В. Є.** 407
*КРИТИЧНЕ МИСЛЕННЯ ТА МОВНА ОСОБИСТІТЬ:
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ВЗАЄМОЗВ'ЯЗКУ В
ОСВІТНЬОМУ ПРОЦЕСІ СТАРШОЇ ШКОЛИ*
- Голопич І. М., Оверчук О. Б., Перцева В. А.** 419
*ОСОБЛИВОСТІ МОВНОГО ОФОРМЛЕННЯ ЕЛЕКТРОННИХ
ДОКУМЕНТІВ*
- Гонца І. С.** 433
*ПСИХОЛІНГВІСТИЧНІ ПАРАМЕТРИ УКРАЇНО-ПОЛЬСЬКОЇ
МІЖМОВНОЇ ВЗАЄМОДІЇ*
- Горбаченко А. Л., Рябокучма Т. О., Цимбаленко М. Ю.** 443
*МОВНА РЕПРЕЗЕНТАЦІЯ ЕМОЦІЙ: ПОРІВНЯЛЬНИЙ
АНАЛІЗ АНГЛІЙСЬКОЇ ТА НІМЕЦЬКОЇ МОВ*
- Дерба В. С.** 455
*ВИКОРИСТАННЯ СУЧАСНИХ ЗАСОБІВ ПРОГРАМНОГО
ЗАБЕЗПЕЧЕННЯ ДЛЯ ФІКСАЦІЇ ДІАЛЕКТНОГО МАТЕРІАЛУ*
- Добровольська Н. Л.** 468
*РОЗВИТОК МОВЛЕННСВОЇ АКТИВНОСТІ СТУДЕНТІВ-
ФІЛОЛОГІВ 2 КУРСУ ПРИ ВИВЧЕННІ НІМЕЦЬКОЇ МОВИ
ЯК ДРУГОЇ ІНОЗЕМНОЇ (АНГЛІЙСЬКА — ОСНОВНА)*
- Западинська І. Г.** 478
*КУЛЬТУРА МОВЛЕННЯ МАЙБУТНІХ ПЕРЕКЛАДАЧІВ ЯК
ПРОФЕСІЙНА ЦІННІСТЬ: ТЕОРЕТИЧНІ ЗАСАДИ ТА
МЕТОДОЛОГІЧНІ ОРІЄНТИРИ ФОРМУВАННЯ*
- Ігнатська С. Є., Цюп'як І. К.** 489
*ВЕРБАЛІЗАЦІЯ КОНЦЕПТІВ «ЛЮБОВ» І «КОХАННЯ» В
ЩОДЕННИКОВОМУ ДИСКУРСІ ОЛЕСЯ ГОНЧАРА*



- Калашник О. О.** **502**
ЛІРИЧНА ДРАМА «ЗІВ'ЯЛЕ ЛИСТЯ» ІВАНА ФРАНКА У ПОЕТИЧНО-ХОРЕОГРАФІЧНІЙ ПОСТАНОВЦІ: ОСОБЛИВОСТІ ІНТЕРМЕДІАЛЬНОГО ПЕРЕКОДУВАННЯ
- Камінська О. І.** **518**
ПСИХОЛІНГВІСТИЧНИЙ КЕЙС ВИВЧЕННЯ ІНОЗЕМНОЇ МОВИ В ЗАКЛАДІ ВИЩОЇ ОСВІТИ
- Корнієнко І. В., Сковородецька Р. А.** **529**
КРИМСЬКОТАТАРСЬКА КУЛЬТУРА ЯК ЧИННИК ФОРМУВАННЯ УКРАЇНСЬКОЇ СХІДНОЇ ІДЕНТИЧНОСТІ
- Коробова І. О., Регушевська І. А., Назаренко Н. Г.** **544**
ОСОБЛИВОСТІ ВИКОРИСТАННЯ ІНТЕРАКТИВНИХ МЕТОДІВ І ТЕХНОЛОГІЙ НА ПРАКТИЧНИХ ЗАНЯТТЯХ З УКРАЇНСЬКОЇ ТА ІНОЗЕМНИХ МОВ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ СПОРТИВНОГО СПРЯМУВАННЯ
- Косенко А. В., Дідковська Т. Л., Сорочан О. В.** **558**
СЛЕНГ СОЦІАЛЬНИХ МЕРЕЖ ЯК ПРОБЛЕМА СУЧАСНИХ МОВОЗНАВЧИХ ТА ПЕРЕКЛАДОЗНАВЧИХ ДОСЛІДЖЕНЬ
- Крепель В. І., Ганецька Л. В.** **571**
КОЛЬОРАТИВИ НІМЕЦЬКОЇ МОВИ: ВІД НОМІНАЦІЇ ДО ПРАГМАТИКИ
- Кузьмич О. А.** **588**
ФЕНОМЕН ПЕРЕКЛАДАЦЬКОЇ МАЙСТЕРНОСТІ О. Н. МУШКУДІАНІ (1938 – 2025 рр.)
- Кукушкін В. В., Артиш О. О.** **598**
КОГНІТИВНІ МЕХАНІЗМИ ТВОРЕННЯ НЕОЛОГІЗМІВ У БРИТАНСЬКОМУ ТА АМЕРИКАНСЬКОМУ ВАРІАНТАХ АНГЛІЙСЬКОЇ МОВИ
- Куций І. П., Куца Л. П.,** **612**
ПАМ'ЯТЬ АВТОРИТЕТНОГО СЛОВА В «ІСТОРИЧНОМУ ЗМИСЛІ» ІВАНА ФРАНКА



- Ленартович О. О.** 627
*МОВНО-ВИРАЗОВІ ПАРАЛЕЛІ РОСІЙСЬКО-УКРАЇНСЬКОЇ
ВІЙНИ ТА БРИТАНСЬКО-НІМЕЦЬКОГО ПРОТИСТОЯННЯ В
ДРУГІЙ СВІТОВІЙ ВІЙНІ*
- Луцик Н. М., Воронько Г. М., Крук З. М.** 638
*ВПЛИВ ЦИФРОВОЇ ГЕЙМІФІКАЦІЇ НА ВНУТРІШНЮ
МОТИВАЦІЮ ЗДОБУВАЧІВ ЗВО В ПРОЦЕСІ ВИВЧЕННЯ
ФРАНЦУЗЬКОЇ МОВИ*
- Мазуренко Л. І.** 654
ЕВОЛЮЦІЯ УКРАЇНСЬКОЇ ЕКОЛІНГВІСТИЧНОЇ ДУМКИ
- Малинюк І.В.** 667
*СЕМАНТИЧНІ ТИПИ ЗВУКОНАСЛІДУВАЛЬНИХ СЛІВ
У КИТАЙСЬКІЙ ТА УКРАЇНСЬКІЙ МОВАХ*
- Маркуляк Л. В.** 680
*ХУДОЖНІ МЕРИДІАНИ ПОЕТИЧНОГО ПРОСТОРУ ОЛЕНИ
ТЕЛІГИ: ПОЕЗІЯ ЧИНУ*
- Маштакова Н. В.** 695
*КУЛЬТУРНА ТА ЕКОНОМІЧНА ЗУМОВЛЕНІСТЬ ПРИКМЕТ:
ВИКЛИКИ ДЛЯ ПЕРЕКЛАДАЧА*
- Миськів І. С.** 705
СТРУКТУРНІ ОСОБЛИВОСТІ РЕКЛАМНИХ ТЕКСТІВ
- Мішукова О. М.** 718
*ІСПАНСЬКІ ПАРЕМІЇ З ГАСТРОНОМІЧНИМ КОМПОНЕНТОМ
ЯК ВІДОБРАЖЕННЯ НАЦІОНАЛЬНО-КУЛЬТУРНОЇ
ІДЕНТИЧНОСТІ*
- Момот Н. М.** 730
*КУЛЬТУРА ПРОФЕСІЙНОГО СПІЛКУВАННЯ В УМОВАХ
ЦИФРОВІЗАЦІЇ*
- Муляр І. В., Панченко О. І., Шевчик К. Ю., Клименко Т. А.** 742
*ГРАМАТИЧНІ ОСОБЛИВОСТІ ПЕРЕКЛАДУ АНГЛІЙСЬКИХ
МЕБЛЕВИХ ТЕРМІНІВ*



- Негер О. Б.** 754
ЛІНГВОКУЛЬТУРНИЙ ПОТЕНЦІАЛ ОНІМІВ У ШКІЛЬНОМУ КУРСІ УКРАЇНСЬКОЇ МОВИ
- Нестеренко О. О., Ліксунова С. В.** 766
ЛІНГВАЛЬНІ ОСОБЛИВОСТІ ФОРМУВАННЯ СТЕРЕОТИПНОГО ОБРАЗУ ІНОЗЕМЦЯ В КИТАЙСЬКОМУ ГУМОРИСТИЧНОМУ ДИСКУРСІ
- Ніколаєва Т. М., Антоненко І. І., Калініченко Т. М.** 778
РОЗВИТОК КОГНІТИВНО-МОВЛЕННСВИХ СТРАТЕГІЙ У ПРОЦЕСІ ДИСТАНЦІЙНОГО НАВЧАННЯ ІНОЗЕМНОЇ МОВИ
- Островський О. О., Молнар Є. Р.** 793
КУЛЬТУРНА СПАДЩИНА ПОЕТІВ-ПРОЗАЇКІВ ХІХ-ХХ СТ.
- Панченко О. І., Білоус К. С.** 803
ФОНЕТИЧНІ ТА СТИЛІСТИЧНІ ЗАСОБИ У «КЕНТЕРБЕРІЙСЬКИХ ОПОВІДАННЯХ» ДЖ. ЧОСЕРА
- Панченко О. І., Білоус К. С.** 817
«СНІДАНОК У ТІФФАНІ» Т. КАПОТЕ. ЛІТЕРАТУРНИЙ ТЕКСТ Й ЕКРАНІЗАЦІЯ
- Панченко О. І., Шевчик К. Ю., Вотінцева М. Л.** 831
ПРОБЛЕМА ПЕРЕКЛАДУ ТЕРМІНІВ З АНГЛІЙСЬКОЇ МОВИ УКРАЇНСЬКОЮ У ТЕКСТАХ ГАЛУЗІ ІНТЕРНЕТ-ТЕХНОЛОГІЙ (граматичний аспект)
- Пена Л. І.** 844
ДЕЯКІ АСПЕКТИ ВИВЧЕННЯ ВИБІРКОВОГО КУРСУ «СЛОВОТВІР І ТЕКСТ»
- Петренко В. Ю.** 859
АНГЛІЙСЬКА МОВА ЯК СКЛАДОВА ПРОФЕСІЙНОЇ ПІДГОТОВКИ СТУДЕНТІВ НЕМОВНИХ СПЕЦІАЛЬНОСТЕЙ
- Пілик В. В., Гнатюк О. О.** 869
МОВНА ЕКСПЛІКАЦІЯ КАТЕГОРІЇ ЕМОТИВНОСТІ В ТУРЕЦЬКОМУ МЕРЕЖЕВОМУ ДИСКУРСІ



- Пілик В. В., Ергевереджин Ф. С.** 883
*СТРУКТУРНО-СЕМАНТИЧНІ ОСОБЛИВОСТІ ВИГУКІВ У
ТУРЕЦЬКІЙ МОВІ*
- Пічугіна Т. Є** 897
«ЧАРИ» ГЕРМАНА БРОХА: МІЖ ПОЛІТИКОЮ ТА МІФОМ
- Разуменко І. В., Чихаріна К. І.** 913
*ПОСТКОЛОНІАЛЬНІ МОДЕЛІ НАЦІОНАЛЬНОЇ ІДЕНТИЧ-
НОСТІ У КИТАЙСЬКОМОВНІЙ ЛІТЕРАТУРІ СИНГАПУРУ*
- Савенко Л. П., Юрійчук Н. Д.** 923
*ПРИСЛІВНИК У СУЧАСНІЙ УКРАЇНСЬКІЙ ЛІТЕРАТУРНІЙ
МОВІ: СЛОВОТВІРНІ ТЕНДЕНЦІЇ, СЕМАНТИКО-ФУНКЦІО-
НАЛЬНА СПЕЦИФІКА ТА ОРФОГРАФІЧНІ НОРМИ*
- Семенюк О.Б.** 942
*ЖАНРОВО-СТИЛЬОВІ МОДИФІКАЦІЇ ПРИВАТНОГО ЕПІС-
ТОЛЯРІЮ ВІНСТОНА ЧЕРЧИЛЛЯ*
- Соленко А., Кебало М.** 955
*ЕТИКА СУМНІВУ: АМБІВАЛЕНТНІСТЬ МОРАЛЬНОГО
ВИБОРУ В СУЧАСНІЙ ІНТЕЛЕКТУАЛЬНІЙ ДРАМІ ТА ПРОЗИ*
- Стацюк Р. В.** 966
*ДО ПРОБЛЕМИ КЛАСИФІКАЦІЇ СПЕЦІАЛЬНОЇ ЛЕКСИКИ:
КРИТИЧНИЙ АНАЛІЗ ПОНЯТЬ «ТЕРМІН», «ПРОФЕСІО-
НАЛІЗМ», «НОМЕН»*
- Супрун В. М., Мазур Н. В.** 981
*ФОРМУВАННЯ МІЖКУЛЬТУРНОЇ КОМПЕТЕНТНОСТІ
СТУДЕНТІВ-МЕДИКІВ ПІД ЧАС ВИВЧЕННЯ АНГЛІЙСЬКОЇ
МОВИ*
- Танана С. М.** 989
*КОГНІТИВНИЙ ПІДХІД У ФОРМУВАННІ АНГЛОМОВНОЇ
ЛЕКСИЧНОЇ КОМПЕТЕНТНОСТІ УЧНІВ СТАРШОЇ
ШКОЛИ: КОНСЕРВАТИВНА ЛЕКСИКА*



- Тележкіна О.О., Костюк Ю.М.** 999
УКРАЇНСЬКА ДІАСПОРА В КАНАДІ: ЗБЕРЕЖЕННЯ МОВНОЇ ІДЕНТИЧНОСТІ В МУЛЬТИКУЛЬТУРНОМУ ПРОСТОРИ
- Тулюлюк К. В.** 1010
ВИВЧЕННЯ ІНОЗЕМНОЇ МОВИ ЯК ФАКТОР ФОРМУВАННЯ КРИТИЧНОГО МИСЛЕННЯ В ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ
- Фомін Г. Г.** 1021
ПРО ЖАНРОВУ ПРИРОДУ «МОРОКІВ» ОЛЕКСАНДРА МИХЕДА
- Хавалджи Л.В.** 1030
МОВА ПУБЛІЦИСТИКИ В. ЯВОРІВСЬКОГО ЯК ВІДОБРАЖЕННЯ ЙОГО МОВНОГО СВІТОГЛЯДУ
- Харжевська О. М.** 1044
ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ВИКЛАДАННЯ ІНОЗЕМНОЇ МОВИ ДЛЯ ЗДОБУВАЧІВ ОСВІТИ СПЕЦІАЛЬНОСТІ «ПРАВО» В КОНТЕКСТІ ЮРИДИЧНОГО ДИСКУРСУ
- Хоміцький Н.** 1058
ХУДОЖНЬО-ВИРАЖАЛЬНІ ЗАСОБИ ЛЕКСИКО-СИНТАКСИЧНОЇ ПРИРОДИ У ВОЄННІЙ ПРОЗІ ОЛЕКСАНДРА ВІЛЬЧИНСЬКОГО (на матеріалі повісті «Останні герой»)
- Чайка Л. В., Лозинська Л. Ф., Глінська Н. І.** 1068
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ (CHAT GPT, GRAMMARLY, DEEPL) У НАВЧАННІ АКАДЕМІЧНОГО ПИСЬМА АНГЛІЙСЬКОЮ МОВОЮ
- Чепурна М. В., Панькова А. В., Потенко Л. О.** 1081
КОГНІТИВНО-ПРАГМАТИЧНИЙ ВИМІР ФУНКЦІОНУВАННЯ МЕТАФОРИ В АНГЛОМОВНОМУ МІЖКУЛЬТУРНОМУ КОМУНІКАТИВНОМУ ДИСКУРСІ
- Чонка Т. С., Немеш І.** 1095
ЕТИЧНІ ВИКЛИКИ ТА МОРАЛЬНІ ДИЛЕМИ СУЧАСНОЇ ЖІНКИ У ПОВІСТІ-ПРИТЧІ ОСАНИ ЗАБУЖКО «Я, МІЛЕНА»



Чорній Р. П., Святюк Ю. В., Могельницька Л. Ф. 1109
*ІНФОРМАЦІЙНИЙ ТЕКСТ ЯК КОНСТИТУАНТ ЦИФРОВОГО
ДИСКУРСУ. ПОРІВНЯЛЬНІ ОСОБЛИВОСТІ ТА СТРАТЕГІЇ*

Чорноус О. В. 1122
*ПУБЛІЧНЕ МОВЛЕННЯ ФАХІВЦІВ ТА ГЕНДЕРНИЙ
ДИСКУРС*

Чухно Т. В. 1133
*ДИНАМІКА РОЗВИТКУ ЛЕКСИКИ НІМЕЦЬКОЇ МОВИ ПІД
ВПЛИВОМ АНГЛІЦИЗМІВ ТА ГЛОБАЛІЗАЦІЇ*

Якушенко І. О., Приходько О. О. 1143
*ЗВ'ЯЗОК ІМПЛІЦИДНИХ НАВИЧОК ТА ПРИНЦИПІВ
НЕЙРОЛІНГВІСТИЧНОГО ПІДХОДУ ПРИ ВИВЧЕННІ
ІНОЗЕМНОЇ МОВИ (АНГЛІЙСЬКОЇ)*

Яновець А. І., Гончар К. Л., Чарікова І. В. 1156
*ЕФЕКТИВНІСТЬ ІМЕРСИВНИХ ТЕХНОЛОГІЙ ПРИ ФОРМУ-
ВАННІ ЛЕКСИЧНОЇ КОМПЕТЕНТНОСТІ ПЕРЕКЛАДАЧІВ У
ВИЩІЙ ШКОЛІ*

СЕРІЯ «ПЕДАГОГІКА»

Ahibalova T.M., Shevchenko V.M., Mazhula T.V. 1174
*PROVIDING EFFECTIVE SCAFFOLDING INSTRUCTION
IN FOREIGN LANGUAGE EDUCATION*

Antoniv A.A., Antoniv N.A. 1190
*FORMATION OF PROFESSIONAL COMPETENCIES OF 5TH–
6TH YEAR STUDENTS IN THE PROCESS OF TEACHING
INTERNAL MEDICINE*

Bilan N.I., Khazova O.V. 1199
*ROLE STRUCTURES GOVERNANCE IN THE PROCESSES OF
ENGLISH SYNTACTIC CONSTRUCTIONS GENERATION AND
FUNCTIONING*

Bozhynska M., Grynyova M. 1209
*PRINCIPLES OF FORMATIVE ASSESSMENT IN THE INTEG-
RATED SCIENCE COURSE FOR STUDENTS IN GRADES 7-9*



- Bozhynska M., Grynyova M.** 1222
THE COMPETENCY-ORIENTED VECTOR OF FORMATIVE ASSESSMENT IN THE BLENDED LEARNING FORMAT OF THE INTEGRATED NATURAL SCIENCES COURSE
- Honcharova O.S.** 1235
HUMANITARIAN EDUCATION IN WAR CONDITIONS: CHALLENGES, RISKS AND VALUE GUIDELINES
- Hontarenko I.S.** 1245
DIGITALIZATION OF DISTANCE LEARNING AS A FACTOR IN THE FORMATION OF PROFESSIONAL AND MANAGERIAL COMPETENCE OF FUTURE MANAGERS IN THE FIELD OF PHYSICAL CULTURE
- Knyshevytska L.** 1259
STIMULATING ENGLISH LANGUAGE LEARNING BY BUILDING COMMUNICATIVE COMPETENCE OF UNIVERSITY STUDENTS MAJORING IN INTERNATIONAL RELATIONS
- Koryahin V.M.** 1268
MULTIDIMENSIONAL ASSESSMENT OF PERFORMANCE CHARACTERISTICS IN PROFESSIONAL BASKETBALL PLAYERS
- Kuzina Yu.V.** 1276
FOREIGN EXPERIENCE IN THE USE OF MATHEMATICAL PRINCIPLES FOR TEACHING LOGISTICS IN EUROPEAN UNIVERSITIES
- Lysak H.** 1288
DEVELOPMENT OF STUDENTS' PHONETIC COMPETENCE IN HIGHER EDUCATION
- Paladieva A.F.** 1299
METHODS OF TEACHING LATIN IN HIGHER EDUCATION INSTITUTIONS IN UKRAINE IN THE CONTEXT OF A COMPETENCE-BASED APPROACH
- Petrenko V.Yu.** 1310
LANGUAGE-AWARE EMI IN CONTENT COURSES: INTEGRATION, METHODOLOGY, AND STUDENT ENGAGEMENT



- Pohranychna N.** 1332
THE ROLE OF ARTIFICIAL INTELLIGENCE IN FOREIGN LANGUAGE LEARNING AMONG HIGHER EDUCATION STUDENTS
- Shyrmova T.Ye.** 1345
THE RELEVANCE OF IMPLEMENTING A COMPETENCY-BASED APPROACH INTO THE EDUCATIONAL PROCESS TO SOLVING THE PROBLEM OF EDUCATION QUALITY
- Sukhanova T.Ye., Lazareva O.Ya.** 1356
PSYCHOLOGICAL STRESS AND TRANSFORMATION OF STUDENTS' ATTITUDES TOWARDS LEARNING FOREIGN LANGUAGES IN THE CONTEXT OF THE ONGOING WAR IN UKRAINE
- Troukhanova N.** 1374
ROLE-PLAYING AS AN EFFECTIVE METHOD FOR TEACHING MARITIME ENGLISH TO FUTURE NAVIGATORS
- Vergun A.R., Havryliuk I.M., Yahelo S.P., Vergun O.M., Parashchuk B.M., Kalytovska M.B., Zanik O.I., Makahonov I.O., Oleksiuk O.B.** 1385
ACADEMIC INTEGRITY AS A COMPONENT OF THE SYSTEM OF INTERNAL QUALITY ASSURANCE OF EDUCATIONAL ACTIVITIES IN A MEDICAL UNIVERSITY: SOME ORGANIZATIONAL AND MODERN IMPLEMENTATION ASPECTS
- Voronova Ye.M., Herasymchuk T.V., Gubareva O.S.** 1398
PBL METHODOLOGIES WITH COMMUNICATIVE COMPETENCE DEVELOPMENT
- Voznyuk O.V.** 1411
ANALYSIS OF THE CONTENT AND STRUCTURE OF MULTICULTURAL COMPETENCE IN THE CONTEXT OF GENERAL SYSTEMS THEORY: FOREIGN EXPERIENCE
- Zeniakin O.** 1425
SPEAKING CLUBS AS A WAY OF IMPLEMENTING GERMAN UNIVERSITY TEACHERS' EXPERIENCE IN DEVELOPING STUDENTS' FOREIGN LANGUAGE COMMUNICATIVE COMPETENCE WITHIN EXTRACURRICULAR ACTIVITIES



- Zhukevych I.P., Biriukova N.A., Novikova I.Ie.** 1444
SMART INSTRUCTIONAL DESIGN IN ENGLISH LANGUAGE TEACHING
- Аліксійчук Я.О.** 1456
МЕТОДИКА ФОРМУВАННЯ ПОЛІСТИЛИСТИЧНОЇ КОМПЕТЕНТНОСТІ ЗДОБУВАЧІВ ВИЩОЇ МИСТЕЦЬКО-ПЕДАГОГІЧНОЇ ОСВІТИ В ПРОЦЕСІ ОПАНУВАННЯ БАНДУРНИХ КОМПОЗИЦІЙ
- Андерсон І.В.** 1473
ВИКЛАДАЧІ-УКРАЇНЦІ ЯГЕЛЛОНСЬКОГО УНІВЕРСИТЕТУ: ІСТОРИЧНИЙ ВНЕСОК У РОЗВИТОК ОСВІТИ Й НАУКИ
- Атамась О.А., Гаценко В.П., Гріцишина Ж.М.** 1481
МЕТОДИКА КОНСТРУВАННЯ ЗАНЯТЬ З КЛАСИЧНОЇ АЕРОБІКИ У ПРОЦЕСІ ФАХОВОЇ ПІДГОТОВКИ МАЙБУТНІХ УЧИТЕЛІВ ФІЗИЧНОЇ КУЛЬТУРИ
- Бабич М.Є., Бондар А.В., Самар О.М., Фурманчук Н.М.** 1494
ПЕРЕВЕРНУТЕ НАВЧАННЯ У ВИКЛАДАННІ АНГЛІЙСЬКОЇ МОВИ У ЗВО
- Бартенєва І.О., Кинєва П.П.** 1509
ПІДГОТОВКА ДО ПЕДАГОГІЧНОЇ ПРАКТИКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ В УМОВАХ УНІВЕРСИТЕТСЬКОГО ОСВІТНЬОГО СЕРЕДОВИЩА: ОРГАНІЗАЦІЙНО-МЕТОДИЧНІ ЗАСАДИ
- Безнос Є.О.** 1525
УПРАВЛІННЯ ЯКІСТЮ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МЕНЕДЖЕРІВ ЗОВНІШНЬОЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ
- Бержанір А.Л.** 1540
ФОРМУВАННЯ КЛЮЧОВИХ КОМПЕТЕНТНОСТЕЙ ЗДОБУВАЧІВ ЗАСОБАМИ СОЦІАЛЬНО-ГУМАНІТАРНОЇ ПІДГОТОВКИ



- Білан В., Підлипняк І.** 1551
*ПРОФЕСІЙНА ЕТИКА ВИХОВАТЕЛЯ ЯК ЧИННИК
ЕФЕКТИВНОЇ ВЗАЄМОДІЇ З ДІТЬМИ ТА БАТЬКАМИ*
- Браславська О.В.** 1563
*КОМПЕТЕНТІСНО-ОРІЄНТОВАНИЙ КОНТРОЛЬ ЗА ОСВІТ-
НЬОЮ ДІЯЛЬНІСТЮ МАЙБУТНІХ УЧИТЕЛІВ ГЕОГРАФІЇ*
- Браславська О.В.** 1577
*ПРОФЕСІЙНА ДІЯЛЬНІСТЬ УЧИТЕЛЯ ФІЗИЧНОЇ КУЛЬ-
ТУРИ КРИЗЬ ПРИЗМУ ЗДОРОВ'ЯЗБЕРЕЖУВАЛЬНОЇ КОМ-
ПЕТЕНТНОСТІ*
- Бутенко Г.О.** 1592
*КРАЄЗНАВЧО-ТУРИСТИЧНА РОБОТА ЯК ЗАСІБ ФІЗИЧНОЇ
РЕКРЕАЦІЇ В КОНТЕКСТІ ІНКЛЮЗИВНОГО ФІЗИЧНОГО
ВИХОВАННЯ*
- Ваврисевич Я.С., Безносюк Н.С., Крамаренко І.С.** 1607
*МОДЕРНІЗАЦІЯ ЗМІСТУ ХІМІЧНОЇ ОСВІТИ У ЗВО В
УМОВАХ ОСВІТНІХ СТАНДАРТІВ ЄС*
- Ванда Н.В.** 1624
*ПРОФІЛАКТИКА РЕЛІГІЙНОГО ФАНАТИЗМУ В ПСИХОЛО-
ГІЧНОМУ КОНТЕКСТІ*
- Васильєв С.С.** 1638
*ОСВІТНЬО-ТВОРЧИЙ СТУПІНЬ ДОКТОРА МИСТЕЦТВА У
ДЗЕРКАЛІ ДОПОВІДЕЙ ПРО ЯКІСТЬ ВИЩОЇ ОСВІТИ В
УКРАЇНІ, ЇЇ ВІДПОВІДНІСТЬ ЗАВДАННЯМ СТАЛОГО
ІННОВАЦІЙНОГО РОЗВИТКУ СУСПІЛЬСТВА (2022–2024)*
- Вишківська В.Б., Патлайчук О.В., Савчук С.В.** 1654
*УПРАВЛІННЯ НАВЧАЛЬНИМИ ПРОЄКТАМИ У СФЕРІ
НАЦІОНАЛЬНО-ПАТРІОТИЧНОГО ВИХОВАННЯ*
- Вінтюк Ю.В.** 1667
*ПСИХОЛОГІЧНИЙ АНАЛІЗ СПІЛКУВАННЯ В ПРОЦЕСІ
СІМЕЙНОГО КОНСУЛЬТУВАННЯ ПРИ ПІДГОТОВЦІ
ФАХОВИХ ПСИХОЛОГІВ (на прикладі кінофільму «Весняні
надії»)*



- Гаркавий С.Ф., Бардадим О.В.** 1682
*ІНФОРМАЦІЙНА БЕЗПЕКА У СОЦІАЛЬНІЙ РОБОТІ ТА
АРТМЕНЕДЖМЕНТІ: ТИПОЛОГІЯ ЗАГРОЗ, ЦИФРОВА
КОМПЕТЕНТНІСТЬ, СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА ІНСТИ-
ТУЦІЙНІ СТРАТЕГІЇ ЗАХИСТУ*
- Глушко Т.В., Златовласова О.В.** 1695
*ФОРМУВАННЯ ІНШОМОВНОЇ ДИСКУРСИВНОЇ КОМПЕ-
ТЕНТНОСТІ СТУДЕНТІВ МОВНИХ СПЕЦІАЛЬНОСТЕЙ
ЗАСОБАМИ ІНТЕРАКТИВНИХ ТЕХНОЛОГІЙ*
- Годун Н.І., Миздренко О.М., Палієнко О.А.** 1703
*НАУКОВИЙ ДОРОБОК ПРОФЕСОРА В.О. БЕЦА В ГАЛУЗІ
АНАТОМІЇ ТА ГІСТОЛОГІЇ (КІНЕЦЬ ХІХ СТОЛІТТЯ)*
- Голубова Г.В., Орехова Л.І.** 1716
*ВИКОРИСТАННЯ СУЧАСНОГО МЕТОДИЧНОГО ІНСТРУ-
МЕНТАРІЮ У МОВЛЕННЄВІЙ ПІДГОТОВЦІ УКРАЇНСЬКИХ
ТА ІНОЗЕМНИХ ФАХІВЦІВ МУЗИЧНОГО ПРОФІЛЮ*
- Гомонюк О.М., Левко М.І.** 1728
*ОСОБЛИВОСТІ ФОРМУВАННЯ ГОТОВНОСТІ МАЙБУТНІХ
БАКАЛАВРІВ ДО ВИКОРИСТАННЯ ІННОВАЦІЙ У
ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ*
- Гончар Л.В.** 1742
*ОСНОВНІ НАПРЯМИ ОРГАНІЗАЦІЇ СОЦІАЛЬНОЇ РОБОТИ З
УЧНІВСЬКОЮ МОЛОДДЮ: ДОСВІД УКРАЇНИ І ВЕЛИКОЇ
БРИТАНІЇ*
- Горбань Т.Ю.** 1753
*СОЦІАЛЬНО-ЕКОНОМІЧНИЙ ВІДДІЛ УАН (ВУАН):
ОСОБЛИВОСТІ ЕТАПУ СТАНОВЛЕННЯ ТА ПЕРШИХ РОКІВ
ДІЯЛЬНОСТІ*
- Горват М.В., Кузьма-Качур М.І.** 1765
*ДІЯЛЬНІСНИЙ ПІДХІД У КОНТЕКСТІ ІНТЕГРАЦІЇ
ПРИРОДНИЧОЇ ОСВІТНЬОЇ ГАЛУЗІ В КУРСІ «Я
ДОСЛІДЖУЮ СВІТ»*



- Гордій Н.М.** 1779
ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ГУМАНІСТИЧНОЇ СПРЯМОВАНOSTІ СПІЛКУВАННЯ СТАРШИХ ДОШКІЛЬНИКІВ
- Горохова Т.О.** 1792
ОПТИМІЗАЦІЯ МЕТОДІВ ФОРМУВАННЯ ГРАМАТИЧНОЇ КОМПЕТЕНТНОСТІ МАЙБУТНІХ УЧИТЕЛІВ УКРАЇНСЬКОЇ МОВИ І ЛІТЕРАТУРИ В УМОВАХ ЦИФРОВІЗАЦІЇ
- Грень Л.М., Грибко О.В., Чеботарьов М.К.** 1804
ІСТОРИЧНІ АСПЕКТИ ІНКЛЮЗІЇ В СОЦІАЛЬНІЙ СФЕРІ
- Гришко В.І., Цевух А.І.** 1816
СУД НАД ІСТОРИЧНОЮ ОСОБОЮ ЯК МЕТОД ІНТЕГРОВАНОГО НАВЧАННЯ ІСТОРІЇ ТА ГРОМАДЯНСЬКОЇ ОСВІТИ: МЕТОДИКА ПРОЄКТУВАННЯ І ПРОВЕДЕННЯ
- Гродзь Н.М.** 1829
КОМПЕТЕНТІСНИЙ ПІДХІД ДО ФОРМУВАННЯ КРИТИЧНОГО МИСЛЕННЯ У ВІЙСЬКОВО-ПРОФЕСІЙНІЙ ПІДГОТОВЦІ
- Груць Г.М.** 1840
ВІД ВІЗУАЛЬНОГО ОБРАЗУ ДО ПРОФЕСІЙНОЇ ЦІННОСТІ: КІНЕМАТОГРАФ ЯК ІНСТРУМЕНТ ФОРМУВАННЯ ІНКЛЮЗИВНОЇ КУЛЬТУРИ МАЙБУТНЬОГО ПЕДАГОГА
- Губенко І.Я., Шевченко О.Т., Гнатенко Т.С.** 1853
ПЕДАГОГІЧНІ ТЕХНОЛОГІЇ У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ МАЙБУТНІХ ФАХІВЦІВ ФАРМАЦЕВТИЧНОГО ПРОФІЛЮ
- Гук О.В., Клим М.І.** 1862
ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ВОЛОНТЕРСЬКОЇ ДІЯЛЬНОСТІ У СОЦІАЛЬНІЙ РОБОТІ
- Гуленко В.М.** 1873
ПРОФЕСІЙНО-ПЕДАГОГІЧНА КОМПЕТЕНТНІСТЬ ТРЕНЕРА З ВЕСЛУВАННЯ ЯК НАУКОВО-ПЕДАГОГІЧНА ПРОБЛЕМА



УДК 004:37

[https://doi.org/10.52058/2786-6165-2026-2\(44\)-1682-1694](https://doi.org/10.52058/2786-6165-2026-2(44)-1682-1694)

Гаркавий Сергій Федорович кандидат технічних наук, доцент кафедри військової підготовки ЧНУ ім.Б.Хмельницького м. Черкаси, <https://orcid.org/0009-0001-3443-4486>

Бардадим Олег Валерійович викладач кафедри освітнього, артменеджменту і соціальної роботи ЧНУ ім.Б.Хмельницького, <https://orcid.org/0000-0002-2777-6568>

ІНФОРМАЦІЙНА БЕЗПЕКА У СОЦІАЛЬНІЙ РОБОТІ ТА АРТМЕНЕДЖМЕНТІ: ТИПОЛОГІЯ ЗАГРОЗ, ЦИФРОВА КОМПЕТЕНТНІСТЬ, СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА ІНСТИТУЦІЙНІ СТРАТЕГІЇ ЗАХИСТУ

Анотація. У статті представлено розгорнутий аналіз сучасних викликів інформаційної безпеки у соціальній роботі та артменеджменті, що активно переходять до цифрових форматів діяльності й через це демонструють підвищену вразливість до кібератак. Фахівці цих сфер працюють із конфіденційними персональними даними, цифровими архівами, результатами творчої діяльності, фінансовими документами та транскордонними комунікаціями, що формує складну багаторівневу систему ризиків. У роботі представлено розширену типологію загроз, яка включає соціальну інженерію (фішинг, цільовий фішинг, претекстинг), шкідливе програмне забезпечення різних класів, мережеві та інфраструктурні атаки (DDoS, MITM, експлойти нульового дня), а також нові загрози, породжені штучним інтелектом, серед яких дипфейк-маніпуляції та автоматизовані схеми компрометації доступу. Для кожного типу визначено ключові індикатори, механізми реалізації та можливі наслідки, які можуть впливати на гуманітарні й культурні організації через витоки даних, фінансові втрати, порушення операційної діяльності й зниження довіри користувачів. У статті запропоновано цілісний комплекс правил цифрової гігієни, орієнтований на практичне застосування: використання менеджерів паролів, багатфакторної автентифікації, шифрування пристроїв, аудит доступу, контроль активності в хмарних сервісах, безпечна робота з публічними мережами, резервне копіювання та моніторинг аномалій. Розроблено чотирирівневу модель цифрової компетентності, яка охоплює базове усвідомлення загроз, операційні навички, аналітичні спроможності та інституційне лідерство в



питаннях кібербезпеки. Для кожного рівня подано типові навчальні завдання, адаптовані до професійних сценаріїв соціальних працівників і артменеджерів. Показано, що поєднання індивідуальної компетентності з організаційною політикою безпеки формує стійку модель кіберзахисту, необхідну для підтримання надійності, етичності та безперервності роботи соціальних і культурних інституцій.

Ключові слова: кібербезпека, соціальна робота, артменеджмент, цифрова компетентність, фішинг, програми-вимагачі, дипфейки, соціальна інженерія, захист персональних даних, інформаційна безпека.

Serhii Harkavyy, Candidate of Technical Sciences, Associate Professor, Department of Military Training, B. Khmelnytskyi National University, Cherkasy, <https://orcid.org/0009-0001-3443-4486>

Oleg Bardadym Lecturer, Department of Education, Art Management, and Social Work, B. Khmelnytskyi National University, <https://orcid.org/0000-0002-2777-6568>

INFORMATION SECURITY IN SOCIAL WORK AND ART MANAGEMENT: TYPOLOGY OF THREATS, DIGITAL COMPETENCE, SOCIAL ENGINEERING, AND INSTITUTIONAL PROTECTION STRATEGIES

Abstract. The article presents an extended analysis of current information security challenges in social work and art management, two sectors undergoing rapid digital transformation and therefore exhibiting heightened vulnerability to cyberattacks. Professionals in these fields operate with sensitive personal data, digital archives, intellectual property, financial documentation, and cross-border communication, creating a complex and multilayered risk environment. The study proposes an expanded typology of cyberthreats encompassing social engineering (phishing, spear-phishing, pretexting), various categories of malicious software, network and infrastructural attacks (DDoS, MITM, zero-day exploits), as well as emerging threats driven by artificial intelligence, such as deepfake manipulation and automated credential-compromise schemes. For each threat type, the article identifies key indicators, operational mechanisms, and potential consequences, which may include data breaches, financial losses, workflow disruptions, and erosion of institutional trust within humanitarian and cultural organizations.

The study offers a comprehensive set of cyber hygiene practices tailored to practical implementation: the use of password managers, multi-factor authentication, device encryption, access auditing, monitoring activity in cloud



environments, safe interaction with public networks, systematic data backup, and anomaly detection. A four-level model of digital competence is introduced, covering basic threat awareness, operational skills, analytical capabilities, and institutional leadership in cybersecurity governance. Each level includes practical training tasks adapted to the professional contexts of social workers and art managers. The findings demonstrate that the integration of individual digital competence with organizational security policies enables the creation of a resilient, multi-layered cybersecurity system essential for maintaining reliability, ethical standards, and continuity of services across social and cultural institutions.

Keywords: cybersecurity, social work, art management, digital competence, phishing, ransomware, deepfakes, social engineering, personal data protection, information security.

Постановка проблеми. Кібербезпека стала фундаментальною передумовою професійної діяльності у всіх наукоємних секторах. У соціальній роботі фахівці оперують надзвичайно чутливими персональними даними, включаючи інформацію про вразливі групи населення, стан здоров'я, економічні умови, міграційну історію та психологічні профілі. В артменеджменті професіонали працюють з цифровими архівами, авторськими правами, міжнародними грантовими контрактами, мистецькими портфоліо та фінансовими транзакціями.

Цілісність та конфіденційність інформації є не лише технічним питанням, а етичною вимогою, яка впливає на права людини, довіру. Численні звіти підтверджують, що гуманітарні, освітні та культурні організації стали пріоритетними мішенями для атак через низький рівень захисних заходів та залежність від електронної комунікації. Ключова суперечність полягає в зростаючій цифровізації соціальних та культурних послуг на тлі недостатньої цифрової та інформаційної безпекової компетентності серед професіоналів. Соціальні працівники активно використовують хмарні сервіси, месенджери та цифрові системи управління справами, тоді як арт-менеджери покладаються на транскордонну комунікацію, платформи цифрового маркетингу, онлайн-фінансові системи та репозиторії для творчих робіт.

Аналіз останніх досліджень і публікацій. Попри критичність безпечної цифрової поведінки, жоден із секторів повністю не інтегрував кібербезпеку у свої професійні стандарти. Як зазначається в українських рамках цифрової компетентності, інформаційна та цифрова грамотність є необхідними для сучасних фахівців, зокрема викладачів природничих наук, де цифрові технології трансформують роль педагога, стимулюючи інтерес та залученість студентів [1]. Аналогічно наголошується на важливості



класифікації веб-ресурсів, верифікації інформації та розуміння інформаційних систем, що безпосередньо корелює зі стійкістю до кіберзагроз [2; 3; 4; 5].

Проблема посилюється глобальними факторами: гібридною війною, масовою дезінформацією, стрімким розвитком штучного інтелекту та зростаючою складністю стратегій кіберзлочинців. Сучасні дослідження кібербезпеки для нетехнічних професій виокремлюють кілька ключових напрямків: моніторинг кіберзагроз [6; 7], еволюція програм-вимагачів [8], аналітика витоків даних [9], освітні рамки цифрової компетентності [10; 15], загрози, генеровані штучним інтелектом, включно з імпровізацією дипфейків [11], та класифікації веб-вразливостей [12]. Українські дослідники підкреслюють діяльнісну складову формування цифрової компетентності, включаючи здатність управляти, оцінювати та створювати цифровий контент відповідально [1]. Цей підхід поширюється на оцінювання надійності інформаційних ресурсів, класифікацію освітніх платформ та дослідження інформаційних систем для інституційного управління - знання, безпосередньо застосовне до цифрової безпеки [2; 3; 4]. Водночас, небагато досліджень безпосередньо адресують виклики кібербезпеки, специфічні для соціальної роботи та арт-менеджменту, що робить актуальним інтегрування загального знання з галузево-специфічними ризиками. Цифрова компетентність визначається як сукупність знань, навичок та ставлень, що забезпечують ефективно та безпечно використання цифрових технологій [15]. Інформаційна та цифрова компетентність включає здатність отримувати доступ до інформації та управляти нею, оцінювати достовірність, інтегрувати та створювати цифрові ресурси, застосовувати цифрові інструменти для розв'язання практичних проблем, комунікувати безпечно та етично [1].

Ці принципи узгоджуються з потребами цифрової компетентності соціальних працівників та арт-менеджерів. Українська рамка наголошує на конкурентоспроможності на ринку праці, здатності оперувати сучасними технологіями та безпечній онлайн-поведінці [10]. Роль цифрової компетентності змінюється від простого технічного користування до відповідального цифрового громадянства. На основі аналізу міжнародної аналітики виокремлюються шість основних категорій загроз: фішинг та цільовий фішинг, компрометація корпоративної електронної пошти, програми-вимагачі, маніпуляції дипфейками та загрози на базі штучного інтелекту, витoki даних та скомпрометоване хмарне сховище, вразливості вебсайтів та цифрових платформ. Кожна загроза має специфічні індикатори ризику та спричинила задокументовані інциденти в гуманітарних та культурних інституціях.



Мета статті. Розробити узагальнену концептуальну рамку кібербезпеки для фахівців соціальної роботи та арт-менеджменту шляхом інтеграції сучасних міжнародних стандартів, типологій кіберзагроз і моделей цифрової компетентності, адаптованих до специфіки цих професій. Для досягнення мети визначено такі завдання: систематизувати ключові категорії кіберзагроз, релевантні для соціальної роботи та артменеджменту; розробити практичний інструментарій ідентифікації кіберризиків через таблиці індикаторів загроз; структурувати правила цифрової гігієни у вигляді узагальнених таблиць із прикладами застосування; створити чотирирівневу модель розвитку цифрової компетентності з кібербезпеки; визначити інституційні механізми захисту та протоколи реагування на кіберінциденти; запропонувати практичні навчальні завдання та симуляційні вправи з формування компетентностей кібербезпеки.

Виклад основного матеріалу. Розглянемо типи інформаційних небезпек **1. Соціальна інженерія** є сукупністю методів психологічного маніпулювання, що використовуються зловмисниками для отримання доступу до даних та систем. **Фішинг** - масова розсилка шахрайських електронних листів, які намагаються виманити облікові дані або фінансову інформацію. Основними ознаками фішингу є несподівані повідомлення нібито від офіційних установ, загальні звернення («Шановний користувач»), вимога термінових дій, помилки у доменах, граматичні помилки та підозрілі вкладення.

Наслідками фішингових атак стають компрометація облікових записів, втрата доступу до організаційних систем, фінансові збитки й розкриття конфіденційних даних. **Цільовий фішинг** (spear phishing) - персоналізована атака, що імітує комунікацію конкретних осіб (керівників, донорів, партнерів), використовуючи реальні контексти та схожі домени. Його ознаками є високий ступінь персоналізації повідомлень, посилання на реальні події, майже ідентичні доменні імена та термінові запити на переказ коштів чи передачу інформації.

Наслідки включають втрату значних фінансових ресурсів, витік стратегічної інформації, компрометацію партнерських відносин і репутаційні ризики.

Претекстинг - маніпулятивна техніка створення вигаданого сценарію (наприклад, «техпідтримка», «аудит»), що спонукає жертву розкрити конфіденційні дані. Його ознаками є несподівані дзвінки, запити на паролі для «верифікації», вимоги надати доступ до внутрішніх документів та створення штучного відчуття кризи. Наслідками стають повний несанкціонований доступ до систем, маніпуляції базами даних, крадіжка інтелектуальної власності та підрив довіри між співробітниками.



2. Шкідливе програмне забезпечення становить другу групу ризиків. Трояни, черв'яки, шпигунське ПЗ та кейлоггери - це програми, що маскуються під легітимні застосунки, поширюються через мережі, відстежують активність та фіксують натискання клавіш. Їх ознаками є уповільнення роботи пристрою, збільшення трафіку, спливаючі вікна, зміна налаштувань браузера, вимкнення антивірусу, поява невідомих програм та зникнення файлів. Наслідки включають витік персональних і фінансових даних, викрадення інтелектуальної власності, втрату контролю над обліковими записами та довготривале перебування зловмисників у системі. **Криптоджекінг** - приховане використання обчислювальних ресурсів користувача для майнінгу криптовалюти. Його ознаками є надмірне навантаження процесора, перегрів пристрою, швидке розрядження батареї та зниження продуктивності. Наслідками виступають неможливість виконання ресурсомістких завдань, прискорене зношення обладнання та виявлення глибших системних вразливостей. Атаки на паролі - це брутфорс, словникові атаки та використання викрадених паролів для отримання доступу до систем. Їх ознаки включають численні невдалі спроби входу, блокування акаунтів, входи з незвичних локацій та неініційовані запити на скидання пароля. **Наслідки** - несанкціонований доступ до критичних систем, компрометація фінансових операцій, витік конфіденційної інформації та модифікація або видалення даних.

3. Мережеві, інфраструктурні та апаратні атаки становлять окремий вектор загроз. DDoS-атаки - перевантаження вебресурсів надмірною кількістю запитів з метою зробити їх недоступними. Ознаки включають повільне завантаження сторінок, помилки таймауту, раптову недоступність та аномальний трафік. Наслідками є зупинка онлайн-сервісів, фінансові й репутаційні втрати та потреба у додаткових витратах на кіберзахист. Атаки «людина посередині» (MITM) - перехоплення трафіку через підроблені Wi-Fi точки. Ознаки: попередження про сертифікати, незвичне перепідключення до мережі, входи з нових пристроїв та підозрілі точки доступу. Наслідки - перехоплення паролів, витік конфіденційної комунікації, доступ до сесійних токенів і компрометація транзакцій. **SQL-ін'єкції** - маніпулювання запитами до баз даних для доступу або зміни інформації. Ознаки: помилки бази, необґрунтований доступ до адмінпанелі, несанкціоновані зміни даних, підозрілі записи в логах. Наслідки: масові витоки персональних і фінансових даних, модифікація записів та створення фіктивних адмін-акаунтів. **Експлойти нульового дня** - використання невідомих розробникам вразливостей. Їх ознаками є обходи захисних механізмів, компрометація без видимої точки входу та відсутність реакції антивірусу. Наслідки включають повну компрометацію системи, масштабне



поширення атаки та необхідність екстрених оновлень. Апаратні імплантати - шкідливі пристрої, що маскуються під звичайні аксесуари. Ознаки: знайдені підозрілі USB, «подарункові» флешки, автоматичне виконання команд після підключення. Наслідки: миттєве викрадення файлів, встановлення бекдорів, компрометація мережі та обходи програмного захисту.

4.Окрему категорію становлять загрози, згенеровані штучним інтелектом. Дипфейк аудіо та відео – підроблені мультимедійні матеріали, що імітують голос чи зовнішність керівників для отримання доступу до ресурсів або примушення до термінових дій. Ознаками є неприродні рухи губ, нехарактерні інтонації, невідповідні фонові шуми, дивні тіні та низька якість відео. **Наслідки:** фінансові втрати, хибні управлінські рішення, репутаційні скандали, підрив довіри в команді, юридичні наслідки та психологічний стрес співробітників [11; 18]. На основі вище згаданих кібератак слід сформулювати правила користування Інтернет мережею

1. Сильні унікальні паролі (8+ символів, змішані символи) слід використовувати через менеджери паролів (Bitwarden, 1Password, KeePass), наприклад, для системи обліку клієнтів / для адмінпанелі сайту галереї. Недотримання цього правила сприяє легкому злому акаунтів і витоку конфіденційних даних. Ніколи не варто використовувати один і той самий пароль для різних сервісів, адже унікальні паролі для електронної пошти, CRM та хмарного сховища / для сайту галереї, онлайн-банкінгу, соцмереж запобігають загрозі, коли злом одного облікового запису ставить під загрозу всі сервіси.

2. Увімкнення багатфакторної автентифікації (MFA) із застосуванням Google Authenticator, Microsoft Authenticator або Authy дозволяє забезпечити додатковий рівень безпеки при доступі до бази даних клієнтів / до системи управління грантами та адміністрування сайту. Несанкціонований доступ до систем навіть при знанні пароля стає неможливим. Регулярне оновлення програмного забезпечення через автоматичне оновлення ОС, антивірусу та додатків забезпечує безпеку CRM-системи / системи бронювання квитків і вебсайту галереї, запобігаючи використанню відомих вразливостей зловмисниками та атакам ransomware.

3. Використання антивірусного та антишпигунського програмного забезпечення з регулярним скануванням захищає ПК соціальних працівників / ПК та сервери галереї від вірусів, троянів та шпигунських програм, які можуть вкрасти дані або пошкодити систему. Обережне використання електронної пошти та посилань, включаючи перевірку відправника та застосування фільтрів спаму, допомагає уникати відкриття підозрілих листів / переходів за сумнівними посиланнями, що зменшує ризик фішингу та зараження шкідливим ПЗ.



4. Безпечне використання хмарних сервісів із шифруванням файлів, обмеженням доступу та резервним копіюванням дозволяє захистити персональні дані клієнтів / зберігати фото та матеріали виставок, зменшуючи ймовірність витоку даних або доступу сторонніх. Обмеження доступу та прав користувачів через надання доступу лише за необхідністю та аудит прав забезпечує контроль доступу соціальних працівників лише до своїх клієнтів / працівників галереї до своїх систем, запобігаючи несанкціонованому доступу та внутрішнім загрозам.

5. Навчання та підвищення кіберобізнаності через регулярні тренінги та симуляції фішингових атак підвищує безпеку персоналу соціальних працівників / співробітників галереї, зменшуючи ризики, пов'язані з людським фактором. Безпечне використання публічних мереж із застосуванням VPN та униканням доступу до критичних систем у відкритих Wi-Fi забезпечує захист при підключенні до CRM / вебсайту галереї від перехоплення трафіку та крадіжки логінів і паролів.

6. Регулярне резервне копіювання даних за допомогою автоматичного створення бекапів захищає інформацію клієнтів / копії медіафайлів виставок від втрат через збій, атаки ransomware або випадкове видалення. Шифрування пристроїв та даних (BitLocker, FileVault, шифрування мобільних пристроїв) забезпечує захист ноутбуків соціальних працівників / планшетів та ПК галереї, зменшуючи ризик витоку даних у разі викрадення або втрати пристрою.

7. Контроль соціальних мереж через налаштування приватності, обмеження публікацій та двофакторну автентифікацію дозволяє закривати соціальні профілі / контролювати публікації галереї, мінімізуючи публікацію конфіденційної інформації та репутаційні втрати. Безпечне використання USB та зовнішніх носіїв через сканування перед підключенням та шифрування захищає документи / медіафайли виставок від шкідливого ПЗ та витоку даних.

8. Моніторинг підозрілої активності за допомогою систем моніторингу та сповіщення про аномалії дозволяє контролювати доступ до бази клієнтів / адмінпанелі сайту галереї, зменшуючи ризик непомічених несанкціонованих дій. Захист мобільних додатків із застосуванням антивірусу на смартфоні та блокування сторонніх додатків забезпечує безпечне використання офіційних мобільних CRM-додатків / управління продажами та квитками галереї, запобігаючи зараженню мобільних пристроїв, крадіжці даних та втручанню в роботу систем.

Розвиток цифрової компетентності для фахівців соціальної роботи та артменеджменту здійснюється через чотири послідовні рівні, що дозволяє поступово нарощувати навички від базового усвідомлення до інститу-



ційного лідерства, аналогічно до рамки компетентностей для громадянина, яка пропонує систему рівнів освоєння: від базового ознайомлення до повної самостійності та стратегічного впливу.

На рівні базового усвідомлення фокус спрямований на розпізнавання фішингу, увімкнення багатофакторної автентифікації та використання менеджера паролів, а також розуміння базових загроз. У соціальній роботі це реалізується через аналіз фішингових листів, виявлення ключових індикаторів (невідповідність домену, граматичні помилки, терміновість, підозрілі вкладення), створення складних паролів для систем обліку клієнтів та увімкнення MFA для робочої пошти. В артменеджменті практичні завдання включають налаштування менеджера паролів для облікових записів галереї, увімкнення двофакторної автентифікації для email та фінансових систем, перевірку налаштувань приватності хмарних сховищ та аналіз потенційно фішингових листів із пропозиціями грантів. Додаткове завдання: створити тестовий фішинговий лист і оцінити його як справжній або шахрайський; очікуваний результат: правильна ідентифікація всіх ознак фішингу.

На рівні операційної компетентності учасники опановують аудит хмарного сховища, оцінку достовірності ресурсів, ідентифікацію вразливостей та застосування принципів кібергігієни. Соціальні працівники виконують симуляції підозрілих входів у системи, відключають мережу, змінюють паролі, повідомляють IT-відділ та керівника, здійснюють самоаудит облікових записів і перевірку встановленого програмного забезпечення. В артменеджменті операційні завдання охоплюють аудит публічних посилань на хмарні сховища, обмеження доступу для колишніх співробітників, перевірку шифрування фінансових документів та налаштування безпеки соціальних мереж. Додаткове завдання: провести аудит власного Google Drive і видалити непотрібні публічні посилання; очікуваний результат: усі документи доступні лише для авторизованих користувачів.

Рівень аналітичної компетентності включає розробку моделей загроз, аналіз артефактів дипфейків, реагування на складні інциденти та оцінку ризиків проєктів. Соціальні працівники створюють карту загроз робочого дня, визначають ймовірність і наслідки ризиків на різних етапах взаємодії з клієнтами, аналізують витoki даних та розслідують компрометації. В артменеджменті практичні завдання передбачають детекцію дипфейків у відео та аудіо, розробку протоколів верифікації запитів на фінансові операції та оцінку ризиків міжнародних виставок із формуванням матриці ризиків і пріоритизацією загроз. Додаткове завдання: провести аналіз короткого відео на наявність ознак дипфейку; очікуваний



результат: точне визначення підроблених елементів та запропоновані заходи для верифікації[19; 20]..

На рівні інституційного лідерства учасники опановують написання внутрішніх регуляцій, навчання колег, впровадження GDPR-політик, управління інцидентами та стратегічне планування безпеки. Соціальні працівники розробляють політику кібербезпеки для організацій, що працюють із вразливими групами, створюють річні програми навчання персоналу та симуляції фішингу. В артменеджменті завдання включають навчання всіх ролей у культурному центрі та створення протоколів інцидент-менеджменту для сценаріїв компрометації сайтів, витоку контрактів або атак програм-вимагачів із призначенням ролей, ланцюгами комунікації, юридичними процедурами та PR-стратегіями. Додаткове завдання: розробити короткий внутрішній регламент реагування на кіберінциденти; очікуваний результат: документ, який чітко визначає дії персоналу при критичних інцидентах і забезпечує швидке реагування [16].

Додаткові активності включають використання детекторів дипфейків, симулятори фішингу та самоаудит цифрової гігієни, що охоплюють перевірку паролів, аналіз пристроїв, сканування хмарних сховищ і оцінку загального рівня цифрової безпеки. Карта загроз для соціальної справи або мистецького проєкту дозволяє системно візуалізувати потенційні кіберризики на різних етапах роботи, від первинного контакту з клієнтом чи партнером до архівування матеріалів після завершення проєкту, сприяючи інтеграції безпечних практик у повсякденні робочі процеси[17; 20].

Висновки. Інформаційна безпека у соціальній роботі та артменеджменті є не просто технічною функцією, а основною етичною відповідальністю професіоналів цих галузей. Інтеграція рамок цифрової компетентності, типологій загроз та практичних вправ дозволяє інституціям значно знизити вразливість перед кіберзагрозами. Багаторівнева модель компетентності підтримує професійний розвиток фахівців, тоді як організаційні політики забезпечують системний захист. Розширена типологія кібератак, адаптована до специфіки обох секторів, демонструє різноманітність та складність сучасних загроз, від соціальної інженерії до атак на бази штучного інтелекту.

Систематизація індикаторів кіберризиків у табличному форматі з конкретними прикладами для соціальної роботи та арт-менеджменту забезпечує практичний інструментарій для швидкої ідентифікації потенційних загроз у повсякденній діяльності. Правила кібергігієни, представлені у структурованому вигляді з технічною реалізацією та галузевими прикладами, дозволяють фахівцям негайно впроваджувати захисні практики без потреби у глибоких технічних знаннях.



Чотирирівнева модель розвитку цифрової компетентності з конкретними практичними завданнями для кожного рівня створює чіткий освітній трек від базового усвідомлення до інституційного лідерства, дозволяючи організаціям планувати довгострокові програми навчання персоналу. Інтеграція інституційних механізмів захисту з індивідуальним розвитком компетентностей забезпечує багаторівневий підхід до кібербезпеки, де технічні рішення підтримуються людським фактором та організаційною культурою.

Майбутні дослідження мають зосередитися на ризиках, пов'язаних із штучним інтелектом, порівняльних міжнародних практиках кібербезпеки в гуманітарному та культурному секторах, а також психологічних факторах, що впливають на дотримання правил кібербезпеки серед фахівців допоміжних професій. Особливу увагу варто приділити вивченню бар'єрів впровадження захисних механізмів у ресурсообмежених організаціях та розробці економічно доступних рішень для малих неурядових організацій та культурних ініціатив. Перспективним напрямком є також дослідження ефективності різних форматів навчання кібербезпеки для нетехнічних професіоналів та розробка галузево-специфічних сертифікаційних програм

Література

1. Шпак, В., & Бардадим, О. (2022). Формування інформаційно-цифрової компетентності викладачів природничих наук: діяльнісна складова. *Вища освіта України*, 1(90), 153–170. <https://doi.org/10.38014/osvita.2022.90.14>
2. Бардадим, О. В. (2022). Класифікація освітніх веб-ресурсів. *Наукові записки. Серія: Педагогічні науки*, 207, 89–99. <https://doi.org/10.36550/2415-7988-2022-1-207-89-99>
3. Бардадим, О. (2024). Сервіси для перевірки фактів. *Zenodo*. <https://doi.org/10.5281/zenodo.14832217>
4. Бардадим, О. (2025). Види інформаційних систем управління закладом освіти. Матеріали IV Міжнародної конференції «Цифрові інновації та соціальні трансформації в освіті». *Zenodo*. <https://doi.org/10.5281/zenodo.14840251>
5. Бардадим, О. (2025). Статистика соціальних явищ. *Zenodo*. <https://doi.org/10.5281/zenodo.14837856>
6. CERT-UA. (2023). Звіти про кіберзагрози. <https://cert.gov.ua>
7. ENISA. (2023). *Threat Landscape Report 2023*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2023>
8. Sophos. (2023). *State of Ransomware Report*. <https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2023-wp.pdf>
9. Verizon. (2023). *Data Breach Investigations Report*. <https://www.verizon.com/business/resources/reports/dbir/>
10. Міністерство освіти і науки України. (2021). *Рамка цифрової компетентності для України*. <https://mon.gov.ua/ua/npa/ramka-cifrovoi-kompetentnosti>
11. Europol. (2024). *Facing Reality? Law Enforcement and Deepfakes*. <https://www.europol.europa.eu/publications-documents/facing-reality-law-enforcement-and-deepfakes>



12. OWASP Foundation. (2023). OWASP Top 10 Vulnerabilities. <https://owasp.org/Top10/>
13. NIST. (2020). Cybersecurity Framework. National Institute of Standards and Technology. <https://www.nist.gov/cyberframework>
14. European Commission. (2021). General Data Protection Regulation (GDPR). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
15. European Commission. (2021). DigComp 2.2: The European Digital Competence Framework. https://joint-research-centre.ec.europa.eu/digcomp/digcomp-2-2-2021_en
16. Microsoft Security. (2023). Phishing Trends Analysis. <https://www.microsoft.com/security/blog/phishing-trends-2023>
17. IBM Security. (2023). Cost of a Data Breach Report. <https://www.ibm.com/reports/data-breach-2023>
18. Google Security. (2023). Safe Browsing Transparency Report. <https://safebrowsing.google.com/transparency-report/>
19. Cisco. (2022). Cybersecurity Threat Trends. <https://www.cisco.com/c/en/us/products/security/security-reports.html>
20. McAfee Labs. (2023). Cyberthreat Report. <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2023.pdf>

Reference

1. Shpak, V., & Bardadym, O. (2022). Formuvannia informatsiyno-tsyfrovoyi kompetentnosti vykhovateliv pryrodnychkh nauk: diialnisna skladova [Formation of information-digital competence of natural science teachers: activity component]. Kyiv: Vyscha osvita Ukrainy [in Ukrainian]. <https://doi.org/10.38014/osvita.2022.90.14>
2. Bardadym, O. V. (2022). Klasyfikatsiia osvitnikh web-resursiv [Classification of educational web resources]. Kyiv: Naukovi zapysky. Serii: Pedahohichni nauky [in Ukrainian]. <https://doi.org/10.36550/2415-7988-2022-1-207-89-99>
3. Bardadym, O. (2024). Servisy dlia perevirky faktiv [Fact-checking services]. Zenodo [in Ukrainian]. <https://doi.org/10.5281/zenodo.14832217>
4. Bardadym, O. (2025). Vydy informatsiynykh system upravlinnia zakladom osvity [Types of information management systems in educational institutions]. Materyaly IV Mizhnarodnoi konferentsii "Tsifrovi innovatsii ta sotsialni transformatsii v osviti" [in Ukrainian]. <https://doi.org/10.5281/zenodo.14840251>
5. Bardadym, O. (2025). Statystyka sotsialnykh iavysch [Statistics of social phenomena]. Zenodo [in Ukrainian]. <https://doi.org/10.5281/zenodo.14837856>
6. CERT-UA. (2023). Zvity pro kiberzahrozy [Reports on cyber threats]. Kyiv [in Ukrainian]. <https://cert.gov.ua>
7. ENISA. (2023). Threat Landscape Report 2023. European Union Agency for Cybersecurity [in English]. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2023>
8. Sophos. (2023). State of Ransomware Report [in English]. <https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2023-wp.pdf>
9. Verizon. (2023). Data Breach Investigations Report [in English]. <https://www.verizon.com/business/resources/reports/dbir/>
10. Ministerstvo osvity i nauky Ukrainy. (2021). Ramka tsyfrovoyi kompetentnosti dlia Ukrainy [Digital competence framework for Ukraine]. Kyiv [in Ukrainian]. <https://mon.gov.ua/ua/npa/ramka-cifrovoi-kompetentnosti>



11. Europol. (2024). Facing Reality? Law Enforcement and Deepfakes [in English]. <https://www.europol.europa.eu/publications-documents/facing-reality-law-enforcement-and-deepfakes>
12. OWASP Foundation. (2023). OWASP Top 10 Vulnerabilities [in English]. <https://owasp.org/Top10/>
13. NIST. (2020). Cybersecurity Framework. National Institute of Standards and Technology [in English]. <https://www.nist.gov/cyberframework>
14. European Commission. (2021). General Data Protection Regulation (GDPR) [in English]. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
15. European Commission. (2021). DigComp 2.2: The European Digital Competence Framework [in English]. https://joint-research-centre.ec.europa.eu/digcomp/digcomp-2-2-2021_en
16. Microsoft Security. (2023). Phishing Trends Analysis [in English]. <https://www.microsoft.com/security/blog/phishing-trends-2023>
17. IBM Security. (2023). Cost of a Data Breach Report [in English]. <https://www.ibm.com/reports/data-breach-2023>
18. Google Security. (2023). Safe Browsing Transparency Report [in English]. <https://safebrowsing.google.com/transparency-report/>
19. Cisco. (2022). Cybersecurity Threat Trends [in English]. <https://www.cisco.com/c/en/us/products/security/security-reports.html>
20. McAfee Labs. (2023). Cyberthreat Report [in English]. <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2023.pdf>

Дата першого надходження статті до видання: 14.02.2026

Дата прийняття статті до друку після рецензування: 28.02.2026

Журнал

«Вісник науки та освіти»

№ 2(44) 2026

Формат 60x90/8. Папір офсетний.
Гарнітура Times New Roman.
Ум. друк. арк. 8,2.

Видавець:
Всеукраїнська асамблея докторів наук з державного управління
Свідоцтво серія ДК №4957 від 18.08.2015 р., Андріївський узвіз, буд.11, оф 68, м. Київ, 04070.