УДК: 37.091.12-051:004.9
DOI: https://doi.org/10.54662/veresen.2.2025.03

Максим Запорожченко,
ORCID iD 0000-0001-9256-2091
завідувач центру
цифрової освіти та медіакультури
Миколаївський обласний інститут
післядипломної педагогічної освіти
вул. Адміральська, 4-а, 54001, м. Миколаїв, Україна
m.zaporozhchenko@moippo.mk.ua

Ганна Шевченко,
ORCID iD 0000-0001-6723-6059
методист центру
цифрової освіти та медіакультури
Миколаївський обласний інститут
післядипломної педагогічної освіти
вул. Адміральська, 4-а, 54001, м. Миколаїв, Україна
ganna.shevchenko@moippo.mk.ua

ЦИФРОВА БЕЗПЕКА ЯК СКЛАДНИК ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ ПЕДАГОГІЧНИХ ПРАЦІВНИКІВ

У методичній статті досліджено проблему цифрової безпеки педагогічних працівників в умовах інформаційного суспільства. Розглянуто найпоширеніші типи кіберзагроз та їхній можливий уплив на професійну діяльність освітян, а також надано рекомендації щодо протидії кожній. Проаналізовано теоретичні основи цифрової компетентності. Запропоновано рішення щодо використання вільного програмного забезпечення для організації освітнього процесу як альтернативу неліцензованим версіям поширених програм та операційних систем. У роботі розвинено ідею взаємозалежності цифрової грамотності та інформаційної безпеки педагогів. Виокремлено специфічні загрози в умовах війни. Уперше представлено систематизований перелік безпечних програмних рішень для освітян з урахуванням українського контексту.

Ключові слова: *інформаційне суспільство; кібератаки; кіберзагрози; освіта; педагогічні працівники; цифрова безпека; цифрова компетентність.*

Постановка проблеми. Розвиток інформаційного суспільства у XXI столітті характеризується стрімкою диджиталізацією всіх сфер людської діяльності, зокрема освіти, що призвело до радикальних змін у способах організації навчального процесу. За даними ЮНЕСКО, у 2020 році близько 1,6 мільярда учнів і педагогів у світі зіткнулися з необхідністю переходу на онлайн-платформи через пандемію COVID-19, що підкреслило критичну важливість цифрової безпеки в умовах глобальних викликів (Education during COVID-19 and beyond, 2020).

В Україні ці процеси набули особливої актуальності з початком повномасштабної війни у 2022 році, коли дистанційне навчання стало не лише альтернативою, а й основним способом забезпечення безперервності освіти. Цифрова безпека як складник інформаційної стала невід'ємною частиною професійної діяльності пе-

дагогів, що дедалі частіше стають мішенями кібератак через недостатню обізнаність і вразливість інфраструктури. Ситуація ускладнюється тим, що освіта, за своєю природою, є відкритою системою, яка передбачає обмін інформацією між учителями та школярами, це так само робить її привабливою для зловмисників. Перехід до цифрових технологій без належного рівня цифрової грамотності педагогів створює нові ризики, які потребують негайного вирішення. У цьому контексті цифрова безпека виходить за рамки суто технічного питання, охоплюючи соціальні, психологічні та організаційні аспекти, що потребують комплексного підходу – від теоретичного осмислення до розроблення практичних рішень. Актуальність проблеми зумовлена не лише зростанням кіберзагроз, а й необхідністю адаптації системи освіти до умов інформаційного суспільства, де безпека даних є запорукою ефективного функціонування.

Незважаючи на визнання цифрових навичок як ключової компетентності сучасного педагога, на практиці спостерігаємо суперечність між вимогами до цифрової грамотності та реальним рівнем її сформованості в освітян. Також помітний розрив між технічним забезпеченням закладів освіти та здатністю педагогів ефективно використовувати наявні цифрові ресурси. Крім того, систему підвищення кваліфікації часто зосереджують на загальних цифрових інструментах, залишаючи поза увагою аспекти інформаційної безпеки. Це породжує ситуацію, коли педагоги залишаються вразливими до кіберзагроз, не маючи необхідного обсягу знань для адекватного реагування. Отже, виникає потреба в комплексному підході до формування цифрової компетентності, що охоплював би не лише технічні навички, а й безпековий складник з урахуванням сучасних викликів, спричинених війною та процесом цифрової трансформації освіти.

Метою статті є теоретичне обґрунтування та аналіз набуття компетентності з цифрової безпеки освітян в інформаційному суспільстві.

Убачаємо такі ключові **завдання**:

1) визначити теоретичні основи цифрової компетентності освітян як передумови безпечної та результативної педагогічної діяльності в умовах диджиталізації;
2) проаналізувати головні кіберзагрози для педагогів на основі сучасних досліджень;
3) запропонувати рекомендації для протидії цифровим небезпекам та інші варіанти рішення щодо програмного забезпечення закладів освіти.

Аналіз наукових досліджень і публікацій. Проблема цифрової безпеки в освіті є предметом уваги як міжнародних, так і українських дослідників. Звіт Microsoft показує, що освітній сектор є одним із найвразливіших: 12 % кібератак Російської Федерації проти України спрямовані на заклади освіти через низький рівень безпеки, що робить цю сферу сприйнятливою для атак (Microsoft, 2022, с. 42).

Результати аналітичного розслідування Verizon (2024) свідчать про те, що в 2024 році сталося 1 780 кіберінцидентів в сфері освітніх послуг, із яких 1537 призвели до витоку даних, 50 % атак були спрямовані на викрадення облікових даних студентів та викладачів, а 68 % атак стали можливими через дії співробітників (неуважність, помилки, недотримання правил безпеки) (Verizon, 2024, с. 61). Міжнародний досвід, описаний у звіті ENISA (2024), свідчить, що країни, які активно впроваджують програми кіберосвіти, демонструють більшу стійкість до кібератак, ніж ті, де таких програм бракує (ENISA, 2024, с. 10). Виходячи з цього, цифрова трансформація освіти потребує не лише технічних рішень, а й системного підходу до навчання педагогів, що передбачає кібербезпеку як обов'язковий складник.

Із розвитком технологій та розширенням доступу до різноманітних джерел інформації освітня спільнота почала усвідомлювати необхідність захисту інформаційних ресурсів та формування відповідних навичок у педагогів та учнів.

Тематику цифрової безпеки освітян розглянуто в розвідках Ф. Каени, К. Реде-

кер (Caena F., Redecker Ch., 2019), трансформаційних диджитал-процесів у вищій освіті – у працях Меліси Бонд, Вікторії Марін, Каріни Дольх (Bond M., Marin V., Dolch C., 2019), Х. Янссен, С. Стоянова (Janssen J., Stoyanov S., 2013), дослідження цифрової компетентності українських учителів представлено у працях О. Х. Кузьмінської, М. В. Мазорчук, Н. В. Морзе (Кузьмінська О. Х., 2019), умови формування цифрової компетентності вчителя в післядипломній освіті аналізували І. П. Воротникова (Воротникова І. П., 2019), І. В. Іванюк, О. В. Овчарук (Іванюк І. В., Овчарук О. В., 2021).

Важливим у контексті розвитку цифрових компетентностей в освіті вважаємо дослідження М. Прокоф'євої та Л. Султанової, які у своїх роботах пропонують дотримуватися концепції «fake-free-освіти», тобто сучасної цифрової освіти, яка базується на принципах визнання знань найвищою цінністю суспільства, доброчесності та критичного мислення (Прокоф'єва М. О., Султанова Л. Ю., 2022, с. 10).

Питання кібербезпеки в цифровому навчальному середовищі висвітлено в наукових статтях В. Бикова та О. Бурова, які зокрема описують найактивніші приховані загрози для дітей, що походять з комп'ютерної мережі:

- вірусні атаки;
- кіберзлочинність (спамерство, кардінг, фішинг, ботнети тощо);
- загрози від мережевого серфінгу (кібербулінг, «дорослий» контент, незаконний вміст, насильство в режимі онлайн, розголошення приватної інформації, платні послуги тощо) (Биков В. Ю., Буров О. Ю., 2019, с. 319). Переконані, що розуміння того, з якими загрозами стикаються сучасні діти в мережевому середовищі, дасть змогу краще сформувати заходи для протидії ним в освітній системі в цілому.

Виходячи з аналізу наявних звітів і досліджень, уважаємо, що питання цифрової безпеки є пріоритетним компонентом трансформації освіти. Недостатня обізнаність педагогів у сфері кібербезпеки, а також високий рівень вразливості закладів освіти до хакерських атак, що підтверджено міжнародними аналітичними даними, потребують системного підходу до підготовки педагогів, відповідно − розвитку належних компетентностей, критичного мислення та формування культури відповідального послуговування цифровими технологіями.

Виклад основного матеріалу. Відповідно до Концептуально-референтної рамки цифрової компетентності педагогічних і науково-педагогічних працівників від Міністерства цифрової трансформації України (2021), означену здатність належить визначати як динамічну комбінацію знань, умінь, навичок, способів мислення, поглядів, цінностей, інших особистих якостей у сфері цифрових технологій, що засвідчує успішну соціалізацію особи, професійну та/або навчальну діяльність із використанням таких технологій (там само, 2021, с. 13). Цифрова компетентність педагогічних працівників є основоположним складником їхньої професійної реалізації та успішної інтеграції в сучасне суспільство.

Авторський колектив у складі Н. В. Морзе, О. В. Базелюка, І. П. Воротникової, Н. П. Дементієвської, О. Г. Захар та ін. в «Описі цифрової компетентності педагогічного працівника» зазначили, що ця навичка має охоплювати широкий спектр складників, зокрема медіаграмотність, уміння аналізувати та критично оцінювати інформаційні дані, дотримання безпеки в цифровому середовищі, співпрацю в інтернеті, а також знання про сучасні технології та пристрої (Опис цифрової компетентності педагогічного працівника, 2019, с. 3). Крім того, важливою є здатність учителів та викладачів використовувати відкриті ресурси та технології для професійного розвитку, навчати учнів ефективного використання таких інструментів під час здобуття освіти та в повсякденному житті, виконувати різноманітні завдання за допомогою технологій, оцінювати результати освітньої діяльності з використанням інноваційних методів, а також розуміти основи кодування, штучного інтелекту, віртуальної та до-

повненої реальності.

Дванадцять галузей цифрової компетентності визначили Х. Янссен, С. Стоянов та ін., демонструючи, що цифрова грамотність – це не статична застосовна в конкретних контекстах для різних цілей та сфер навичка, а система компетенцій, що розвивається (Janssen J., Stoyanov S., 2013, с. 473–478).

Щоб сформувати відповідні компетентності, педагог має бути залучений до безперервного професійного розвитку, мати доступ до сучасних технологій та можливість застосовувати їх у різноманітних освітніх форматах.

Онлайн-опитування вчителів щодо їхньої цифрової компетентності в умовах організації дистанційного навчання від працівників Інституту цифровізації освіти НАПН України (2022) свідчить про те, що загальна динаміка з підвищення її рівня є позитивною, але не досить інтенсивною. Це пов'язано з певними обмеженнями: швидкий перехід на дистанційні форми навчання та недостатня підготовленість системи освіти до відповідних трансформацій (Іванюк І. В., Овчарук О. В., 2022, с. 104). Розвиток цифрової компетентності педагогів має ґрунтуватися не лише на визначенні стандартів, а й на активному залученні вчителів до процесу самооцінювання, рефлексії та професійного зростання, що дає змогу перетворювати використання цифрових технологій у навчанні відповідно до викликів XXI століття.

Це дає підстави авторам розглядати цифрову компетентність педагогів як багатовимірне поняття, що охоплює знання, навички, ставлення, цінності та здатність критично мислити й діяти в інформаційному середовищі. Названа компетентність є теоретично обґрунтованою передумовою для безпечної, ефективної та адаптивної педагогічної діяльності в умовах цифровізації освіти.

Диджитал-трансформація освіти, прискорена такими глобальними викликами, як пандемія COVID-19, та локальними факторами, зокрема війною в Україні, створила безпрецедентні умови для зростання кіберзагроз. Перехід до дистанційного навчання збільшив залежність від цифрових платформ, одночасно підвищивши їхню привабливість для зловмисників. Звіт Microsoft підкреслює, що освіта є однією з найбільш атакованих сфер у світі (Microsoft, 2022, с. 14). Ці загрози варіюються від соціальних атак, таких, як фішинг, до технологічних, як DDoS, і мають прямий уплив на діяльність педагогів. Аналіз цих загроз необхідний для розуміння їхньої природи, масштабів і наслідків, а також для розроблення ефективних стратегій протидії.

У 2024 році багато українських користувачів Telegram почали скаржитись на втрату доступу до свого облікового запису, що сталося після участі в «опитуванні» на прохання знайомого контакта (https://bit.ly/41CVj3X). Листи подібного характеру (рис. 1) із закликом проголосувати за «близьку родичку» почали надходити й освітянам, і через свою необачність частина колег теж ставали жертвами шахраїв.

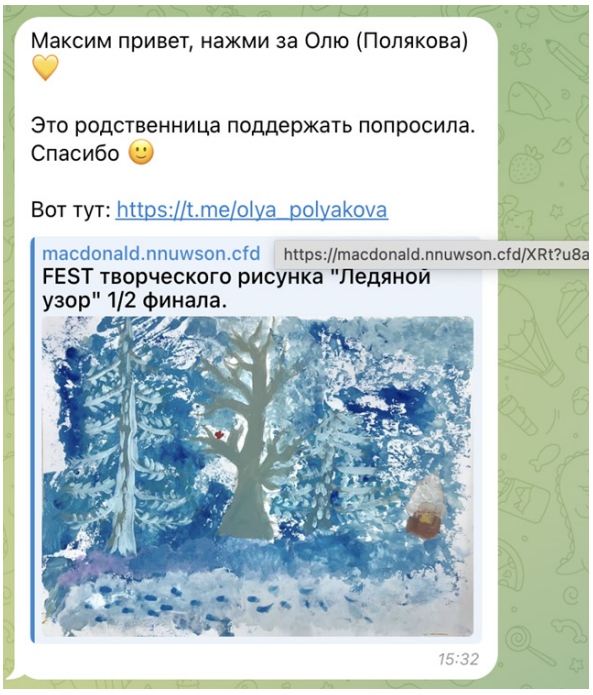

Рис. 1. Скриншот шахрайського листа із проханням проголосувати.

Джерело: авторський варіант

Ця шахрайська схема має назву «фішинг» (від англійського «риболовля») – виманювання в неуважних чи довірливих користувачів їхніх персональних даних. Класична фішингова схема передбачає наявність «наживки» – у цьому випадку прохання «підтримати голосом» та покликання, за яким треба перейти. Після того, як користувач «клюнув» на «наживку», його просять увести свій номер телефону (логін), пароль і підтвердити свій вхід (рис. 2).

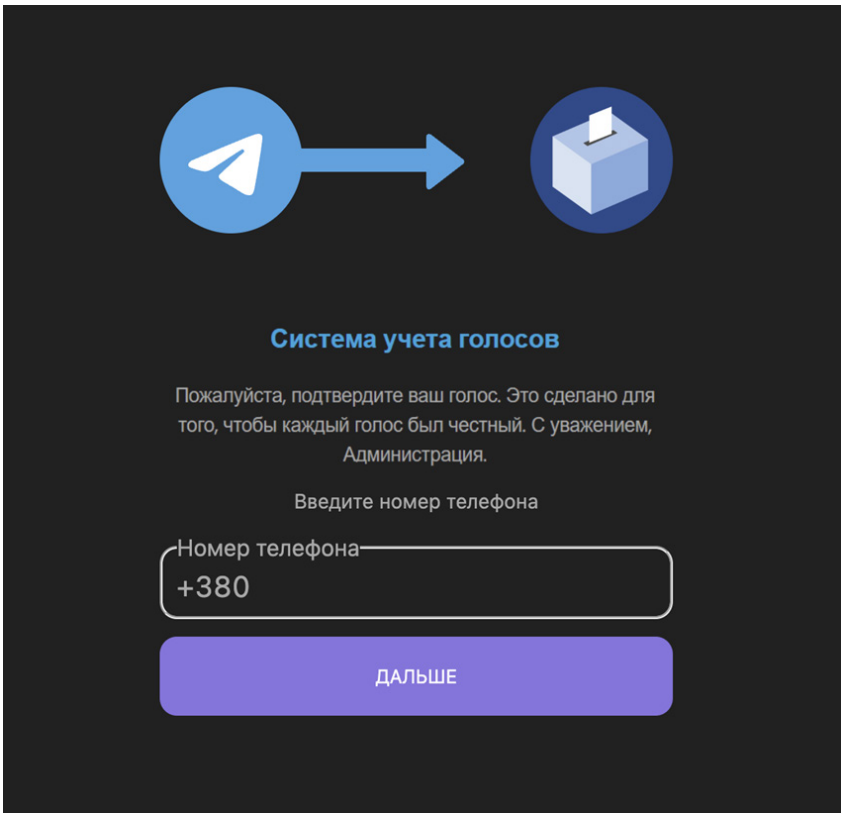

Рис. 2. Скриншот шахрайського ресурсу з виманювання персональних даних.

Джерело: авторський варіант

Результатом таких необачних дій є набуття доступу шахраїв до облікового запису, через який вони поширюватимуть такі листи далі, читатимуть приватне листування, завантажуватимуть фото, відео, документи для подальшого шантажування чи інших протиправних дій.

Фішинг є провідною загрозою через його доступність і високу результативність. Verizon (2024) зазначає, що сучасна фішингова атака розгортається менше ніж за 60 секунд – користувачі вводять свої дані в шахрайські форми вже через 21 секунду після відкриття електронного листа (Verizon, 2024, с. 9). Такі листи часто маскують під офіційні повідомлення від адміністрацій чи державних органів, що ускладнює їхню ідентифікацію без підготовки.

Шахраї використовують різні тактики, наприклад, повідомлення про виграш, термінові вимоги оновити дані або навіть погрози блокування акаунта. Щоб не потрапити в пастку, дотримуйтеся цих правил:

1. Перевіряйте відправника повідомлення. Шахраї можуть підробити ім'я відправника, тому уважно перевіряйте e-mail або номер телефону. Офіційні компанії надсилають листи переважно з власних та перевірених доменів, наприклад, *@moippo.mk.ua* або *@bank.com*, а не *@gmail.com* (пошту, яку може створити будь-який користувач) чи *@security-alert123.com* (приклад домену, створеного для шахрайства).

2. Не переходьте за підозрілими покликаннями. Якщо вам надійшло повідом-

лення з вимогою «терміново змінити пароль» або «оновити дані», не поспішайте вчиняти якісь дії. Не натискаючи, наведіть курсор на покликання або утримайте палець (на смартфоні), щоб побачити справжню адресу. Якщо URL має дивний вигляд або містить помилки (*paypall-secure-login.com* замість *paypal.com*) – це пастка.

3. Не вводьте дані на сумнівних сайтах. Якщо сайт просить увести ваш пароль чи платіжну інформацію, переконайтеся, що він справжній. Перевірте, чи захищеним є з'єднання в адресному рядку (рис. 3), а також чи збігається адреса з офіційним сайтом. Шахраї можуть підробити дизайн сайту, але не можуть створити ідентичний домен.

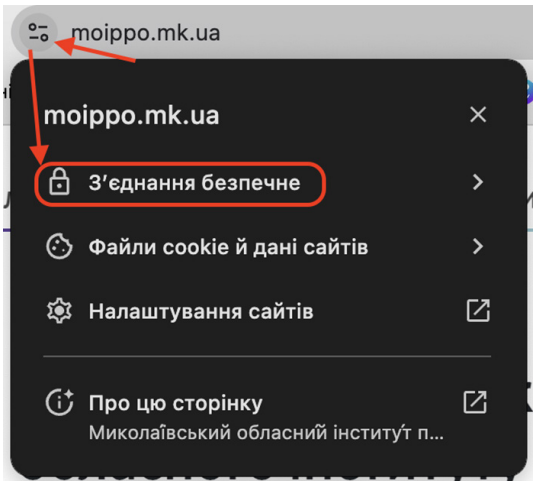

Рис. 3. Перевірка з'єднання в браузері «Google Chrome».

Джерело: авторський варіант

4. Не відкривайте підозрілі файли. Фішингові атаки часто містять вкладення, що можуть мати віруси або шкідливі програми. Якщо вам надіслали файл, якого ви не очікували, навіть від знайомого, не відкривайте його без перевірки.

5. Будьте обережні з терміновими повідомленнями. Шахраї часто намагаються змусити вас діяти швидко: «Ваш акаунт буде заблоковано за 24 години!» або «Ваша картка заблокована, оновіть дані негайно!» (рис. 4). Тиск на користувача – один із методів упливу на користувача. Завжди перевіряйте інформацію через офіційні канали (наприклад, заходьте в акаунт банку через додаток, а не за покликанням чи номером телефону в повідомленні).

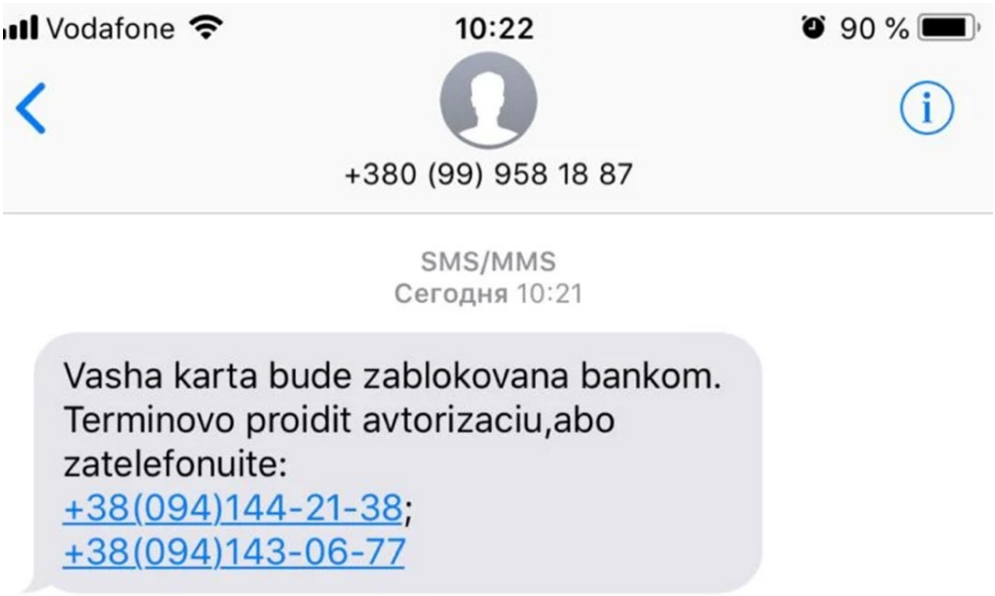

Рис. 4. Приклад фішингового повідомлення про «блокування картки».

Джерело: https://fakty.com.ua/ua/ukraine/20180625-vasha-karta-bude-zablokovana-pryvatbank-poperedyv-pro-sms-shahrajstvo/

6. Якщо повідомлення здається підозрілим, знайдіть офіційні контакти компанії на її сайті та уточніть інформацію. Також можна ввести підозрілий e-mail або номер телефону в Google – можливо, він уже відомий як шахрайський.

Хмарні технології відіграють ключову роль в організації освітнього процесу в Україні під час війни, забезпечуючи зручність спілкування між учнями й учителями та впровадження нових методів навчання. У цьому контексті особливо важливим є захист конфіденційності даних. Відповідно до міжнародних стандартів, таких, як GDPR (https://gdpr-info.eu/), заклади освіти повинні прозоро збирати інформацію та впроваджувати політику для запобігання її викраденню або неналежному використанню. Недотримання цих норм може негативно вплинути на репутацію закладу та створити додаткові ризики для безпеки, такі, як:

- Компрометація облікових записів: зловмисники можуть використовувати фішингові атаки для викрадення паролів учнів або учителів, набуваючи доступ до навчальних платформ.
- Уразливості програмного та апаратного забезпечення: заклади освіти мають регулярно оновлювати програмне забезпечення та підтримувати технічні засоби в актуальному стані.
- Внутрішні загрози: людський фактор часто стає причиною порушень безпеки. Це можуть бути неправильні налаштування платформ або необережне поводження з конфіденційними даними.
- Недостатня видимість хмарних ресурсів: брак контролю над хмарними сервісами ускладнює виявлення загроз і реагування на них.
- Недостатність пріоритетності ризиків: адміністрація закладів може бути перевантажена рекомендаціями щодо безпеки. Важливо визначати пріоритети для ефективного захисту даних.
- Розширення дозволів: неналежне управління доступом до хмарних ресурсів може збільшити вектори атак.
- Поява нових загроз: безпекові ризики постійно змінюються, тому важливо відстежувати їхню еволюцію та адаптувати заходи протидії.
- Щоб забезпечити якісний освітній процес навіть у складних умовах війни, необхідно інтегрувати хмарні технології з системами безпеки, а також навчати вчителів та учнів основ цифрової грамотності та кіберзахисту.

Наступною поширеною загрозою для освітян є використання несанкціонованого, російського або неліцензійного програмного забезпечення (ПЗ), що не лише підвищує вразливість до фішингових атак, а й загрожує безпеці даних у цифровому навчальному середовищі. У контексті інформаційного суспільства та прискореної цифрової трансформації освіти, спричиненої пандемією COVID-19 і повномасштабною війною Росії проти України, таке ПЗ стає слабкою ланкою, яку зловмисники активно експлуатують.

В Україні з 2019 року дистанційне навчання стало основою безперервності освіти, але водночас відкрило нові можливості для кібератак, особливо через людський фактор і недостатню цифрову компетентність педагогів. Неліцензійне ПЗ («піратські» копії операційної системи «Windows», офісного пакету від «Microsoft», додатки «Adobe» тощо), завантажене з ненадійних джерел, часто містить уразливості чи шпигунські модулі, які полегшують фішингові атаки. Звіт ENISA Threat Landscape 2024 підкреслює, що «software vulnerabilities» (уразливість програмного забезпечення) у неліцензійних програмах підвищують ризик компрометації даних (ENISA, 2024, с. 34).

Наприклад, фальшиві чи модифікова-

ні версії додатків для відеозв'язку «Zoom» або «Microsoft Teams», завантажені з ненадійних джерел замість офіційних сайтів, можуть містити приховані бекдори (метод обходу стандартних процедур автентифікації), через них шахраї надсилають фішингові листи, маскуючи їх під «оновлення» чи «повідомлення від адміністрації», або викрадають дані користувачів.

Особливу загрозу становить ПЗ російського походження, як-от додатки компаній «Kaspersky», «Dr.Web», «1C», «Yandex», «Mail.ru» та інші, а також російські неліцензовані версії популярних операційних систем / програм, сайти з краденими копіями фільмів, серіалів, музичний творів. Використання програмного забезпечення, розробленого в РФ чи за її підтримки, становить загрозу національній безпеці через можливі вбудовані механізми збору інформації. Для педагогів це може означати витік конфіденційних даних, кібератаки, шантаж, вивід із ладу операційних систем та програм, що встановлені на таких операційних системах. У воєнний час використання російського ПЗ набуває етичного виміру: навіть безкоштовні продукти своїми податками підтримують економіку агресора.

Важливим є те, що несанкціоноване ПЗ не отримує оновлень безпеки, що робить його ідеальним каналом для фішингу та несанкціонованого збирання інформації про користувача. Державна спецслужба зв'язку у своєму звіті за І півріччя 2024 року, присвяченому російським кібероперація̈м в Україні, зазначає, що кількість інцидентів, пов'язаних із поширенням шпигунського програмного забезпечення (ШПЗ) у 2024 році зросла на 40 % порівняно з 2023 роком, а значну частку окреслених випадків становить поширення ШПЗ через «піратське» програмне забезпечення (Російські кібероперації: аналітика за І півріччя 2024 року, с. 11). Зважаючи на зазначені ризики, надання закладам освіти лише ліцензійного програмного забезпечення має стати пріоритетом органів державної та місцевої влади, управління освітою областей та територіальних громад.

Окрім технічних ризиків, застосування неліцензійного ПЗ порушує Закон України «Про авторське право і суміжні права» (https://zakon.rada.gov.ua/laws/show/3792-12#Text), стандарти GDPR (Загальний регламент про захист даних) (https://www.gdpr.org.ua/) та ліцензійні угоди користувача ПЗ, що може призвести до адміністративної відповідальності та репутаційних втрат.

В умовах війни та спричиненому нею загострені економічних проблем в Україні перешкодою на шляху отримання ліцензованого «софту» для освітян є його вартість або неможливість придбання через особливості закупівельних процедур у бюджетних установах. Для найпоширеніших програм та операційних систем є безкоштовні альтернативи з відкритим кодом, які, хоч і не є повноцінними замінниками платних, але дозволяють сучасному вчителеві чи викладачу виконувати необхідні завдання.

Альтернативою ОС «Windows» можуть стати Unix-подібні операційні системи на основі ядра «Linux», наприклад, «Ubuntu» (https://ubuntu.com/), яка вирізняється простотою, стабільністю, повною українською локалізацією та підтримкою освітнього ПЗ, що робить його ідеальним для новачків і шкіл; «Linux Mint» (https://linuxmint.com/), базований на «Ubuntu», із зручним інтерфейсом, схожим на «Windows», низькими системними вимогами та вбудованими програмами, що полегшує перехід для педагогів; «Lubuntu» (https://lubuntu.me/), легка версія «Ubuntu» з мінімальними вимогами до ресурсів (достатньо 1 гігабайта операційної пам'яті), підходить для застарілих комп'ютерів; а також «Manjaro» (https://manjaro.org/), швидкий і гнучкий дистрибутив на базі «Arch Linux» із найновішим ПЗ і частковою локалізацією, який найкраще пасує технічно підкованим користувачам, готовим до періодичного налаштування, хоча для масового використання в закладах освіти стабільніші «Ubuntu» чи «Mint» можуть бути практичнішими.

Альтернативою для «Microsoft

Office» можуть стати безкоштовні офісні пакети, наприклад, «LibreOffice» (https://www.libreoffice.org/), відкритий пакет із текстовими редакторами, таблицями й презентаціями, сумісний із форматами .docx, .xlsx і .pptx, із регулярними оновленнями від спільноти; «Google Workspace for Education» (https://edu.google.com/), хмарний сервіс із Docs, Sheets і Slides, безкоштовний для шкіл, із вбудованим захистом від фішингу та можливістю спільної роботи онлайн; «OnlyOffice» (https://www.onlyoffice.com/), гнучке рішення з відкритим кодом і хмарною інтеграцією, яке підтримує формати «Microsoft Office» та має простий інтерфейс, зручний для педагогів; а також «WPS Office» (https://www.wps.com/), безкоштовний пакет із сучасним дизайном, схожим на «Microsoft Office», хоча з обмеженнями в безкоштовній версії, що робить його менш універсальним, але придатним для базових завдань.

Варто звернути увагу і на онлайн-інструмент для створення навчальних матеріалів «Canva» (https://www.canva.com/), що пропонує безкоштовну версію «Canva for Education» (https://www.canva.com/education/) для освітян, забезпечуючи доступ до преміум-функцій безкоштовно. Ця платформа дозволяє педагогам легко створювати візуально привабливі презентації, інфографіку, плакати, робочі аркуші та відео завдяки інтуїтивно зрозумілому редактору та тисячам готових шаблонів, адаптованих для навчання. Учителі можуть налаштувати віртуальний клас, запрошувати учнів до співпраці в реальному часі, а також надавати зворотний зв'язок безпосередньо в проєктах. «Canva for Education» підтримує безпечне середовище з відфільтрованим контентом, а також пропонує інструменти ШІ (наприклад, «Magic Write»), які допомагають створювати унікальний контент, заощаджуючи час педагогів і розвиваючи творчість учнів.

Висновки та перспективи досліджень. Дослідження проблеми цифрової безпеки педагогічних працівників в умовах інформаційного суспільства засвідчило її багатогранність і критичну важливість для забезпечення ефективного функціонування освітньої системи. Аналіз теоретичних засад цифрової компетентності показав, що вона є ключовим чинником у формуванні здатності педагогів протистояти кіберзагрозам, які дедалі частіше стають невід'ємною частиною їхньої професійної діяльності. Установлено, що найпоширенішими типами кіберзагроз для освітян є фішинг, використання неліцензійного або російського програмного забезпечення, які цілеспрямовано посилюють в умовах воєнного часу в Україні. Ці загрози не лише створюють ризики для безпеки персональних даних, негативно впливають на якість освітнього процесу, але є неетичними в нинішні часи.

Запропоновані рекомендації щодо протидії кіберзагрозам містять як технічні заходи (оновлення програмного забезпечення, використання безпечних хмарних сервісів), так і підвищення рівня цифрової грамотності через системне навчання. Особливу увагу приділено альтернативам неліцензійного програмного забезпечення, зокрема безкоштовним рішенням із відкритим кодом, що здатні забезпечити базові потреби педагогів у цифровому навчальному середовищі. Доведено, що інтеграція таких інструментів водночас із упровадженням політики безпеки, сумісної з міжнародними стандартами, може значно знизити вразливість освітніх закладів до кібератак.

Подальші дослідження у сфері цифрової безпеки педагогів убачаємо у вивченні психологічних аспектів упливу кіберзагроз на професійну діяльність освітян, зокрема стресу та вигорання, для створення комплексних моделей підтримки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Биков В. Кібербезпека в цифровому навчальному середовищі / В. Биков, О. Буров, Н. Дементієвська // Інформаційні технології і засоби навчання. – 2019. – Т. 70, вип. 2. –

С. 313–331. DOI: https://doi.org/10.33407/itlt.v70i2.2876.

2. Воротникова І. П. Умови формування цифрової компетентності вчителя у післядипломній освіті / І. П. Воротникова // Open educational e-environment of modern University. – 2019. – № 6. – С. 101–118.

3. Іванюк І. В., Овчарук О. В. Аналіз результатів опитування щодо цифрової компетентності вчителя в умовах організації дистанційного навчання / І. В. Іванюк, О. В. Овчарук // Імідж сучасного педагога. – 2023. – Т. 4, 205 : Григорій Сковорода: творення Людини. – С. 101–104. Режим доступу: https://doi.org/10.33272/2522-9729-2022-4(205)-101-104.

4. Іванюк І. В., Овчарук О. В. Проблеми та потреби вчителів в організації дистанційного навчання в Україні під час карантину, спричиненого пандемією COVID-19: результати дослідження 2021 / І. В. Іванюк, О. В. Овчарук // Інформаційні технології і засоби навчання. – 2021. – Т. 85, 5. – С. 29–41. ISSN 2076-8184. Режим доступу: https://doi.org/DOI:10.33407/itlt.v85i5.4669.

5. Концептуально-референтна рамка цифрової компетентності педагогічних і науково-педагогічних працівників. – Київ : Мінцифра, 2021. – 70 с.

6. Кузьмінська О. Дослідження цифрової компетентності студентів та вчителів в Україні // Інформаційно-комунікаційні технології в освіті, дослідженнях та промисловому застосуванні / О. Кузьмінська, М. Мазорчук, Н. Морзе, В. Павленко, А. Прохоров // ICTERI 2018: матеріали міжнар. конф. / за ред. В. Єрмолаєва, М. Суарес-Фігероа, В. Яковини, Г. Майра, М. Нікітченка, А. Співаковського. – Cham : Springer, 2019. – (Communications in Computer and Information Science; Vol. 1007). DOI: https://doi.org/10.1007/978-3-030-13929-2_8.

7. Опис цифрової компетентності педагогічного працівника / Н. Морзе, О. Базелюк, І. Воротникова та ін. – Київ, 2019. – 53 с. – ISSN: 2414-032.

8. Прокоф'єва М., Султанова Л. Цифрова безпека в галузі вищої освіти: аналітичні матеріали / М. Прокоф'єва, Л. Султанова. – Кропивницький : Імекс-ЛТД, 2022. – 38 с.

9. Російські кібероперації: аналітика за І півріччя 2024 року. – Київ: Держспецзв'язку, 2024. – 27 с.

10. Bond M., Marín V. I., Dolch C. et al. Digital transformation in German higher education: student and teacher perceptions and usage of digital media. International Journal of Educational Technology in Higher Education. – 2018. – Vol. 15. – Article number: 48. – DOI: https://doi.org/10.1186/s41239-018-0130-1.

11. Caena F., Redecker C. Aligning teacher competence frameworks to 21st century challenges: The case for the European Digital Competence Framework for Educators (Digcompedu). European Journal of Education. – 2019. – Vol. 54. – P. 356–369. – DOI: https://doi.org/10.1111/ejed.12345.

12. Data Breach Investigations Report 2024 [Electronic resource]. – New York: Verizon, 2024. – 100 p. – Retrieved from: https://verizon.com/dbir.

13. Education during COVID-19 and beyond [Electronic resource]. – New York: United Nations, 2020. – 26 p. – Retrieved from: https://bit.ly/43znfa2.

14. ENISA Threat Landscape 2024 [Electronic resource]. – Athens: ENISA, 2024. – 131 p. – Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

15. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2021: From April 2020 to mid-July 2021. – Athens: ENISA, 2021. – 114 p.

16. Guidelines for the Governance of Digital Platforms: Safeguarding freedom of expression and access to information through a multistakeholder approach [Electronic resource]. – Paris: UNESCO, 2023. – 108 p. – Retrieved from: https://unesdoc.unesco.org/ark:/48223/pf0000387339.

17. Microsoft Digital Defense Report 2022 [Electronic resource]. – Redmond: Microsoft, 2022. – Retrieved from: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

DIGITAL SECURITY AS A COMPONENT OF PROFESSIONAL COMPETENCE FOR TEACHING STUFF

Zaporozhchenko Maksym,
Head of the Centre for Digital Education and Media Culture
Mykolaiv In-Service Teachers Training Institute
4-a Admiralska Street, 54001, Mykolaiv, Ukraine
m.zaporozhchenko@moippo.mk.ua

Shevchenko Hanna,
Methodologist at the
Centre for Digital Education and Media Culture
Mykolaiv In-Service Teachers Training Institute
4-a Admiralska Street, 54001, Mykolaiv, Ukraine
ganna.shevchenko@moippo.mk.ua

The article examines the urgent issue of educators' digital security within the context of a rapidly developing information society and increasing reliance on digital technologies in the education sector. It investigates the theoretical foundations of digital competence, conceptualizing it as a multidimensional construct that encompasses not only technical skills but also values, attitudes, and critical thinking. Digital competence is identified as a key factor in ensuring the safe, ethical, and effective use of ICT in pedagogical practice.

The authors analyse the range of cyber threats faced by educators, including phishing, credential theft, malware distribution and using unlicensed or Russian software, all of which could compromise personal and institutional data. Vulnerabilities in cloud services and data privacy issues are discussed in the context of global trends and national reports. Special attention is given to the impact of the COVID-19 pandemic and the full-scale war in Ukraine, both of which intensified educators' exposure to digital threats and necessitated a rapid shift to remote learning.

The aim of the study is to provide a theoretical rationale and practical recommendations for enhancing educators' resilience to digital threats. The proposed measures include the use of open-source software, consistent digital hygiene education, adherence to international data protection standards (e.g., GDPR), and the development of institutional cybersecurity policies.

The findings emphasize the necessity of a systemic approach that integrates technical infrastructure, policy-level safeguards, and professional development initiatives. Promoting digital awareness and fostering a security-oriented culture among educators is presented as a prerequisite for maintaining the integrity and effective functioning of modern education systems.

Keywords: *cyber attacks; cyber threats; digital competence; digital security; education; information society; teaching staff.*

REFERENCES

1. Bond, M., Marín, V. I., & Dolch, C. (2018). Digital transformation in German higher education: Student and teacher perceptions and usage of digital media. International Journal

of Educational Technology in Higher Education, 15, 48. DOI: https://doi.org/10.1186/s41239-018-0130-1 (eng).

2. Bykov, V., Burov, O. & Dementievska, N. (2022). Kiberbezpeka v tsyfrovomu navchalnomu seredovyshchi [Cybersecurity in the digital learning environment]. *Informatsiini tekhnolohii i zasoby navchannia*, 70(2), 313–331. DOI: https://doi.org/10.33407/itlt.v70i2.2876 (ukr).

3. Caena, F., & Redecker, C. (2019). Aligning teacher competence frameworks to 21st century challenges: The case for the European Digital Competence Framework for Educators (DigCompEdu). European Journal of Education, 54(3), 356–369. DOI: https://doi.org/10.1111/ejed.12345 (eng).

4. Data Breach Investigations Report 2024 [Electronic resource]. New York: Verizon, 2024. – 100 p. Retrieved from: https://verizon.com/dbir (eng).

5. Education during COVID-19 and beyond [Electronic resource]. – New York: United Nations, 2020. – 26 p. – Retrieved from: https://bit.ly/43znfa2 (eng).

6. ENISA Threat Landscape 2024 [Electronic resource]. – Athens: ENISA, 2024. – 131 p. – Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (eng).

7. European Union Agency for Cybersecurity (ENISA). (2021). ENISA Threat Landscape 2021: From April 2020 to mid-July 2021. Athens (eng).

8. Guidelines for the Governance of Digital Platforms: Safeguarding freedom of expression and access to information through a multistakeholder approach [Electronic resource]. – Paris: UNESCO, 2023. – 108 p. – Retrieved from: https://unesdoc.unesco.org/ark:/48223/pf0000387339 (eng).

9. Ivaniuk, I. V., & Ovcharuk, O. V. (2023). Analiz rezultativ opytuvannia shchodo tsyfrovoi kompetentnosti vchytelia v umovakh orhanizatsii dystantsiinoho navchannia [Analysis of the survey results on teachers' digital competence in distance learning]. *Imidzh suchasnoho pedahoha*, 4 (205), 101–104. DOI: https://doi.org/10.33272/2522-9729-2022-4(205)-101-104 (ukr).

10. Ivaniuk, I. V., & Ovcharuk, O. V. (2021). Problemy ta potreby vchyteliv v orhanizatsii dystantsiinoho navchannia v Ukraini pid chas karantynu, sprychynenoho pandemiieiu COVID-19: rezultaty doslidzhennia 2021 [Problems and needs of teachers in organizing distance learning in Ukraine during the COVID-19 pandemic: 2021 survey results]. *Informatsiini tekhnolohii i zasoby navchannia*, 85 (5), 29–41. DOI: https://doi.org/10.33407/itlt.v85i5.4669 (ukr).

11. (2021). *Kontseptualno-referentna ramka tsyfrovoi kompetentnosti pedahohichnykh i naukovo-pedahohichnykh pratsivnykiv* [Conceptual and reference framework for digital competence of teaching and academic staff]. Kyiv: Mintsyfra (ukr).

12. Kuzminska, O., Mazorchuk, M., Morze, N., Pavlenko, V. & Prokhorov, A. (2019). Doslidzhennia tsyfrovoi kompetentnosti studentiv ta vchyteliv v Ukraini [Study of digital competence of students and teachers in Ukraine]. In V. Yermolaiev, M. Suarez-Figueroa, V. Yakovina, G. Mayr, M. Nikitchenko, & A. Spivakovskyi (Eds.). *Information and Communication Technologies in Education, Research, and Industrial Applications. ICTERI 2018* (Vol. 1007, pp. 97–111). Springer. DOI: https://doi.org/10.1007/978-3-030-13929-2_8. (ukr).

13. Microsoft. (2022). Microsoft Digital Defense Report 2022. Redmond. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022 (eng).

14. Morze, N., Bazelyuk, O., Vorotnykova, I., Nanaieva, T., Pasichnyk, O., & Chernikova, L. (2019). *Opys tsyfrovoi kompetentnosti pedahohichnoho pratsivnyka* [Description of teacher's digital competence]. Kyiv (ukr).

15. Prokofieva, M., & Sultanova, L. (2022). *Tsyfrova bezpeka v haluzi vyshchoi osvity:*

Analitychni materialy [Digital security in the field of higher education: Analytical materials]. Kropyvnytskyi: Imeks-LTD (ukr).

16. (2024). Rosiiski kiberooperatsii: Analityka za I pivrichchia 2024 roku [Russian cyber operations: Analytics for the first half of 2024]. Kyiv: State Special Communications (ukr).

17. Vorotnykova, I. P. (2019). Umovy formuvannia tsyfrovoi kompetentnosti vchytelia u pisliadyplomnii osviti [Conditions for the formation of teachers' digital competence in postgraduate education]. *Open Educational E-environment of Modern University*, (6), 101–118 (ukr).

Стаття надійшла до редакції: 30.05.2025
Прийнято до друку: 11.06.2025