УДК 070:004.056“364”

DOI 10.32840/cpu2219-8741/2024.1(57).5

Н. Л. Дащенко

кандидат філологічних наук, доцент
доцент кафедри журналістики
e-mail: nataladash@gmail.com; ORCID: 0000-0002-6189-6897
Тернопільський національний педагогічний університет імені Володимира Гнатюка
вул. М. Кривоноса, 2, м. Тернопіль, 46027, Україна

О. В. Кушнір

кандидат наук із соціальних комунікацій, доцент
доцент кафедри журналістики
e-mail: oksanakush8@gmail.com; ORCID: 0000-0003-3201-5285
Тернопільський національний педагогічний університет імені Володимира Гнатюка
вул. М. Кривоноса, 2, м. Тернопіль, 46027, Україна

Т. В. Решетуха

кандидат наук із соціальних комунікацій, доцент
доцент кафедри журналістики
e-mail: reshtetyana@gmail.com; ORCID: 0000-0003-4515-3425
Тернопільський національний педагогічний університет імені Володимира Гнатюка
вул. М. Кривоноса, 2, м. Тернопіль, 46027, Україна

ЦИФРОВА БЕЗПЕКА ЖУРНАЛІСТІВ РЕГІОНАЛЬНИХ МЕДІА: АКТУАЛІЗАЦІЯ В УМОВАХ ВІЙНИ

Мета дослідження *– проаналізувати рівень володіння цифровими компетентностями в практичній діяльності регіональних журналістів в умовах війни.*

Методологія дослідження. *Для визначення рівня володіння журналістами компетентностями цифрової безпеки було використано комплекс теоретичних та емпіричних методів. Зокрема, описовий метод надав змогу з’ясувати суть основних понять і визначень; аналітико-синтетичний метод – окреслити теоретико-методологічну базу вивчення проблеми; метод анкетування – сформувати емпіричну базу дослідження; загальнонаукові методи узагальнення та інтерпретації даних забезпечили систематизацію отриманих результатів анкетування.*

Результати. *Гібридні війни XX–XXI ст. актуалізували проблему цифрової безпеки глобального та національного медіапросторів, яка неповно осмислена теоретично й недостатньо усвідомлена журналістами-практиками. В особистому та професійному житті медійники постійно стикаються із цілим спектром загроз цифрового характеру, який визначив предмет проведеного у червні 2023 р. анкетування в середовищі різних за віком, досвідом роботи працівників різноформатних регіональних медіа. Опитування стосувалося розуміння цифрової безпеки журналіста загалом та оперування цифровими навичками в умовах війни, що зумовлює потребу особистої та професійної цифрової освіти.*

Новизна. *З’ясовано рівень осмислення цифрових загроз і володіння відповідними безпековими навичками журналістами регіональних медіа.*

Практичне значення. *Результати дослідження можуть бути корисними для медіаменеджерів при прийнятті управлінських рішень, для медіатренерів при формуванні тематики навчання та підбору контингенту слухачів, для журналістів при плануванні професійної та самоосвіти.*

Ключові слова: *регіональна журналістика, безпекова парадигма, цифрова компетентність, цифрова безпека, цифрові загрози.*

І. Вступ

Розвиток інформаційного суспільства сьогодні передбачає активне створення та споживання великого обсягу різноформатних інформаційних продуктів із залученням широкого спектра цифрових технологій. Відтак цифрова компетентність є ключовою в сучасному світі. Вона передбачає критичне та відповідальне використання цифрових технологій для навчання, праці, дозвілля та

участі в суспільному житті. Володіння цифровими компетентностями забезпечує цифрову безпеку особистості, колективів та країни загалом.

Гібридні війни та збройні конфлікти XXI ст. змінили тенденції розвитку медіагалузі, зокрема актуалізували проблему цифрової безпеки глобального та національного медійних середовищ. Це зумовило реакцію передусім серед журналістів-практиків і призвело до появи відповідних розділів («Цифрова безпека журналіста») у посібниках про роботу журналіста в небезпечних умовах [3; 4; 9; 14], тематичного контенту на спеціалізованих журналістських сайтах [5; 11; 13], навчальних курсів на онлайн-платформах [12], організації профільних тренінгів для медіафахівців тощо. Проте, на думку докторки наук із соціальних комунікацій Вікторії Шевченко, «культура цифрової безпеки журналістської діяльності, на жаль, не набула широкого поширення». За її підрахунками, «54% журналістів і 52% служб новин не забезпечують заходів безпеки своїх засобів зв'язку» [16, с. 113]. Також відсутнє теоретичне осмислення українськими журналістикознавцями означеної проблеми, поодинокі наукові студії лише побіжно її окреслюють [2; 16].

Повномасштабна російсько-українська війна загострила проблему цифрової безпеки журналістів загальнонаціональних та регіональних медіа. Це зумовило необхідність аналізу розуміння журналістами концепту «цифрова безпека» та фактичного володіння відповідними навичками.

II. Постановка завдання та методи дослідження

Мета дослідження – проаналізувати рівень володіння цифровими компетентностями у практичній діяльності регіональних журналістів в умовах війни. Об'єкт дослідження – професійний та особистий простір журналістів регіональних медіа у період повномасштабної російсько-української війни. Предмет – цифрові компетентності українських журналістів, призначені для забезпечення цифрової безпеки.

У процесі дослідження застосовано такі методи: описовий – для з'ясування суті основних понять і визначень; аналітико-синтетичний – задля окреслення теоретико-методологічної бази вивчення проблеми; метод анкетування – з метою формування емпіричної бази дослідження; загальнонаукові методи узагальнення та інтерпретації даних забезпечили систематизацію отриманих результатів анкетування.

Загалом результати дослідження можуть бути використані керівниками медіаорганізацій при формулюванні кваліфікаційних вимог до працівників, тренерами з медіаосвіти – при формуванні навчального контенту для відповідної категорії слухачів, журналістами – при організації професійної та самоосвіти.

III. Результати

Міністерством цифрової трансформації України у 2021 р. на основі європейської концептуально-еталонної моделі цифрових компетентностей для громадян DigComp 2.1: The Digital Competence Framework for Citizens було розроблено «Опис рамки цифрових компетентностей для громадян України». У документі аргументовано необхідність їх запровадження в Україні, визначено структуру і зміст реєстру, вказано рівні володіння цифровими компетентностями [7]. В узагальненій структурі цього документа як окрему складову виокремлено «Безпеку у цифровому середовищі». У неї включено такі компетентності: захист пристроїв та безпечне підключення до мережі Інтернет; захист персональних даних і приватності; безпека в інтернеті; захист особистих прав споживача від шахрайства і зловживань; захист здоров'я і благополуччя; захист навколишнього середовища [7, с. 9].

Громадяни України постійно стикаються із загрозами цифрового характеру (кібер-атаки (хакерські), фішинг-атаки, поширення дезінформації, шахрайство в мережі, блокування вебресурсів, доступ до інтернету, доступ до інформації, захист персональних даних). Їх моніторинг від початку повномасштабного вторгнення в Україну здійснює громадська організація «Платформа прав людини» (ГО «ППЛ»). Вона збирає й аналізує інформацію про потенційні порушення цифрових прав громадян, результати подає в аналітичних звітах «Війна у цифровому вимірі та права людини» [6].

У правовому й науковому дискурсах відсутнє однозначне трактування терміна «цифрова безпека»: спектр поглядів варіює від ототожнення його з інформаційною безпекою [1] до тлумачення як одного з її елементів [10], натомість журналістам-практикам пропонуються рекомендації щодо її реалізації [5; 11; 13; 17; 18].

На основі аналізу дефініцій пропонуємо авторське розуміння поняття «цифрова безпека журналістської діяльності»: захищеність функціональних складових медіаорганізацій, яка реалізується через заходи, спрямовані на забезпечення конфіденційності, цілісності і захищеності інформації від несанкціонованого втручання та зменшення зовнішніх і внутрішніх ризиків в інформаційному середовищі.

З початком повномасштабної російсько-української війни цифрова безпека стала невід'ємним атрибутом захисту цілісності, доступності, конфіденційності інформації, а відтак – базовою в системі фахових компетентностей журналістів. За результатами моніторингу Інституту масової інформації, з 24 лютого 2022 р. по 24 грудня 2023 р. країна-агресор скоїла 62 кібератаки на українські медіа [15].

У червні-липні 2023 р. було проведене дослідження «Цифрові загрози для журналістів та блогерів: літо 2023», у якому взяли участь 100 респондентів, з яких 70% журналістів, 22% блогерів та 8% тих, хто поєднує журналістику й блогерство. За результатами цього моніторингу, з початком повномасштабного вторгнення 37% журналістів та 82% блогерів відзначили зростання кібертиску. Серед цифрових загроз, які виокремлюють опитані, найчастішими є фішинг (21% / 23%), видалення сторінок (0% / 18%), злам акаунту (21% / 4%), зараження вірусом (17% / 0%), викрадення інформації з ноутбука / комп'ютера (3% / 0%). Лише 11% журналістів і жоден блогер не стикалися із цифровими загрозами [15].

Рівень загроз продовжує зростати, тому медійникам варто постійно дбати про безпеку особистого інформаційного простору, причому покращувати рівень власної медіаграмотності. З метою з'ясувати розуміння фахівцями поняття цифрової безпеки у професійному середовищі у червні 2023 р. проведено анкетування львівських, тернопільських, хмельницьких медіапрацівників. При підготовці анкети взято до уваги загрози цифрового характеру, які моніторить ГО «ППЛ» [6].

В опитуванні взяли участь 39 медіафахівців таких вікових категорій: 18–25 років – 17 осіб, 26–35 років – 9, 36–45 років – 5, 46–60 років – 5, більше 60 років – 3; гендерного складу: чоловіки – 9, жінки – 30. Професійна належність респондентів така: періодика – 11 осіб, телебачення – 4, радіо – 1, онлайн-видання – 19, одночасна задіяність у різноформатних медіа – 4. Досвід роботи більшості опитаних – 1–5 років (16) або до 1 року (7). До другої групи переважно належать молоді журналісти, віковий статус яких передбачає вправне володіння сучасними ґаджетами та способами їх захисту від загроз. Працівники старшого віку з достатнім досвідом роботи в медіа (4 особи – 6–10 років, 3–11–15 років, 9 – понад 15 років) зобов'язані постійно адаптовуватися до функціональних оновлень пристроїв, які забезпечують безпеку у професійному середовищі.

Питання проведеного анкетування сфокусовано на проблемах надійності паролів, доцільності приєднання до незахищених мереж (wi-fi), убезпечення від онлайн-шахрайства, практикування підвищення рівня цифрової безпеки медійників.

На питання про частоту зміни пароля відповіді респондентів зосередилися на таких варіантах: раз на пів року (9), раз на 3–4 місяці (4), раз на місяць (1). Показово, що 12 осіб повністю впевнені в надійності своїх паролів, тому не змінюють їх, а 13 готові змінити їх лише при підозрі розкриття. Отже, 64% опитаних формують контингент тих, хто ставить під загрозу особисті дані в мережі. Прикметно, що більшість – це молоді люди віком 18–25 років (44%), які ще здобувають журналістську освіту або недавно були студентами. Також не змінюють паролів або роблять це рідко респонденти віком 46+ (6), які мають значний професійний стаж (понад 15 років), але, очевидно, менш адаптовані до сучасних технологічних викликів журналістської діяльності.

Підходи до безпеки власних акаунтів простежуємо за відповідями на запитання про розмаїтість паролів: один пароль на 2–3 акаунти використовує 11 респондентів; для кожного акаунту створює інший 21 особа; переконані в надійності одного пароля для всіх випадків 7 опитаних. Трохи більше від половини опитаних (54%) дотримуються рекомендацій фахівців щодо унікальності паролів для кожного акаунту [4, с. 103; 14], зокрема окремі паролі мають 13 респондентів віком від 18 до 35 років, 8 – віком від 36 до 60 років, натомість не використовують їх медіапрацівники старші 60 років (рис. 1).

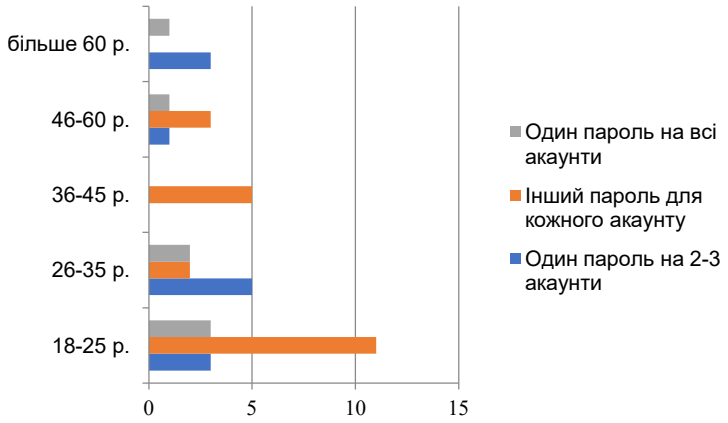

Рис. 1. Використання паролів для захисту акаунтів медіапрацівниками

Розуміння безпечності створюваних паролів було визначено шляхом вибору з-поміж запропонованих: As1zx2qw3df4cv5; LB#2000-ck_ya; Tanichka_24_07_2004. Найнадійнішим респонденти вважають перший (22 відповіді), далі – другий (13), і навіть примітивний третій пароль знайшов своїх прихильників (2). Відповіді респондентів засвідчили, що журналісти у більшості або знайомі

з рекомендаціями фахівців із кібербезпеки щодо довжини та складності пароля (від 12 символів, використання малих і великих букв, цифр, спеціальних символів), або інтуїтивно створюють довгі і нетривіальні паролі.

Існують різні фактори автентифікації: фактор знання (те, що ми знаємо: пароль або PIN-код), фактор володіння (те, що ми маємо: мобільний пристрій або посвідчення особи) і фактор властивості (те, що є частиною нас: відбиток пальця або голос). Додатковими факторами є розташування і час. Врахування цих чинників для власної інформаційної безпеки свідчить про володіння особою безпековою компетентністю. У практиці вона реалізується через використання методів двофакторної автентифікації (2FA): отримання коду текстовим повідомленням, програма для автентифікації, push-сповіщення, програмні маркери, голосова автентифікація тощо.

Проведене анкетування виявило практику застосування в інформаційному середовищі двофакторної автентифікації. Доцільною в усіх випадках вважають її 17 опитаних журналістів, 10 із яких – особи віком 18–25 років; потрібною лише у важливих облікових записах – 16; корисною тільки у соцмережах – 4. Виявилися випадки нерозуміння самого поняття і процесу двома особами, старшими 60 років.

Більшість опитаних (18) не користується wi-fi у громадських місцях, що свідчить про розуміння загроз для професійної діяльності, які посилюються у незахищених мережах. Проте інші респонденти (15) послуговуються цією бездротовою технологією для приватного користування і навіть регулярно (6). Такі відповіді наштовхують на припущення, що багато журналістів (53,8%) розмежовують професійну та приватну безпеку, що свідчить про загалом недостатнє розуміння цифрової безпеки. Адже переважно в одному ґаджеті зосереджена інформація (контакти, паролі тощо), що стосується всіх сфер життя.

Одностайні відповіді респондентів свідчать про розуміння фішингу як виду інтернет-шахрайства (39) та розповсюдженості підробок в інтернет-середовищі (36). Вважаємо, що кількісно великий відсоток відповідей (100% / 92%) вказує про масовість зазначених небезпек та ймовірне стикання з ними медіапрацівників чи в професійній сфері, чи в приватному житті. Анкетування журналістів засвідчило дисонанс між впевненістю у надійності паролів до власних акаунтів (відтак – використання «надійного» пароля для всіх випадків) та усвідомленням масштабності шахрайства в інформаційному просторі, яке спричиняє небезпеку підробки дзвінків та смс з телефонного номера, листів у електронній пошті, діяльності фейкових сайтів.

Відповідно актуалізується проблема опірності цим загрозам в інформаційному середовищі (готовності протистояти, уникати, надійно захищати інформацію), яку можна виробляти шляхом формування відповідних навичок. Таку необхідність підтверджують відповіді респондентів про важливість цифрової компетентності для безпечної діяльності журналіста. Її оцінено дуже високо: за шкалою від 1 до 10 відповіді починаються від позначок 8 (4) і 9 (3), максимально виявляються в оцінці 10 (30). Отже, 77% респондентів усвідомлюють потребу мати чи формувати безпечний інформаційний простір. Важливо, що 25 опитаних (64%) мають досвід участі в тренінгах для журналістів із цифрової безпеки, інші не мають такого досвіду (7 осіб) або чули про такі заходи, але участі в них не брали (7). Прикметно, що негативні відповіді дали різні за віком респонденти, більшість із яких працює в друкованих медіа (9) (рис. 2).

Попри одностайність в усвідомленні необхідності цифрової компетентності як складової безпечної медіадіяльності (95%), результати опитування засвідчили неоднозначне розуміння поняття «цифрова безпека журналіста», продемонструвавши шкалу відповідей від примітивного, загального, часткового, поверхового розуміння до глибокого осмислення. Типові відповіді такі: *основна складова безпечної роботи журналіста; захист файлів від вторгнення іншими користувачами; захищеність у соціальних мережах та в житті; захист особистої інформації (персональних даних), безпека електронної пошти та пристроїв, шифрування; практична діяльність, спрямована на захист комп'ютерних систем і мереж, загалом особистих даних; надійні паролі, коректне налаштування двофакторних авторизацій, безпечні соцмережі / месенджери; знання про власну безпеку в інтернеті, застосування їх на практиці та постійне вдосконалення своїх навичок; кібербезпека журналіста (безпека акаунтів, пристроїв тощо), комунікаційна безпека та захищеність даних, здобутих журналістом у процесі роботи; захист від кібератак, безпека вебсайтів, електронної пошти, конфіденційність.*

Зустрічаються відповіді, які демонструють некоректне розуміння предмета обговорення (*соціальний інжиніринг як складова цифрової безпеки)*, підміну розуміння поняття способами (*використання двоетапної перевірки, створення надійного пароля, захист від блокування та цензури, шпигунства*) та результатами самоубезпечення від загроз (*захист від стеження, збереження доступу до особистих даних та інформації*), переведення в площину психологічної безпеки (*самовідновлення*), надмірне узагальнення (*надійна захищеність усіх ресурсів, захист усього, що міститься у ґаджетах*).

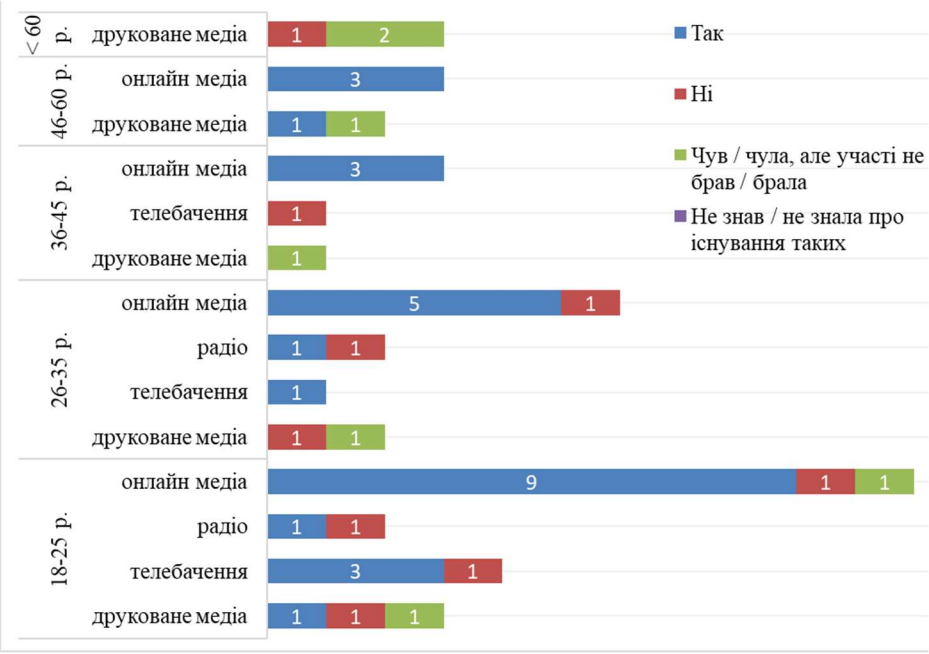

Рис. 2. Участь медійників у тренінгах з цифрової безпеки

Моніторинг володіння цифровими компетентностями працівниками регіональних медіа виявив прогалини в усіх аспектах досліджуваної проблеми. Різні за віком та досвідом праці журналісти продемонстрували необхідність їх залучення до різних форм професійної та самоосвіти. Тому вважаємо доцільним більше уваги зосереджувати на цифрових безпекових компетентностях у процесі навчання в закладах вищої освіти. Наприклад, при вивченні дисциплін журналістського фаху, як-от: «Цифрові технології у професійній діяльності», «Журналістський фах: інтернет-журналістика», «Медіабезпека», – та окремих вибіркових компонентів професійної підготовки[1] [8].

На думку В. Шевченко, випускники факультетів журналістики швидше адаптуються до сучасних медійних технологій і часто більш придатні до цифрових умов діяльності, ніж досвідчені працівники редакцій [16, с. 111]. Науковиця вважає, що журналісти прагнуть додаткового цифрового навчання, але не можуть взяти в ньому участь через надмірну завантаженість чи / та відсутність ініціативи керівництва редакції щодо його організації [16, с. 111]. Дійсно, з-поміж опитаних нами осіб 14 (36%) не брали участі у тренінгових програмах із цифрової безпеки, навіть якщо знали про їх проведення. Відтак медіаменеджерам варто мотивувати своїх працівників до відвідування спеціалізованих тренінгів, організовувати їх безпосередньо в редакціях, ввести в штатний розпис посаду відповідального за цифрову безпеку чи консультанта із цих питань.

IV. Висновки

Гібридна війна Росії проти України актуалізувала цифровий вектор безпеки професійної діяльності журналістів поряд із фізичним, психологічним, правовим складниками безпекової парадигми. За відсутності глибокого теоретичного осмислення суті досліджуваного поняття медіафахівці визнають його значення як складника професійної компетентності у зв'язку зі зростанням цифрових загроз особистого та професійного інформаційного простору журналістів. Результати анкетування львівських, тернопільських, хмельницьких медіапрацівників, проведеного в червні 2023 р., засвідчили як неоднозначне, часто поверхове або хибне розуміння респондентами поняття «цифрова безпека журналіста», так і недостатній рівень оперування цифровими навичками в умовах війни. Це зумовлює потребу в проведенні практикоорієнтованих тренінгів, а також визначає нові вимоги до формування фахових компетентностей у здобувачів вищої освіти за освітньою програмою 061 Журналістика.

Питання безпеки повинно стати першочерговою нормою професійної діяльності журналістів, а подальші наукові пошуки можуть розвиватися в напрямі кореляції цифрової та психологічної складових безпечної професійної діяльності медіафахівців.

Список використаної літератури

1. Грабар Н. С. Інформаційна безпека в умовах становлення глобального інформаційного суспільства. *Державне управління: удосконалення та розвиток*. 2019. № 7. URL: http://www.dy.nayka.com.ua/?op=1&z=1461 (дата звернення: 11.01.2024).

[1] Назви дисциплін орієнтовні і подані відповідно до ОПП «Журналістика» Тернопільського національного педагогічного університету імені Володимира Гнатюка.

2. Давидова Л. В., Зайко Л. Я. Цифрова безпека як складник професійної діяльності журналістів. *Дослідження інновацій та перспективи розвитку науки і техніки у XXI столітті* : матер. Міжнар. наук.-практ. конф., м. Рівне, 25–26 листопада 2021 р. Рівне : ВД «Гельветика», 2021. Ч. 1. С. 210–212.
3. Журналіст і (не) безпека : посібник для журналістів / уклад. : І. Земляна, М. Ратушний, І. Чулівська, О. Голуб. Київ : IMI, 2016. 192 с.
4. Земляна І. Робота під PRESSом. Посібник для безпечної повсякденної роботи медійників. Київ : IMI, 2020. 148 с. URL: https://imi.org.ua/upload/books/2019/07/03/Posibnyk-z-bezpeky-2020.pdf?fbclid=IwAR3tctn7V0mBXDEClei5u0Q4cF5VcKhWrEJ3RNVxfrqV3xEOhhwR6CuC7eQ (дата звернення: 11.01.2024).
5. Кібербезпека. *Jmama*. URL: https://j-mama.imi.org.ua/article/cybersecurity (дата звернення: 11.01.2024).
6. Моніторинг дотримання цифрових прав. *Платформа прав людини*. URL: https://www.ppl.org.ua/monitoring/monitoring-cifrovix-prav (дата звернення: 11.01.2024).
7. Опис рамки цифрових компетентностей для громадян України. *Міністерство цифрової трансформації.* 2021. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf (дата звернення: 11.01.2024).
8. Освітньо-професійна програма «Журналістика» першого (бакалаврського) рівня вищої освіти. *Сайт ТНПУ*. URL: https://tnpu.edu.ua/about/public_inform/akredytatsiia%20ta%20litsenzuvannia/osvitni_prohramy/bakalavr/fizh/061_2023.pdf (дата звернення: 11.01.2024).
9. Посібник з безпеки для журналістів : посібник для репортерів у небезпечних зонах. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381168 (дата звернення: 11.01.2024).
10. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2 (5). С. 162–169. URL: https://doi.org/10.37750/2616-6798.2012.2(5).271955 (дата звернення: 11.01.2024).
11. Цифрова безпека журналіста : відеопосібник від АУП. URL: https://www.aup.com.ua/cifrova-bezpeka-zhurnalista-videopos/ (дата звернення: 11.01.2024).
12. Цифрова безпека журналістів та інших працівників медіа. *Prometheus*. URL: https://prometheus.org.ua/course/course-v1:Prometheus+DSJ101+2022_T1 (дата звернення: 11.01.2024).
13. Цифрова безпека: поради. *Committee to Protect Journalists.* URL: https://cpj.org/uk/2022/03/%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0-%D0%BF%D0%BE%D1%80%D0%B0%D0%B4%D0%B8/ (дата звернення: 11.01.2024).
14. Цифрова безпека : посібники для кращого захисту від зловживань в Інтернеті. URL: https://cpj.org/uk/2022/05/%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0-%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%D0%B8-%D0%B4%D0%BB%D1%8F-%D0%BA%D1%80%D0%B0%D1%89%D0%BE%D0%B3/ (дата звернення: 11.01.2024).
15. Цифрові загрози для журналістів та блогерів: літо 2023. *IMI.* URL: https://imi.org.ua/infographics/tsyfrovi-zagrozy-dlya-zhurnalistiv-ta-blogeriv-lito-2023-i55771 (дата звернення: 11.01.2024).
16. Шевченко В. Трансформація професії журналіста в цифровому середовищі. *Вісник Львівського університету. Серія: Журналістика.* 2019. Вип. 45. С. 108–116.
17. Яких правил цифрової поведінки слід дотримуватися журналістам – у Київському ЦЖС відбувся тренінг. URL: https://nsju.org/novini/yakyh-pravyl-czyfrovoyi-povedinky-slid-dotrymuvatysya-zhurnalistam-u-kyyivskomu-czzhs-vidbuvsya-trening/ (дата звернення: 11.01.2024).
18. Як? Практичні поради з цифрової безпеки. *Лабораторія цифрової безпеки*. URL: https://yak.dslua.org/ (дата звернення: 11.01.2024).

References

1. Hrabar, N. S. (2019). Informatsiina bezpeka v umovakh stanovlennia hlobalnoho informatsiinoho suspilstva [Information security in the conditions of the formation of the global information society]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok,* 7. Retrieved from http://www.dy.nayka.com.ua/?op=1&z=1461 [in Ukrainian].
2. Davydova, L. V., & Zaiko, L. Ya. (2021). Tsyfrova bezpeka yak skladnyk profesiinoi diialnosti zhurnalistiv [Digital security as a component of the professional activity of journalists], *Doslidzhennia innovatsii ta perspektyvy rozvytku nauky i tekhniky u XXI stolitti,* materialy Mizhnarodnoi naukovo-praktychnoi konferentsii [Research on innovations and prospects for the development of science and technology in the 21st century, Proceedings of the Internetional Scientific and Practical Conference]. Rivne [in Ukrainian].

3. Zemlyana, I., Ratushny, M., Chulivska, I. & Golub, O. (2016). *Zhurnalist i (ne) bezpeka: posibnyk dlia zhurnalistiv* [Journalist and (in)security: a guide for journalists]. Kyiv: Institute of Mass Information [in Ukrainian].
4. Zemliana, I. *Robota pid PRESSom. Posibnyk dlia bezpechnoi povsiakdennoi roboty medivnykiv* [Work under PRESS. A guide for the safe daily work of journalists]. Kyiv: Institute of Mass Information [in Ukrainian].
5. Kiberbezpeka [Cyber security]. *Jmama: sait.* Retrieved from https://j-mama.imi.org.ua/article/cybersecurity [in Ukrainian].
6. Monitorynh dotrymannia tsyfrovykh prav [Monitoring of compliance with digital rights]. *Platforma prav liudyny.* Retrieved from https://www.ppl.org.ua/monitoring/monitoring-cifrovix-prav [in Ukrainian].
7. Opys ramky tsyfrovykh kompetentnostei dlia hromadian Ukrainy [Description of the framework of digital competences for citizens of Ukraine.]. *Ministerstvo tsyfrovoi transformatsii: sait.* Retrieved from https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf [in Ukrainian].
8. Osvitno-profesiina prohrama «Zhurnalistyka» pershoho (bakalavrskoho) rivnia vyshchoi osvity [Educational and professional program «Journalism» of the first (bachelor) level of higher education]. *TNPU.* Retrieved from https://tnpu.edu.ua/about/public_inform/akredytatsiia%20ta%20litsenzuvannia/osvitni_prohramy/bakalavr/fizh/061_2023.pdf [in Ukrainian].
9. Posibnyk z bezpeky dlia zhurnalistiv: Posibnyk dlia reporteriv u nebezpechnykh zonakh [Safety Guide for Journalists: A Guide for Reporters in Danger Zones]. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000381168 [in Ukrainian].
10. Furashev, V. M. (2012). Kiberprostir ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti [Cyberspace and information space, cyber security and information security: essence, definition, differences]. *Informatsiia i pravo*, 2 (5), 162–169 [in Ukrainian].
11. Tsyfrova bezpeka zhurnalista : videoposibnyk vid AUP [Journalist's digital safety: a video guide from AUP]. *Akademiia ukrainskoi presy*. Retrieved from https://www.aup.com.ua/cifrova-bezpeka-zhurnalista-videopos/ [in Ukrainian].
12. Tsyfrova bezpeka zhurnalistiv ta inshykh pratsivnykiv media [Digital security of journalists and other media workers]. *Prometheus*. Retrieved from https://prometheus.org.ua/course/course-v1:Prometheus+DSJ101+2022_T1 [in Ukrainian].
13. Tsyfrova bezpeka: porady [Digital security: tips]. *Committee to Protect Journalists*. Retrieved from https://cpj.org/uk/2022/03/%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0-%D0%BF%D0%BE%D1%80%D0%B0%D0%B4%D0%B8/ [in Ukrainian].
14. Tsyfrova bezpeka: Posibnyky dlia krashchoho zakhystu vid zlovzhyvan v Interneti [Digital security: Guides to better protect against online abuse]. Retrieved from https://cpj.org/uk/2022/05/%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0-%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%D0%B8-%D0%B4%D0%BB%D1%8F-%D0%BA%D1%80%D0%B0%D1%89%D0%BE%D0%B3/ [in Ukrainian].
15. Tsyfrovi zahrozy dlia zhurnalistiv ta bloheriv: lito 2023 [Digital threats to journalists and bloggers: summer 2023]. *Instytut masovoi informatsii.* Retrieved from https://imi.org.ua/infographics/tsyfrovi-zagrozy-dlya-zhurnalistiv-ta-blogeriv-lito-2023-i55771 [in Ukrainian].
16. Shevchenko, V. (2019). Transformatsiia profesii zhurnalista v tsyfrovomu seredovyshchi [Transformation of the journalist profession in a digital medium]. Visnyk Lvivskoho univer-sytetu. Seriia: Zhurnalistyka*,* 45, 108–116. doi: 10.30970/vjo.2019.45.9991 [in Ukrainian].
17. Yakykh pravyl tsyfrovoi povedinky slid dotrymuvatysia zhurnalistam – u Kyivskomu TsZhS vidbuvsia treninh [What are the rules of digital behavior that journalists should follow – a training was held at the Kyiv City Center for Social Security]. Retrieved from https://nsju.org/novini/yakyh-pravyl-czyfrovoyi-povedinky-slid-dotrymuvatysya-zhurnalistam-u-kyyivskomu-czzhs-vidbuvsya-trening/ [in Ukrainian].
18. Yak? Praktychni porady z tsyfrovoi bezpeky [As? Practical advice on digital security]. *Laboratoriia tsyfrovoi bezpeky*. Retrieved from https://yak.dslua.org/ [in Ukrainian].

Стаття надійшла до редакції 16.01.2024.

Received 16.01.2024.

Dashchenko N., Kushnir O., Reshetukha T. Digital Security of Journalists in Regional Media: Actualisation in Wartime

The research aims *to analyze the level of digital competencies proficiency among journalists in regional media operating under wartime conditions.*

Research methodology. *A combination of theoretical and empirical methods was employed to determine journalists' proficiency in digital security competencies. Specifically, the descriptive method clarified the essence of key concepts and definitions, while the analytical-synthetic method outlined the theoretical and methodological foundation of the research problem. The survey method constituted the empirical foundation of the research. General scientific methods of data generalization and interpretation resulted in the systematic organization of the survey results.*

The results*. Hybrid Wars of the 20th–21st centuries have brought attention to the problem of digital security in the global and national media space, which is not fully explored theoretically and not sufficiently understood by practicing journalists. In both personal and professional spheres, media practitioners constantly face a spectrum of digital threats, which determined the subject of the survey conducted in June 2023 among individuals of different ages and levels of experience in diverse regional media formats. The survey focused on the comprehension of digital security under wartime conditions, thereby highlighting the importance of both personal and professional digital education.*

The novelty *of the research lies in clarifying the level of comprehension of digital threats and proficiency in corresponding security skills among journalists in regional media.*

Practical meaning*.The results of this research can prove valuable for media managers in decision-making processes, for media trainers in shaping training themes and selecting the audience, and for journalists in planning their professional and self-development.*

Key words: *regional journalism, security paradigm, digital competence, digital security, digital threats.*