УДК 007: 304 : 004.9 [004.49; 004.58; 659.3+004.6]
DOI https://doi.org/10.32782/2710-4656/2024.2.2/44

Цапок О. М.
Черкаський національний університет імені Богдана Хмельницького

Коваль С. В.
Черкаський національний університет імені Богдана Хмельницького

ЗАПОБІГАННЯ ФІШИНГУ ЯК СКЛАДНИК ЦИФРОВОЇ БЕЗПЕКИ ОБЛІКОВИХ ЗАПИСІВ МЕДІЙНИКІВ В УМОВАХ ВІЙНИ

У статті акцентовано на важливості цифрової безпеки в діяльності журналістів під час російської війни проти України, адже ворог здійснює активні кібератаки і в медійній площині. У цьому контексті вразливими можуть стати облікові записи (акаунти) журналістів, через що потрібно приділяти особливу увагу їхньому цифровому захисту. Однією з найбільш поширених форм цифрових загроз обліковим записам медійників є фішинг, за допомогою якого зловмисники зламують їхні акаунти, надсилаючи їм повідомлення зі шкідливими гіпертекстовими посиланнями.

У роботі описано різновиди активних форм фішингу проти облікових записів журналістів. До них належить зламування їхнього акаунта для подальшого фішингу на інші акаунти, розсилання зловмисних повідомлень з небезпечними гіперпокликаннями, а також позначення сторінок журналістів у повідомленнях про нібито деактивування цих сторінок протягом 24 годин. Крім того, схарактеризовано два типи фішингу проти журналістів. Констатовано, що перший тип спричинений їхньою професійною діяльністю й спрямований проти неї, а другий становить комерційний фішинг, застосований для заволодіння коштами медійників й незаконним отриманням фінансових надходжень від інших користувачів через використання зламаних акаунтів журналістів.

Посутню увагу в публікації приділено шляхам запобігання пошкодження облікових записів журналістів. Їх диференційовано на психологічні та технічні. Наголошено, що з психологічного боку журналісти мають застосовувати правило «zero trust» (нульової довіри), виявляти уважність та обережність щодо отриманих повідомлень, які можуть містити шкідливі покликання, звертати увагу на адресанта та стиль отриманого сповіщення. З технічного боку цифровий захист облікових записів медійників від фішингу ґрунтується на правильному виборі пароля для акаунта, унікальності паролів для кожного з облікових записів журналістів, застосуванні двофакторної автентифікації. Розкрито алгоритм дій медійників у разі підозри та виявлення факту зламування їхнього облікового запису. Теоретичні й практичні аспекти публікації ілюстровано прикладами із журналістської практики.

Ключові слова: *акаунт, цифрова безпека, гіперпосилання, двофакторна автентифікація, кібератака, нульова довіра, обліковий запис, пароль, фішинг.*

Постановка проблеми. Цифрова захищеність завжди була актуальною в діяльності журналістів з моменту її диджиталізації. Однак особливого значення їхня цифрова безпека набула під час повномасштабного вторгнення Росії в Україну, коли ворожа сторона почала активно використовувати інформаційно-цифровий простір для ведення війни, зокрема, здійснюючи цифрові атаки на українських медійників. Так, Державна служба спеціального зв'язку та захисту інформації у перші місяці війни загалом констатувала зростання кількості інформаційно-психологічних операцій, спрямованих у соціальних мережах та месенджерах на населення України. У цей період зафіксовано злам акаунтів військових та публічних осіб, зокрема журналістів, шляхом фішингу для подальшого розміщення в них пропаганди та закликів до українців здаватися [5].

Станом на початок 2024 року зазначена організація вказала, що кібератаки здійснено за допомогою завчасного отримання зловмисниками доступу до комп'ютерних систем через використання скомпрометованих VPN-акаунтів, а також через виявлені недоліки налаштувань та вразливі місця програмного забезпечення. Шпигування з боку кіберзлочинців відбувалося з використанням модифікованого шкідливого програмного забезпечення [11]. У контексті названих цифрових загроз одним із поширених способів завдання шкоди медійникам, зокрема їхнім обліковим записам,

є фішинг. На те, що він становить невіддільний складник російсько-української війни, вказала також Незалежна медійна рада у своїх рекомендаціях щодо цифрової безпеки журналістів у воєнних умовах [9]. Тож питання цифрової захищеності медійників під час війни, зосібна захищеність їхніх акаунтів від фішингу, наразі становить особливу значущість.

Аналіз останніх досліджень і публікацій. Цифрова безпека журналістів неодноразово привертала увагу дослідників та фахівців-практиків. Так, В. Шевченко зазначила про важливість культури цифрової безпеки журналістів та підвищення обізнаності щодо неї завдяки участі у фахових тренінгах та семінарах [15, с. 113]. На актуальність цифрової безпеки як складника фахової діяльності журналістів вказали науковці Л. В. Давидова та Л. Я. Зайко [2]. Щодо фішингу, то в різних джерелах знаходимо певні аспекти його розкриття в контексті діяльності журналістів. Так, експерти із громадської організації «Лабораторія цифрової безпеки» спільно з медіаекспертою І. Земляною до початку повномасштабної війни розробили ряд цінних порад журналістам щодо їхньої цифрової безпеки, зокрема спрямованих на забезпечення надійності паролів облікових записів, безпечної роботи в браузерах та на персональних комп'ютерах [3, с. 102–106]. Також слушні поради щодо цифрової безпеки в зоні бойового конфлікту надали представники організації «Репортери без кордонів» у посібнику з безпеки для журналістів [8]. Медіаексперт І. Розкладай схарактеризував різновиди сучасного фішингу проти журналістів та дав окремі поради щодо його запобігання й подоланню наслідків від нього [6]. Попри наявні джерела, поки що немає цілісного викладу важливих теоретико-практичних відомостей щодо цифрової безпеки акаунтів медійників в аспекті фішингових атак на їхні облікові записи. Тож існує потреба більш детального аналізу та систематизованого розкриття особливостей фішингу на облікові записи медійників та цифрового захисту цих записів від нього, що й становить актуальність пропонованого дослідження.

Постановка завдання. Під час війни рівень цифрових загроз для медійників значно зріс. Улітку 2023 року громадська організація «Інститут масової інформації» провів опитування серед журналістів та блогерів про цифрові небезпеки, яких вони зазнали. З-поміж інших опитані виокремили злам акаунтів, спостереження і стеження за ними, зараження вірусами цифрового обладнання, викрадення інформації з комп'ютера [14]. Урахувуючи зазначене, вважаємо за потрібне зосередити увагу на одній з найпоширеніших цифрових загроз у діяльності медійників – на зламі їхнього акаунта, зокрема з використанням фішингу як найпоширенішого способу реалізації цього кіберпорушення.

Мета нашої публікації – розкрити особливості цифрового захисту акаунтів журналістів в онлайнових сервісах та убезпечення від фішингу як поширеного способу атаки на облікові записи медійників. Доречно схарактеризувати специфіку фішингових атак під час війни та захисту від них особистих профілів медійників у соціальних мережах.

Поставлена мета передбачає вирішення в дослідженні таких завдань: 1) розкрити поняття фішингу, його мету, особливості застосування та наслідки від цього; 2) описати різновиди фішингових атак на акаунти журналістів; 3) схарактеризувати безпекові заходи, які мають вжити медійники для запобігання такій цифровій загрозі, та подальші їх кроки, якщо таку загрозу виявлено.

Виклад основного матеріалу. Насамперед зазначимо, що облікові записи в різних онлайнових сервісах, як-от соціальні мережі, для зловмисників можуть становити цінні інформаційно-цифрові надбання, особливо в тому разі, якщо вони мають тривалу історію функціонування. Мета використання таких активів буває різною. Наприклад, кіберзлочинці можуть за допомогою одних зламаних профілів зламувати інші, розсилати через них віруси, використовувати для популяризації інших облікових записів у ботофермах.

Характеризуючи особливості цифрового захисту облікових записів медійників, доцільно подати визначення цього поняття. Тож обліковий запис – це частина сайту або сервісу, яка доступна лише конкретному користувачеві після авторизації. Він містить його особисту інформацію, а також відомості, що дають змогу його ідентифікувати під час підключення до системи. Щоб зловмисники не заволоділи обліковими записами користувачів, зокрема медійників, ці записи потрібно належно захистити від втручання сторонніх осіб. Такий захист варто вибудувати з урахуванням найпоширеніших способів злому акаунтів. До них фахівці із цифрової безпеки зараховують такі:

– фішинг (введення логіна та пароля на підробленому сайті);

– скидання пароля через опцію «Я не пам'ятаю свій пароль»;

– повторне використання пароля (застосування однакових паролів для різних облікових записів);

– перехоплення смс-повідомлення [4].

Далі зосередимо нашу увагу на найпоширенішому способі зламу облікових записів журналістів й способах захисту від нього – фішингу. За своєю суттю це форма кібершахрайства, коли особа видає себе за когось іншого, щоб шляхом надсилання шкідливих листів незаконно отримати доступ до облікових записів особи, її персональних даних або отримати її кошти. Саме за його допомогою найчастіше кіберзлочинці пошкоджують облікові записи журналістів, котрі працюють із соцмережами та для котрих ці мережі становлять платформи спільного доступу до інформації, якою вони діляться та з якою працюють. Цей спосіб зламу акаунтів зловмисники активно використовували й до повномасштабного вторгнення Росії в Україну, у 2021 році, про що, наприклад, у своєму аналізі вказали експерти з «Лабораторії цифрової безпеки» [12]. Проте особливо така форма кібератак активізувалася під час війни. Так, за твердженням медіаюриста І. Розкладая, фішинг у соцмережах став негативним трендом 2023 року. За період з травня до листопада зазначеного року він подав до адміністрацій соціальних мереж компанії «Мета», зокрема «Фейсбуку», понад 30 тис. повідомлень про фішингові атаки [6]. На підставі аналізу цих атак І. Розкладай виокремив три різновиди фішингу. До першого різновиду належить таке втручання в акаунт, після якого зламаний обліковий запис використовують для подальшого фішингу на інші облікові записи.

Другий різновид фішингу, коли кіберзлочинці, розраховуючи на низьку пильність користувачів, зокрема медійників, розсилають їм зловмисні сповіщення і повідомлення, що імітують повідомлення сторінок адміністрацій соцмереж. У таких повідомленнях шахраї вказують, що сторінка користувача порушила правила соцмережі щодо розміщення контенту, і вона згодом буде видалена, і щоб цього не сталося, їм пропонують підтвердити доступ до сторінки шляхом переходу за розміщеним покликанням. Щойно користувач це зробить і введе свої логін та пароль, він відразу втрачає доступ до своєї сторінки, натомість доступ до неї отримують зловмисники. Для розсилання цих сповіщень вони використовують сервіс гостьових повідомлень. Наприклад, фейсбук дозволяє надсилати повідомлення, навіть якщо користувач не має в ньому свого акаунта. Гостьовий акаунт діє протягом доби й зникає, але в чаті адресата надіслане повідомлення залишається, тому важливо його не відкривати, а сам чат видалити.

Одним зі способів другого різновиду фішингу є тегання різних акаунтів та сторінок із повідомленням, що ці сторінки деактивують протягом 24 годин за порушення. Зловмисники пропонують оскаржити таке рішення за покликанням, яке є фішинговим. Користувач, зокрема журналіст, хибно думає, що воно переводить його на фейсбук, і якщо він захоче за ним перейти, то йому потрібно залогінитись. Коли це відбувається – стається злам акаунта. Щодо цього фахівці з «Лабораторії цифрової безпеки» радять пам'ятати, що адміністрації соціальних мереж «Фейсбук» та «Інстаграм» ніколи не повідомляють про скарги через репости й теги, аби довести до відома користувачів про порушення. Якщо таке сталося, вони надсилають відомості про порушення через попапи чи сповіщення, крім того, цю інформацію можна переглянути у support inbox [12].

Ще одним різновидом фішингу, за спостереженням медіаюриста І. Розкладая, є злам облікового запису, через який поширюють дописи про можливість отримання соціальних виплат, наприклад від ООН, НАТО, «Червоного Хреста», застосунку «Дія». Необачні користувачі у такому разі самі надають дані шахраям. Вважаючи, що вводять логін у фейсбук, насправді вони вводять логін в інше місце, у якому крадуть їхні дані [7].

Варто зазначити, що зламування акаунтів журналістів шляхом фішингу відбувається як для перешкоджання їхній професійній діяльності, так і для комерційного шахрайства, пов'язаного із незаконним отриманням коштів від громадян за допомогою використання даних зі зламаного акаунта. У першому випадку зловмисники ретельно вивчають дані конкретного журналіста, щоб потім сформулювати таке фішингове повідомлення, яке не викличе у нього підозри у неправдоподібності. Наприклад, так було у випадку із броварським журналістом Д. Карпієм, якому порушники надіслали повідомлення із псевдопропозицією співпраці із виданням «Тиждень». Для переконливості в тексті повідомлення вказано, що його автор нібито давно стежить за роботою журналіста у виданнях «Маєш право знати» та «Трибуна-Бровари», із якими він насправді співпрацював.

Комерційний фішинг, тобто незаконне отримання коштів чи банківських даних через зламаний акаунт, є однією із вагомих причин такого пошкодження акаунтів користувачів-медійників під час війни. Він спрямований на те, щоб через використання облікового запису відомої людини виманити в інших користувачів кошти, які нібито в них просить справжній власник акаунта на благодійність чи для інших потреб. Так, у 2023 році відома телеведуча каналу «1+1» В. Хамайко пові-

домила, що її обліковий запис в телеграмі зламали зловмисники й розсилали з нього повідомлення її друзям та знайомим з проханням позичити великі суми грошей. Щоб медійниця не змогла зайти у свій акаунт, вони змінили пароль до нього [10].

Щодо фішингу, також варто вказати на зламування акаунтів не лише окремих медійників, а й навіть облікових записів певних медіа, щоб надсилати з них зловмисні повідомлення підписникам цих медіа. Як приклад, наведемо історію із Суспільним мовником, яка трапилася у березні 2022 року. Тоді зловмисники, зламавши акаунт медіа, розсилали від нього повідомлення із покроковою інструкцією, як «допомогти вимкнути вебсайти агресора». Інструкція містила спонукання розпакувати надісланий файл та запустити програму. На це відреагували представники Суспільного із закликом не відкривати листи й не переходити за посиланням, зазначивши, що жодних листів користувачам вони не надсилали. Працівники Суспільного також наголосили, що офіційна розсилка від мовника відбувається з їхньої офіційної пошти, повідомлення пресслужби Суспільного публікують на його офіційному сайті або на офіційних сторінках у фейсбуці та інстаграмі [13].

Щоб не стати жертвою фішингу, медійникам потрібно подбати про захист своїх акаунтів. Він може мати нетехнічний характер, тобто базуватися на психології мислення й правильній поведінці журналіста, а також мати технічне спрямування, пов'язане з цифровим захистом його облікового запису. Щодо першого аспекту, психологічного, то важливим правилом досягнення безпеки облікового запису є так звана «zero trust» – нульова довіра: медійникам потрібно не довіряти жодним лінкам у листах чи запитам від сторонніх осіб у директі, завантаженням контенту з незнайомих сайтів, вони мають все ретельно перевіряти.

З психологічного боку фішинг тісно пов'язаний з емоціями: шахраї у своїх повідомленнях використовують емоційно забарвлені конструкції, щоб вплинути на користувачів й спонукати їх до бажаних, необдуманих дій, що призведуть до зламу акаунта. Тож медійники мають бути уважними, якщо повідомлення впливає на їхній емоційний стан, викликаючи страх, сором, надію, обіцянку виграшу тощо. Журналістам потрібно бути особливо обачними з повідомленнями, які закликають їх зробити щось похапцем, нашвидкуруч або ж містять надто привабливі пропозиції, пов'язані із переходом за посиланнями чи завантаженнями доданих файлів. Вони мають уважно переглядати дані облікового запису відправника і сам вміст повідомлення, щоб пересвідчитися у правдивості такого. Уважність допоможе їм помітити певні відхилення від звичних стилістичних конструкцій, орфографії, виявити певні зміни у розкладці клавіатури чи тоні основного повідомлення відправника. Наявність таких елементів свідчитиме про підробний чи зламаний обліковий запис, із якого було надіслане повідомлення медійникам.

Зазначимо, що журналістам під час війни не варто нехтувати безпекою зламу облікового запису в електронних скриньках, який може статися через фішинг. Насамперед їм слід уважно перевіряти адресу відправника, зазвичай у ній може траплятися помилка в одній літері чи в символі, на яку не звертають уваги (*noreply.ssuport@gmail.com*, замість *no-reply@accounts.google.com*). Також досить часто зловмисники застосовують неперсональне звернення («*Шановний користувач*», «*Вітаємо*», і далі подано скопійований e-mail користувача тощо) і занадто узагальнений підпис («*Команда підтримки* / *Support team* / *Команда Google акаунтів*» тощо).

Як «гачки» у фішингових атаках проти медійників кіберзлочинці використовують такі елементи: у темі листа вони акцентують на важливості надісланого повідомлення («*Терміново!*», «*Ваш акаунт зламано!*», «*Увага! Ваш акаунт буде деактивовано!*» тощо), а також розміщено заклик до термінової реакції медійників («*У вас є 24 години!*», «*Терміново оновіть пароль!*», «*Терміново підтвердьте пароль!*», «*Терміново оновіть дані!*» та ін.). У повідомленнях особливу увагу журналістам потрібно звертати на лінки, які можуть бути замаскованими й вести на фішингові сайти (їх можна перевірити в базі Google *transparencyreport.google.com/safebrowsing/search*). Скорочені покликання доречно перевіряти за допомогою сервісів *unshorten.it* чи *checkshorturl.com*. Якщо в листі до медійників є вкладення, то варто обережно відкривати архіви з паролем чи відеофайли. Це можна зробити через Google-диск або перевірити на сайті *virustotal.com*.

Щодо технічного цифрового захисту акаунтів медійників під час війни, традиційними є поради встановити для входу надійний пароль. Для цього він повинен відповідати таким вимогам: бути довгим й мати понад 12 символів; не містити особистої інформації, яку легко дізнатись (імена дружини/чоловіка, дітей, клички тварин, дату народження тощо); до нього обов'язково мають входити букви, цифри, спеціальні символи; унікальність (окремий пароль для кожного облікового запису). Унікальності пароля журналісти мають приділити особливу увагу: не можна

повторювати пароль від облікових записів у фейсбуці, інтернет-банкінгу, e-mail тощо, адже у разі витоку даних вони можуть втратити доступ до всіх облікових записів. Крім того, паролі варто змінювати хоча б раз на рік, за умови, що вони відповідають зазначеним вище вимогам і не були скомпрометовані. Перевірити, чи не було витоків паролів, пов'язаних з акаунтами журналістів у соціальних мережах, можна за допомогою сервісу *https://haveibeenpwned.com/*. Якщо їхній e-mail був зафіксований серед витоків баз даних паролів, то необхідно відразу його змінити.

Особливе місце в цифровому захисті облікових записів журналістів має подвійна, або двофакторна, автентифікація. Саме вона убезпечила Українського журналіста проєкту «Схеми» Г. Шабаєва, коли зловмисники намагалися отримати доступ до його акаунта в телеграмі у лютому 2024 року. Невідомі змогли перехопити смс-повідомлення з кодом для входу в акаунт журналіста, проте саме двофакторна автентифікація завадила це зробити [1].

Подвійна, або двофакторна, автентифікація базується на використанні одразу двох різних способів підтвердження особи. У процесі такої авторизації сервіс щоразу пропонуватиме журналістам підтверджувати обома способами, що вони власники цього облікового запису. Зауважимо, що облікові записи без двоетапної перевірки не можна вважати повноцінно захищеними, однак також важливо правильно її налаштувати.

Під час входу через смартфон (через SMS, месенджер або push-повідомлення) після введення основного пароля журналістам необхідно також ввести одноразовий пароль, який буде надісланий на їхній смартфон. Якщо вони застосовують програму *«Генератор кодів»*, після введення основного пароля їм потрібно ввести спеціальний код, який генерується у відповідному додатку на смартфоні або мобільному додатку сайту. Ці коди оновлюються кожні тридцять секунд. Резервні коди слугують як запасний варіант у разі втрати основного пароля. Їх рекомендовано зберігати в паперовому форматі, наприклад, у блокноті. Цей метод допоможе у випадку втрати доступу до SIM-карти або телефону.

Якщо у журналістів виникли підозри, що до їхнього акаунта хтось отримав доступ, то необхідно зробити такі важливі кроки. Насамперед якщо вони отримали повідомлення про новий вхід у їхній акаунт, хоч самі не логінилися на новому пристрої, то важливо не панікувати й не переходити за надісланим лінком. Краще перевірити в обліковому записі, з яких пристроїв здійснено вхід в обліковий запис журналіста. Якщо вони помітили пристрої, у яких не залогінені, то варто зробити їх скриншот для подальшого розслідування цього інциденту і вилогінитися з тих пристроїв, які їм не належать. Після цього одразу слід змінити пароль.

Про зазначену вище проблему обов'язково необхідно повідомити ІТ-фахівця редакції. Варто переглянути всі налаштування безпеки облікового запису та переконатися, що вони не були змінені (наприклад, способи відновлення облікового запису, авторизовані додатки, переадресація тощо).

У разі неможливості ввійти в обліковий запис, тобто коли пароль до нього вже змінено, слід запустити процес відновлення пароля через кнопку «Я не пам'ятаю пароль». Залежно від типу облікового запису, можливо, медійникам необхідно буде підтвердження особи (так, фейсбук просить надсилати своє фото з офіційним документом). Процес відновлення доступу може тривати від кількох днів до кількох тижнів. Якщо один з облікових записів медійника було скомпроментовано, то варто перевірити безпеку інших акаунтів, а також попередити про це колег.

Висновки. Отже, цифрова безпека українських медійників під час повномасштабної війни набула особливого значення. Один із поширених видів кіберзагроз у їхній діяльності в цей період становить фішинг як спосіб зламу облікових записів (акаунтів) і незаконне заволодіння особистими даними медійників через надсилання їм повідомлень зі шкідливими лінками. Фішинг проти журналістів буває або професійно спрямованим, пов'язаним з їхньою фаховою діяльністю, або комерційним, щоб далі використовувати акаунти медійників для шахрайського заволодіння їхніми коштами та коштами інших користувачів. Щоб убезпечити себе від цього, журналістам слід застосовувати психологічні аспекти захисту (бути уважними щодо отриманих повідомлень та обачними щодо покликань у них, застосовувати правило нульової довіри, перевіряти акаунти адресантів), а також технічні аспекти цифрового захисту акаунтів (правильно обирати пароль, встановлювати двофакторну автентифікацію, застосовувати програму генерування кодів тощо).

Пропоноване дослідження здійснене в руслі аналізу однієї із кіберзагроз цифровій безпеці журналістів під час війни – фішингу. Надалі доречно буде детально з'ясувати особливості цифрової безпеки медійників у разі виникнення інших загроз, наприклад, смс-бомбінг, соціальна інженерія, шкідливе програмне забезпечення та ін.

Список літератури:

1. Герасименко Я. Журналіст-розслідувач «Схем» заявив, що його акаунт у Telegram намагалися зламати. Перехопили SMS для входу. URL: https://is.gd/PfLubs (дата звернення: 26.03.2024).
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*: матеріали Міжнар. наук.-практ. конф. (м. Рівне, 25–26 лист. 2021 р.). Рівне : Видавничий дім «Гельветика», 2021. Ч. 1. С. 210–212.
3. Земляна І. Робота під Pressom. Посібник для безпечної повсякденної роботи медійників. Інститут масової інформації. Київ, 2020. 148 с.
4. Лабораторія цифрової безпеки: річний звіт за 2020 рік. URL: https://dslua.org/publications/laboratoriia-tsyfrovoi-bezpeky-richnyy-zvit-za-2020-rik/ (дата звернення: 26.03.2024).
5. Орлова В. Російські хакери дедалі більше атакують пересічних українців: як не стати жертвою. URL: https://is.gd/tMEiEs (дата звернення: 26.03.2024).
6. Поліковська Ю. Медіаексперт розповів, чому фішинг став негативним трендом у соцмережах. URL: https://is.gd/2CIRoa (дата звернення: 26.03.2024).
7. Поліковська Ю. Шахраї розсилають фішингові повідомлення адміністратором сторінок у фейсбуці. URL: https://is.gd/IFFcal (дата звернення: 26.03.2024).
8. Посібник з безпеки для журналістів. Посібник для репортерів у небезпечних зонах. Київ: НСЖУ, 2022. 151 с.
9. Рекомендація №20: Цифрова безпека журналістів (і не тільки) в умовах війни. URL: https://is.gd/nDiVE1 (дата звернення: 26.03.2024).
10. Робейко О. Шахраї масово зламують Telegram-акаунти українців й вимагають гроші у їхніх контактів. URL: https://is.gd/4jRaZC (дата звернення: 26.03.2024).
11. Ситуація на кіберфронті станом на початок 2024 року: що потрібно знати? URL: https://is.gd/Xd86uJ (дата звернення: 26.03.2024).
12. Фішинг, паролі та sms-бомбінг: основні загрози 2021 року. URL: https://is.gd/JT14wY (дата звернення: 26.03.2024).
13. Фішингові листи приходять від нібито Суспільного. URL: https://imi.org.ua/news/fishyngovi-lysty-pryhodyat-vid-nibyto-suspilnogo-i44199 (дата звернення: 26.03.2024).
14. Цифрові загрози для журналістів та блогерів літо 2023. URL: https://imi.org.ua/infographics/tsyfrovi-zagrozy-dlya-zhurnalistiv-ta-blogeriv-lito-2023-i55771 (дата звернення: 26.03.2024).
15. Шевченко В. Трансформація професії журналіста в цифровому середовищі. Вісник Львівського університету. Серія Журналістика. 2019. Випуск 45. С. 108–116.

Tsapok O. M., Koval S. V. PHISHING PREVENTION AS PART OF THE DIGITAL SECURITY OF JOURNALISTS' ACCOUNTS IN THE WARTIMES

The article highlights the significance of digital security for journalists during the Russian war against Ukraine, as the enemy is actively conducting cyberattacks in the media. In this context, journalists' accounts may become vulnerable, so their digital protection should be paid special attention. One of the most common forms of digital threats to media accounts is phishing, whereby attackers hack into their accounts by sending them messages with malicious hypertext links.

This paper describes the types of active forms of phishing against journalists' accounts. These include hacking into their accounts for further phishing to other accounts, sending malicious messages with dangerous hyperlinks, and marking journalists' pages in messages about the alleged deactivation of these pages within 24 hours. In addition, two types of phishing against journalists are characterized. It is stated that the first is caused by and directed against their professional activities. The second is commercial phishing, used to seize media outlets' funds and illegally obtain financial revenues from other users through hacked journalist accounts.

The publication focuses on ways to prevent damage to journalists' accounts. They are differentiated into psychological and technical ones. It is emphasized that, from a psychological point of view, journalists should apply the rule of zero trust. Journalists should be attentive and cautious about received messages that may contain malicious messages, and pay attention to the addressee and the style of the received notification. On the technical side, the digital protection of media accounts from phishing is based on the correct choice of a password for the account, the uniqueness of passwords for each of the journalists' accounts, and the use of two-factor authentication. The algorithm of actions of media professionals in case of suspicion and detection of the fact of hacking their accounts is revealed. Theoretical and practical aspects of the publication are illustrated with examples from journalistic practice.

Key words: *account, digital security, hyperlink, two-factor authentication, cyberattack, zero trust, password, phishing.*