DOI 10.15276/imms.v15.no2.187
УДК 004.56

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No.2, pp. 187-195

РОЗРОБКА ВДОСКОНАЛЕНОЇ МЕТОДИКИ ОПОВІЩЕННЯ НАСЕЛЕННЯ ПРО КІБЕРІНЦИДЕНТИ

О.І. Гарасимчук, Т.А. Костишин, О.О. Любчик, М.Є. Швед

Національний університет «Львівська політехніка»
12, Степана Бандери вул., м. Львів, 79013, Україна
Emails: oleh.i.harasymchuk@lpnu.ua, tetiana.kostyshyn.kb.2021@lpnu.ua, olha.liubchyk.kb.2021@lpnu.ua, mariia.y.shved@lpnu.ua

В умовах активного впровадження цифрових технологій у суспільне життя та як наслідок зростання кількості кіберзагроз, особливо в контексті повномасштабної війни в Україні, питання ефективного інформування населення про кіберінциденти набуває критичної важливості. Традиційні засоби масової інформації не завжди здатні забезпечити необхідну швидкість та охоплення для оперативного оповіщення, що перетворює соціальні мережі та месенджери на ключові канали комунікації в сучасних умовах. У даній статті розглянуто наявні системи оповіщення населення про кіберінциденти та на основі аналізу запропоновано покращену методику донесення інформації до суспільства. Головною метою цього дослідження є розробка вдосконаленої системи оповіщення населення про кіберінциденти із використанням соціальних мереж, які на даний момент є найефективнішою платформою для швидкого поширення інформації. Дослідження доповнює наявні моделі комунікації в умовах кіберзагроз новими елементами цифрової взаємодії та підвищенням участі користувачів. Запропоновані рекомендації можуть бути застосовані державними структурами для удосконалення механізмів оповіщення за рахунок використання покращеної структури повідомлення, чат-ботів Telegram, візуалізації, інтерактивного навчання, додаткових каналів зворотного зв'язку та залучення інфлюенсерів. Подане у статті дослідження має якісний характер і базується на порівняльному аналізі інформаційних повідомлень у соціальних мережах від державних установ. У результаті дослідницької роботи запропоновано покращену модель інформування про кіберінциденти з використанням комплексного, інноваційного підходу, адаптованого до українських умов. У подальшій перспективі доцільно оцінити ефективність нової моделі після її впровадження на основі порівняння досягнутих результатів із наявними на даний момент.

Ключові слова: кіберінцидент, соціальні мережі, оповіщення, кібербезпека, комунікація.

Вступ. Зі стрімкою цифровізацією світу кібербезпека стає одним із провідних напрямків, що потребують розвитку та інвестицій, адже інформаційні технології, які тепер доступні суспільству впливають як і на кожного громадянина окремо так і на державу загалом. Разом із цим зростає й кількість кіберінцидентів – атак, шахрайств, витоків даних, що несуть загрозу як окремим користувачам, так і національній безпеці в цілому [1]. Особливо гостро ця проблема стоїть для України, що активно інтегрується у глобальний цифровий простір і водночас стикається із численними кіберзагрозами, у тому числі на фоні збройного конфлікту [2-4].

Розвитку потребують багато напрямків кібербезпеки, але один із головних для забезпечення захисту громадян державою – це вчасне і ефективне інформування населення про виникнення кіберінцидентів. Звичайні користувачі повинні володіти інформацією про загрози та дієві способи їм протидії щоб значно знизити ризики та мінімізувати негативний вплив на суспільство. Проте, часто у кризових ситуаціях ми стикаємось із реальністю, в якій традиційні засоби масової інформації такі як телебачення та інформаційні видання не можуть забезпечити необхідну швидкість оповіщення і охоплення.

Соціальні мережі та месенджери, завдяки своїй масовості, оперативності та інтерактивності, стають основними каналами комунікації для інформування громадськості у цифрову епоху. Вони дають змогу не лише швидко поширювати важливу інформацію, а й отримувати зворотний зв'язок від користувачів, що сприяє формуванню більш активної та свідомої аудиторії. Проте використання цих платформ для поширення повідомлень про кіберінциденти пов'язане з низкою викликів — від контролю якості інформації та протидії дезінформації до забезпечення конфіденційності та захисту персональних даних.

Мета дослідження. Метою даного дослідження є проаналізувати особливості подання інформації про кіберінциденти в різних соціальних мережах, що регулярно висвітлюють кіберзагрози та запропонувати покращений метод оповіщення.

Теоретичні основи дослідження. Телеграм-канал Держспецзв'язку став одним з основних джерел інформації про кібератаки на державні органи та критичну інфраструктуру України. Подача інформації тут характеризується оперативністю, офіційністю та технічною конкретикою. Як правило, повідомлення містять: (1) короткий виклад суті інциденту, (2) технічні деталі або ідентифікатори загрози, (3) посилання на додаткову інформацію (сайт CERT-UA чи офіційний веб-сайт Служби) та (4) рекомендації або заклик до дій [5].

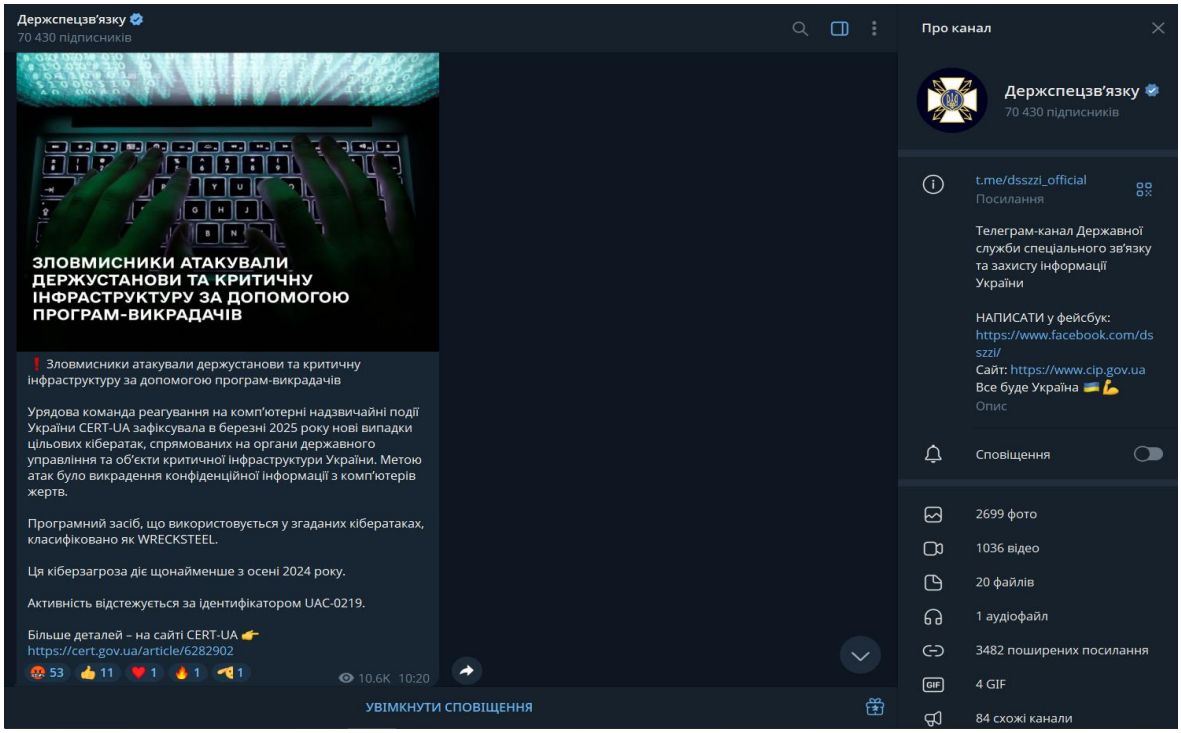

Рис. 1. Telegram-канал Держспецзв'язку

Важливим аспектом є наявність практичних порад у повідомленнях Держспецзв'язку. Часто після опису кібератаки публікуються рекомендації фахівців, як запобігти подібним атакам або зменшити їхній вплив. Канал орієнтований одразу на кілька категорій аудиторії: і на технічних спеціалістів (яким потрібні детальні кроки для захисту), і на широке коло користувачів, які можуть постраждати (їм пояснюють, куди повідомити про інцидент). Для ширшої публіки Держспецзв'язку також публікує загальні поради з кібергігієни у зручному форматі. Наприклад, окремі дописи присвячені простим правилам, як убезпечити дані на зовнішніх носіях (флешках, дисках): сканувати антивірусом, вимкнути автозапуск, не використовувати чужі носії тощо. Такі матеріали подаються списком з підкресленням ключових дій, що зручно для сприйняття.

Іншим ключовим джерелом є комунікації Кіберполіції України через Telegram, Facebook та X. Подача інформації від кіберполіції має свою специфіку: акцент на захисті громадян

від онлайн-злочинів (шахрайств, фішингу, крадіжок даних) та на результатах розслідувань кіберзлочинів. Стиль повідомлень більш прикладний, з роз'ясненнями доступною мовою, без надмірно технічних деталей – адже орієнтований на масову аудиторію користувачів Інтернету.

Під час війни кіберполіція фіксує численні випадки шахрайства, що експлуатують тему війни та волонтерства: фейкові збори коштів "на ЗСУ", фальшиві виплати постраждалим чи продаж неіснуючих товарів для військових [6]. Як тільки з'являється нова схема, правоохоронці готують попередження у соціальних мережах. Структура таких попереджень типово містить: (1) застереження-заклик до громадян бути пильними, (2) опис того, як працює схема шахраїв, (3) поради, як не стати жертвою.

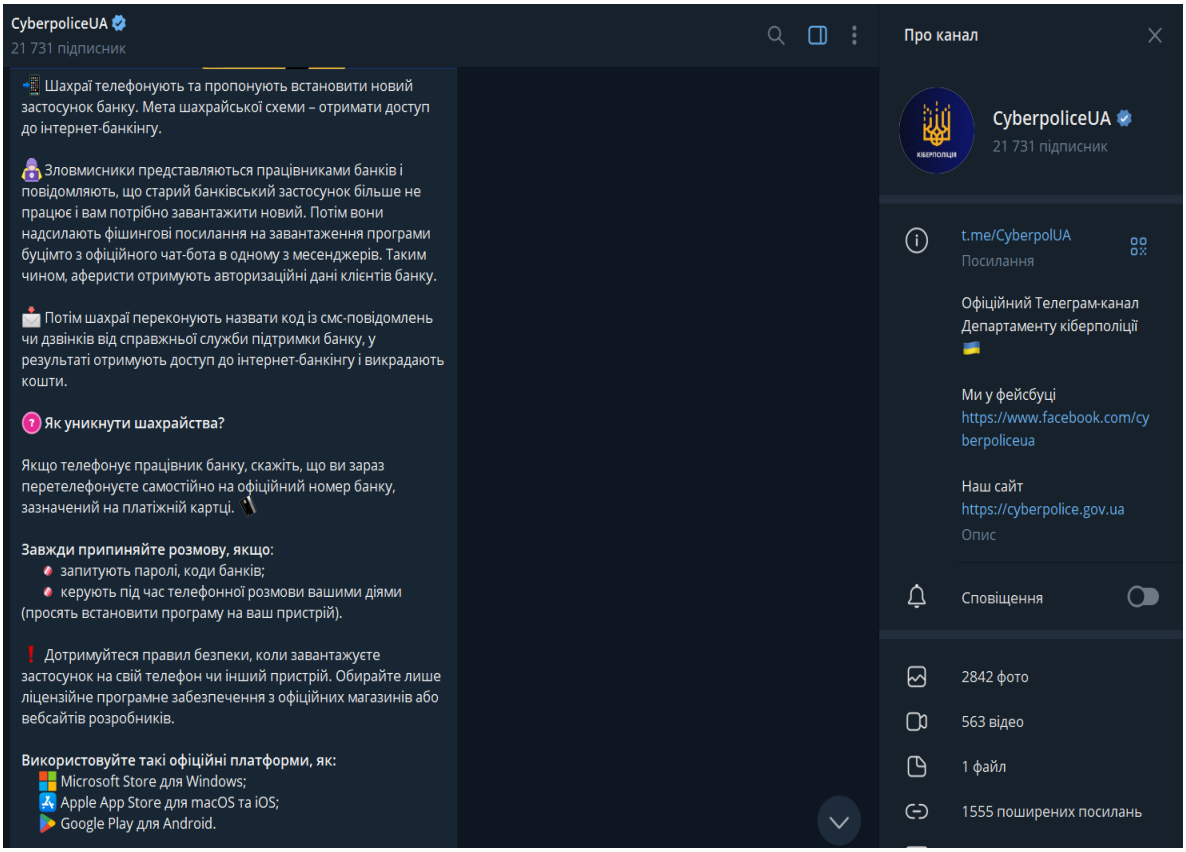

Рис. 2. Telegram-канал кіберполіції CyberpoliceUA

Кіберполіція зосереджується на безпеці простих користувачів, дає практичні поради і негайно реагує на нові шахрайські схеми, що виникають у зв'язку з війною. Завдяки соцмережам ці попередження швидко ширяться – їх підхоплюють регіональні адміністрації, ЗМІ, освітні установи, дублюючи на своїх ресурсах [7], що множить охоплення.

Варто згадати, кіберполіція також активно використовує Facebook та X для кіберпопереджень. Ці матеріали доповнюють Telegram-попередження, роблячи їх більш доступними широкій аудиторії. За рахунок поєднання різних соцмереж кіберполіція охоплює різні вікові та соціальні групи – від школярів до пенсіонерів[8-9] – і доносить до них знання про актуальні кіберзагрози воєнного часу. До прикладу, сторінка кіберполіції могла дублювати повідомлення про нові кібератаки, а користувачі Facebook та X активно ними ділилися. Однак, месенджери на кшталт Telegram все ж перевершили Facebook та X за швидкістю охоплення [10]: у Telegram люди підписані на канали і отримують миттєві сповіщення, тоді як у Facebook та X алгоритми стрічки могли показати важливе попередження із затримкою.

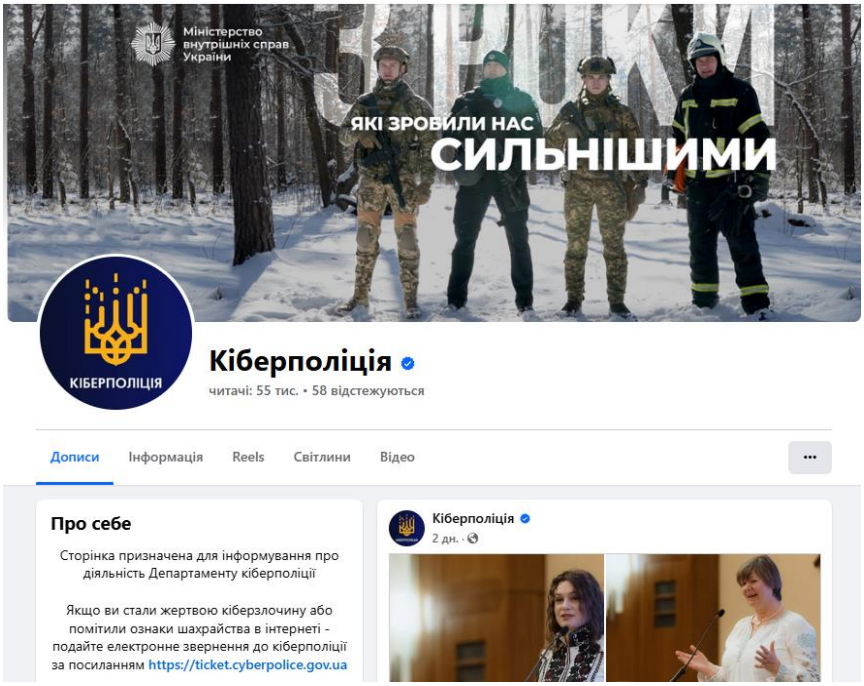

Рис. 3. Офіційна сторінка кіберполіції у Facebook

Рис. 4. Офіційна сторінка кіберполіції Cyberpolice Ukraine в X

Постановка проблеми. З початком повномасштабної війни в Україні різко зросла кількість кібератак на державні установи, критичну інфраструктуру та громадян. Оперативне інформування про такі кіберінциденти стало надзвичайно важливим, адже кібератаки можуть бути частиною гібридної війни та спричиняти дезорганізацію і паніку. ЗМІ, які ще до початку цього десятиліття вважалися головним джерелом оповіщення громадян державою, стали менш ефективними і популярними серед молоді та часто не встигають вчасно повідомляти про нові загрози або не мають достатньої технічної експертизи для детального висвітлення. Натомість соціальні мережі та месенджери стали альтернативним каналом для швидкого донесення інформації про кіберзагрози до різних аудиторій, проте цей напрямок все ще потребує розвитку.

Проблема полягає в тому, щоб проаналізувати, як саме джерела подають інформацію про кіберінциденти (швидкість, структура, наявність порад, орієнтація на аудиторію) та яким чином можна покращити ефективність роботи оповіщення населення про кіберінциденти через соціальні мережі і месенджери.

Результати та обговорення. Проте, існуючі методи інформування населення про кіберінциденти через соціальні мережі та месенджери не завжди повною мірою відповідають зростаючим вимогам користувачів. Для забезпечення своєчасного та всеосяжного інформування пропонується використання покращеної моделі оповіщення, яка має на меті інтегрувати сильні сторони існуючих практик та додати нові елементи для максимального охоплення, своєчасності та дієвості.

Пріоритезація оповіщень. Насамперед рекомендуємо запровадити інтуїтивно зрозумілу для населення класифікацію загроз, які виникають внаслідок кіберінцидентів. Вона полягатиме у поділі за пріоритетністю на червоний, помаранчевий та жовтий рівні загрози.

Таблиця 1.

Система оповіщень із пріоритезацією

Рівень Загрози	**Опис**	**Механізми Сповіщення**
Червоний	Для інцидентів із негайним, широкомасштабним впливом (наприклад, атаки на критичну банківську інфраструктуру, енергетику, державні сервіси першочергової важливості).	1. Миттєві push-сповіщення через мобільні мережі (аналогічно до сигналів повітряної тривоги, якщо технічно можливо та інфраструктурно підтримується). 2. Обов'язкові сповіщення через ключові державні та приватні мобільні додатки (наприклад, "Дія", банківські додатки, додатки комунальних служб). 3. Оповіщення через офіційні канали та чат-бот у Telegram.
Помаранчевий	Для значних загроз, що потенційно можуть мати широкий вплив або спрямовані на конкретні великі групи населення/сектори.	1. Пріоритетне розміщення на офіційних каналах у Telegram. 2. Оперативне інформування всіх ЗМІ.
Жовтий	Загальні попередження про нові схеми шахрайства, поради з кібергігієни, менш критичні технічні вразливості.	1. Публікації на офіційних сторінках у соцмережах. 2. Співпраця зі ЗМІ для регулярних рубрик.

Відповідно до поданої інформації про рівень загрози користувачі зможуть швидко оцінити важливість повідомлення, що надійшло.

Покращена структура повідомлення. Для того, щоб оперативно та результативно інформувати населення про кіберінциденти в соціальних мережах рекомендуємо

дотримуватися чіткої структури повідомлення. Таке повідомлення повинне включати наступні обов'язкові елементи (рис.5).

Рис. 5. Покращена структура повідомлення

Дотримання наведеної структури забезпечує ефективне інформування про кіберінциденти, що зменшує рівень паніки серед населення і підвищує загальний рівень обізнаності щодо поточних кіберризиків.

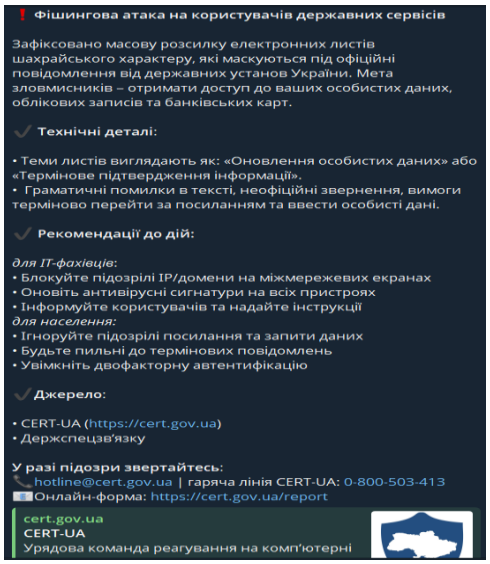

Рис. 6. Приклад повідомлення відповідно до запропонованої покращеної структури

Чат-бот в Telegram для персоналізації. Щоб забезпечити комфортні умови користувачам і дати їм можливість отримувати лише актуальні особисто для них загрози, можна створити окремий чат-бот у Telegram (як ключовому каналі для миттєвого поширення інформації). Він забезпечить механізм вказування особою її сфер інтересів, до прикладу, "IT-фахівець", "батько/мати", "власник бізнесу", "частий відвідувач пошти", "частий пасажир укрзалізниці", "клієнт певного банку" чи "користувач певного мобільно оператора". Завдяки цьому користувачі отримуватимуть попередження, що

враховують специфіку їхньої діяльності та вразливості, з якими вони найімовірніше можуть зіткнутися.

Для швидкого аналізу нових загроз, ідентифікації потенційно вразливих груп населення та автоматизованої адаптації рекомендацій для різних категорій користувачів можна застосувати штучний інтелект. Окрім того, ШІ можна використати для формулювання чітких, зрозумілих інструкцій різними мовами, що суттєво підвищить ефективність комунікації та рівень довіри серед усіх верств населення.

Додатковий спрощений механізм зворотного зв'язку. Ми пропонуємо інтегрувати кнопку "Повідомити про кіберінцидент" у “Дію”, яка є основним мобільним додатком України. Це дозволить громадянам швидко та легко звертатися до Кіберполіції, Держспецзв’язку або CERT-UA, що не лише пришвидшить реагування на інциденти, але й створить у громадян відчуття залученості та партнерства у забезпеченні національної кібербезпеки.

Інтерактивне навчання. В умовах стрімкого зростання кількості та складності кіберзагроз ключовим елементом модернізованої стратегії оповіщення про кіберінциденти стає впровадження інтерактивного навчання з питань кібербезпеки.

Пріоритетним напрямком діяльності стане впровадження інтерактивних навчальних кампанії через доступні цифрові канали. Громадян можна залучити до квізів, симуляцій фішингових атак та навчальних ігор через мобільні додатки та освітні платформи. Систематичне проведення вікторин і тестів у соцмережах та через чат-боти з елементами гейміфікації (рейтинги, досягнення, винагороди) стимулюватиме користувачів регулярно вдосконалювати знання з кібергігієни у захоплюючій формі.

Прямі ефіри з фахівцями Держспецзв'язку та Кіберполіції дозволять громадянам отримувати кваліфіковані консультації та підвищують довіру до державних інституцій. Запроваджена система анонімного збору інформації про підозрілі кіберінциденти від користувачів з подальшим експертним аналізом та публікацією рекомендацій забезпечить оперативне реагування на нові вектори атак.

Візуальний контент. Більш зрозумілим для звичайних користувачів способом донесення інформації є візуальний контент, і хоча його важче створити ніж звичайне текстове повідомлення, та він може значно підвищити ефективність оповіщення. До інструментів візуалізації відносять наприклад: інфографіку та короткі анімовані відеоролики. За рахунок більшої привабливості та пояснення на прикладах можна досягти більших охоплень і зацікавлення аудиторії в захисті від кіберзагроз.

Рис. 7. Постер у форматі інфографіки, для Telegram-каналу кіберполіції

Залучення інфлюенсерів та лідерів думок. Ефективність оповіщення про кіберінциденти значною мірою залежить від охоплення аудиторії та рівня довіри до поширюваної інформації. З метою розширення аудиторії рекомендуємо співпрацювати з громадськими діячами, популярними блогерами, а також місцевими лідерами. Це дозволить підвищити довіру до офіційних повідомлень і рекомендацій.

Також доцільним є розповсюдження інформації через великі регіональні та тематичні групи у Facebook, Telegram-канали ОСББ, батьківські чати та інші подібні об'єднання, оскільки це дозволить донести релевантну інформацію до цільових груп користувачів, враховуючи їхні специфічні потреби та контекст.

Висновки. Представлена вдосконалена модель інформування суспільства про кіберінциденти дозволить забезпечити вищу оперативність розповсюдження повідомлень на більш широку аудиторію. Вона забезпечить прямі сповіщення через мережу та інтеграцію з інформаційними системами ЗМІ, що дозволить досягнути швидшого донесення даних порівняно з традиційними способами інформування.

Пріоритезація та персоналізація оповіщень з цільовими рекомендаціями зробить повідомлення більш релевантними і ефективніше спонукатиме користувачів до конкретних дій. Водночас диверсифікація каналів комунікації знизить залежність від одного джерела, що підвищить загальну стійкість системи. Активне залучення користувачів через інтерактивні формати сприятиме кращому засвоєнню інформації і формуванню культури кібербезпеки. Залучення інфлюенсерів та спільнот допоможе значно розширити охоплення аудиторії, а чіткі інструкції і спрощені механізми повідомлення про інциденти дадуть змогу громадянам швидше реагувати на кіберзагрози.

Отже, комплексний підхід до інформування через соціальні мережі і месенджери дозволить створити більш оперативну, надійну і довірену систему комунікації, яка є важливою складовою зміцнення кібербезпеки України в сучасних умовах.

Список літератури

1. Гайдук О. В., Звєрєв В. П. Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій. *Кібербезпека: освіта, наука, техніка.* 2024. Т.3, №23. С. 225-236.
2. Ciekanowski Z, Żurawski S. Cyber Threat Analysis (CTA) in Current Conflicts. *IgMin Research*. 2024. Т.2 №4. С. 224-227.
3. Никончук Н.С., Маслова О.О. Кіберзлочинність в Україні: виклики сучасності. *Юридичний науковий електронний журнал*. 2021. №9. 202-205.
4. Худолій А. О. Кібербезпека: сучасні виклики перед Україною. *Acta De Historia & Politica: Saeculum XXI*. 2020. С. 138–146.
5. Держспецзв'язку. Атака на «Укрзалізницю» була актом кібертероризму. URL: https://glavcom.ua/country/incidents/ataka-na-ukrzaliznitsju-bula-aktom-kiberterorizmu-derzhspetszvjazku--1052297.html
6. Sud.ua. Онлайн-шахрайство під час війни: як захистити себе від фінансових втрат. URL: https://sud.ua/uk/news/ukraine/299885-onlayn-moshennichestvo-vo-vremya-voyny-kak-zaschitit-sebya-ot-finansovykh-poter#google_vignette
7. Brody-Освіта. Кіберполіція попереджає про шахрайство. Будьте обережні. URL: https://brody-osvita.gov.ua/kiberpoliciya-poperedzhae-13-35-49-21-06-2023/#
8. Провсе. Telegram, YouTube, Facebook, TikTok, Viber, Instagram чи Twitter: звідки українці дізнаються новини? URL: https://provse.te.ua/2024/08/telegram-youtube-facebook-tiktok-viber-instagram-chy-twitter-zvidky-ukraintsi-diznaiutsia-novyny/
9. Опора: найпопулярнішими соцмережами в Україні є телеграм, ютуб та фейсбук. URL: https://ms.detector.media/sotsmerezhi/post/35557/2024-07-16-opora-naypopulyarnishymy-sotsmerezhamy-v-ukraini-ie-telegram-yutub-ta-feysbuk/

10. Данько-Сліпцова А. А. Особливості Telegram як інтернет-платформи поширення соціально значущої інформації. *Український інформаційний простір*. 2023. Т.2 №12. С. 275-286 URL: http://ukrinfospace.knukim.edu.ua/article/view/291193

DEVELOPMENT OF AN IMPROVED METHODOLOGY FOR NOTIFYING THE PUBLIC ABOUT CYBER INCIDENTS

O.I. Harasymchuk, T.A. Kostyshyn, O.O. Liubchyk, M.E. Shved

Lviv Polytechnic National University
12, Stepan Bandera St., Lviv, 79013, Ukraine
Emails: oleh.i.harasymchuk@lpnu.ua, tetiana.kostyshyn.kb.2021@lpnu.ua,
olha.liubchyk.kb.2021@lpnu.ua, mariia.y.shved@lpnu.ua

In the context of the active implementation of digital technologies into public life and the consequent rise in the number of cyber threats, especially amidst the full-scale war in Ukraine, the issue of effectively informing the public about cyber incidents acquires critical importance. Traditional mass media are not always able to provide the necessary speed and reach for timely notification, making social networks and messengers key communication channels under current conditions. This article examines existing public notification systems for cyber incidents and, based on an analysis, proposes an improved methodology for disseminating information to the public. The main goal of this research is to develop an improved system for notifying the public about cyber incidents using social networks and messengers, which are currently the most effective platforms for rapid information dissemination. The research complements existing communication models in the context of cyber threats with new elements of digital interaction and increased user participation. The proposed recommendations can be applied by state structures to improve notification mechanisms through the use of an improved message structure, Telegram chatbots, visualization, interactive learning, additional feedback channels, and the involvement of influencers. The research presented in the article is qualitative in nature and is based on a comparative analysis of informational messages on social networks from state institutions. As a result of the research work, an improved model for informing about cyber incidents has been proposed, using a comprehensive, innovative approach adapted to Ukrainian conditions. In the future, it is advisable to evaluate the effectiveness of the new model after its implementation based on a comparison of the achieved results with those currently available.
Keywords: cyber incident, social networks, notification, cybersecurity, communication.