УДК 351/354:621.395.97:004.738.5.057.4
DOI 10.36030/2310-2837-1(100)-2021-40-45

ЦИФРОВІ СЕРВІСИ ОБМІНУ МИТТЄВИМИ ПОВІДОМЛЕННЯМИ В ПУБЛІЧНОМУ УПРАВЛІННІ: СУТНІСТЬ, КЛАСИФІКАЦІЯ ТА КІБЕРБЕЗПЕКА

А. С. Осьмак,
Київський національний економічний університет імені Вадима Гетьмана

У статті визначено сутність сучасних систем цифрових комунікацій у публічному управлінні. Проведено фактологічний аналіз сучасних засобів цифрових комунікацій та їх використання в діяльності органів публічної влади. Удосконалено структурні підходи до типізації комунікативної підсистеми публічного управління. Визначено, що основою управління інформацією є інформаційно-комунікаційний менеджмент, який базується на стратегії управління інформацією. Запропоновано класифікацію сервісів миттєвих повідомлень за основними функціями. Розглянуто вплив пандемії COVID-19 на зміну ландшафту цифрових комунікацій та проблематику кібербезпеки цифрових повідомлень. Запропоновано систему критеріїв вибору засобу цифрових комунікацій за сферою використання.
Ключові слова: публічне управління; цифрові комунікації; миттєві повідомлення; месенджери; кібербезпека; відеоконференції; голосові сервіси; цифрові трансформації; COVID-19.

DIGITAL INSTANT MESSAGING SERVICES IN PUBLIC ADMINISTRATION: ESSENCE, CLASSIFICATION AND CYBERSECURITY

A. S. Osmak,
Kyiv National Economic University named after Vadym Hetman

The article defines the essence of modern digital communication systems in public administration. A factual analysis of modern means of digital communications and their use in the activities of public authorities. Structural approaches to the typification of the communicative subsystem of public administration have been improved. It is determined that the basis of information management is information and communication management, which is based on information management strategy. The classification of instant messaging services according to the main functions is offered. The impact of the COVID-19 pandemic on the change of the digital communications landscape and the issues of cybersecurity of digital communications is considered. A system of criteria for choosing a means of digital communications by field of application is proposed.
Keywords: public administration; digital communications; instant messaging; messengers; cybersecurity; video conferencing; voice services; digital transformations; COVID-19.

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими та практичними завданнями. З розвитком цифрових технологій усе більшого поширення набувають системи персональних та групових (корпоративних) цифрових комунікацій. На зміну класичним технічним засобам комунікації – системам дротової та мобільної телефонії та радіозв'язку – приходять системи обміну миттєвими повідомленнями (месенджери). Відбулася зміна парадигми суспільних комунікацій, що дало суттєвий поштовх до розвитку цифровізації комунікативних відносин, у тому числі й у сфері публічного управління, що потребує нових підходів у виборі ефективних технічних рішень та врахування проблеми їхньої кібербезпеки. Крім того, всесвітня пандемія COVID-19 та викликані нею карантинні обмеження змінили глобальний комунікативний ландшафт та підходи до використання цифрових сервісів.

Аналіз останніх публікацій за проблематикою та визначення невирішених раніше частин загальної проблеми. Проблематика цифрових трансформацій галузі публічного врядування стала об'єктом досліджень багатьох зарубіжних і українських учених. Так, на нашу думку, варто згадати про ґрунтовний науковий доробок С. Бремена та Д. Креіса, П. Данлеві, Х. Маргетс, С. Бастоу та Дж. Тінклер, А. Вільямса та Х. Хей, А. Антохова, В. Бунь, В. Дрешпака, Г. Почепцова, В. Наместнік, О. Карпенка. Авторами в попередніх дослідженнях уже розглядались як імперативи реалізації цифрового врядування в Україні, так і питання цифрових комунікацій в органах публічної влади (Цифрове врядування, 2020, с. 94–120), натомість невирішеною частиною загальної про-

блеми дослідження залишається наукове питання обґрунтування механізмів упровадження засобів цифрових комунікацій у діяльність органів публічного управління.

Мета статті полягає в науково-теоретичному обґрунтуванні сутності, класифікації, аналізі переваг та прогнозуванні можливих ризиків застосування технологій цифрової комунікації в різних сферах галузі публічного управління в Україні.

Виклад основного матеріалу. Комунікативна підсистема публічного управління охоплює: суб'єкти взаємодії, інформаційні зв'язки, управлінські відносини, процеси взаємодії суб'єктів управління між собою та з іншими суспільними інститутами. До неї також належить інфраструктура, яка забезпечує творення, передавання, пошук і отримання управлінської інформації. Ключовими функціями такої підсистеми є: забезпечення інформаційних обмінів, репрезентації та легітимації системи публічного управління, а також забезпечення цілеспрямованого управлінського впливу (Дрешпак, 2015, с. 11).

Розвиваючи запропоновані раніше структурні підходи до типізації комунікативної підсистеми публічного управління на основі елементів взаємодії (Дрешпак, 2015, с. 12; Бірюков, Лещенко, 2016, с. 155) та складові, які в процесі цифрових комунікацій формують її структуру, можна виокремити дві базові складові, до яких, у свою чергу, входять елементи нижчого рівня:

– вербально-семантична складова, до якої належать: відправник як суб'єкт комунікацій, який формулює повідомлення; повідомлення (інформація в знаковій, вербальній чи іншій формі, яку передає відправник), реципієнт (одержувач, якому спрямоване повідомлення), сприйняття (розуміння реципієнтом повідомлення); зворотний зв'язок (реакція реципієнта на повідомлення);

– технічно-транспортна складова, до якої входить множина технічних та програмних засобів, які забезпечують процеси введення, кодування, шифрування і дешифрування (за потреби), декодування, передачі й відтворення (відображення) повідомлення, а також канали зв'язку, які забезпечують транспортування повідомлення від відправника до реципієнта (реципієнтів).

Варто зауважити, що вербально-семантична складова є сталою за структурою та змістом. Водночас множина елементів технічно-транспортної складової постійно розвивається і вдосконалюється, пропонуючи нові технологічні підходи й технічні рішення. Крім того, розвиток технологій та все ширше впровадження систем штучного інтелекту (ШІ) переводять процеси, які реалізуються вербально-семантичною складовою комунікативної підсистеми публічного управління, на рівень технічно-транспортної складової, коли функції суб'єкта комунікації повністю або частково бере на себе штучний інтелект, який може виступати джерелом повідомлення або виконувати допоміжні вербальні та невербальні завдання, наприклад формування зворотного зв'язку на запит на основі масивів даних, переклад або трансляцію повідомлення відправника тощо.

Для забезпечення повноцінної діяльності комунікативної підсистеми публічного управління має застосовуватися стратегія управління інформацією (Information governance, IG), яка регулює процеси та принципи керування інформацією й даними на основі нормативно-правового забезпечення, урівноважує ризики, які становить інформація, із цінністю, яку інформація надає (Lomas, 2010). Стратегія управління інформацією охоплює: інформаційно-комунікаційний менеджмент, інформаційну безпеку, захист даних та кібербезпеку, управління даними, управління ризиками, конфіденційність, зберігання та архівування даних, управління знаннями, аудит, аналітику тощо.

Основою управління інформацією є інформаційно-комунікаційний менеджмент – система управління інформаційно-комунікаційною сферою суспільства на основі використання форм, методів і технологій правового, економічного, соціального, гуманітарного та політичного менеджменту і маркетингу (Будзан, 2011, с. 26), яка за допомогою інтегрованої комунікації з цільовими аудиторіями сприяє досягненню ефективності комунікаційної діяльності органів публічної влади в умовах мінливого зовнішнього середовища та спрямована на оптимізацію, досягнення ефективної міжсуб'єктної взаємодії, обміну повідомленнями/смислами всередині самих органів влади, а також між органами влади й зовнішнім середовищем.

Метою інформаційно-комунікаційного менеджменту є створення ефективного комунікаційного простору (сукупності суб'єктів, їхніх зв'язків та умов реалізації цих зв'язків) для досягнення цілей і завдань органу влади, отримання позитивного відгуку за умов мінімальних комунікативних втрат. Інформаційно-комунікаційний менеджмент базується на організації, плануванні та управлінні процесами комунікацій, їхньому контролі та оцінюванні ефективності. Ефективною можна вважати таку комунікацію, за якої відносини отримувача та відправника повідомлення є взаємно позитивними, інформаційні шуми мі-

німально викривлюють сенс повідомлення, воно максимально правильно сприйняте, відбулися очікувані зміни в знаннях отримувача, а його поведінка змінилася в заданому напрямі.

Нині одним із найефективніших комунікативних інструментів органів публічної влади є електронні (цифрові) комунікації (телекомунікації), які згідно із законодавством України (Про електронні комунікації, 2015), визначаються як процес передавання та/або приймання інформації, незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій та до яких належать: електронна пошта; пошукові системи; електронні засоби навчання й освіти; засоби масової інформації в мережі «Інтернет»; електронна комерція; інтернет-банкінг; послуги електронного урядування; соціальні мережі та сервіси обміну повідомленнями; голосові та відеоз'єднання.

Серед засобів цифрових комунікації, у тому числі й у сфері публічного управління, найбільш вживаними є саме системи обміну миттєвими цифровими повідомленнями (Instant messaging, IM) – телекомунікаційний цифровий сервіс для обміну текстовими, голосовими, відео- та іншими повідомленнями між цифровими пристроями користувачів через цифрові комп'ютерні мережі.

Найбільшого поширення сервіси миттєвих цифрових повідомлень набули серед мобільних обчислень. Згідно з останніми дослідженнями, обмін миттєвими повідомленнями є найбільш затребуваними сервісами. Частка використання серед усіх мобільних додатків належить саме клієнтам миттєвих повідомлень. Так, додатком Viber користується 96,8 %, Facebook Messenger – 72,3 %, Telegram – 76,8 %, WhatsApp – 42,2 % (Жиленко, 2021). Водночас варто зазначити, що загальний показник проникності мережі «Інтернет» в Україні, за даними початку 2021 р., становить 67,6 % (Kemp, 2021), з яких 66 % – регулярні користувачі мобільними обчисленнями (Дубинський, 2019).

Особливістю систем обміну миттєвими повідомленнями є робота в режимі реального часу, коли зв'язок між користувачами утримується постійно і відправлене повідомлення одразу передається користувачу. Якщо для обміну такими повідомленнями використовується мережа загального користування, для здійснення комунікації застосовується клієнтська програма – месенджер, за допомогою якого також може здійснюватися груповий обмін повідомленнями між декількома співрозмовниками (конференція, чат) та масове розсилання повідомлення учасниками мережі за певною ознакою або попередньою реєстрацією на такі дії.

Система миттєвих повідомлень працює за певним серверним або безсерверним протоколом доступу – набором правил представлення і кодування даних, передачі сигналів та ідентифікації помилок, необхідним для обміну інформацією. Серверний протокол передбачає підключення до центрального сервера мережі обміну повідомленнями. Месенджери в такій системі є клієнтами. У безсерверних протоколах (FChat, NASSI, UChat) повідомлення передаються безпосередньо від одного співрозмовника до іншого за принципами децентралізованої, або пірингової (англ. Peer-to-peer, P2P – рівний до рівного) мережі – оверлейної цифрової мережі, що ґрунтується на рівноправ'ї учасників. Часто в такій мережі відсутні виділені сервери, а кожен вузол є як клієнтом, так і виконує функції сервера. Системи обміну миттєвими повідомленнями можуть функціонувати як окремі програмні продукти, так і використовуватись як комунікативні інструменти в складі інших програмних продуктів. Окремо слід виділити апаратні та програмно-апаратні месенджери, які можуть здійснювати обмін як текстовими повідомленнями, так і іншими даними (телеметрія, GPS-мітки) на рівні пристроїв як за серверним (пейджинг, смсповідомлення), безсерверними (DMR, dPMR), так і за змішаними протоколами (DMR, APCO P25, TETRA, LTE D2D).

Системи обміну миттєвими повідомленнями можна класифікувати за основними функціональними носіями інформаційного змісту:

– клієнти для обміну текстовими повідомленнями;

– клієнти для обміну графічними повідомленнями;

– клієнти для обміну голосовими повідомленнями;

– клієнти для обміну відеоповідомленнями.

Такі системи можуть виконувати свої функції як для персональних, так і для групових та масових комунікацій. Сучасні клієнти для обміну миттєвими повідомленнями здебільшого є універсальними та можуть надавати комплексні сервіси, які повністю або частково охоплюють зазначені функціональні носії. Так, базовою функцією для класичних месенджерів (ICQ, IRC, MyChat, WeChat, QQ, Snapchat, Discord, Line, Facebook Messenger, Telegram, WhatsApp тощо) є обмін текстовими та графічними повідомленнями, програмне забезпечення для інтернет-телефонії VoIP (voice over IP – голос через IP) (Jami, Rakuten Viber, Microsoft Skype, Tviggo, Tango, TeamSpeak, JustVoip, Zello тощо) насамперед призначене для обміну голосовими повідомленнями, а систе-

ми відеоконференцій (Zoom Meeting, Microsoft Teams, Google Meet Cisco Webex Meetings, Slack, GoToMeeting, CyberLink U Meeting, BlueJeans, Lifesize, FreeConference, Starleaf тощо) – для групових відеокомунікацій. Сучасний розвиток технологій вказує на те, що функціональними носіями інформаційного змісту можуть стати також системи нейрокомунікації, побудовані на основі нейрокомп'ютерних інтерфейсів невербального обміну інформацією та впливу.

Запроваджені карантинні обмеження та політика соціальної дистанції, викликані всесвітньою пандемією COVID-19 (SARS-CoV-2), спричинила масовий перехід від прямих вербальних комунікацій до повсюдного використання цифрових комунікаційних інструментів. Відеоконференції стали альтернативою безпосередньому спілкуванню, у тому числі й у сферах публічного управління, освіти, науки, бізнесу на основі як окремих програмних засобів, таких як Zoom, Microsoft Teams, Google Meet та інших, так і розширених відеофункцій у класичних месенджерах – Facebook Messenger, WhatsApp, Viber, Microsoft Skype тощо. Активне використання систем відеоконференцій продемонструвало, що така функція є подекуди надлишковою, оскільки основне смислове навантаження несе саме вербальна комунікація.

Так, запущений у 2020 р. сервіс Clubhouse – соціальна мережа, що ґрунтується виключно на масових вербальних комунікаціях із використанням технології VoIP – став поштовхом до масового розвитку голосових мереж для групових трансляцій у режимі реального часу, створення яких уже анонсували Telegram, Facebook, Twitter, Stereo App Ltd тощо.

Однією з проблем месенджерів є захист інформації користувачів. Варто зазначити, що здебільшого вся критична інформація наведена на стороні розробника і, цілком імовірно, може стати мішенню для хакерів і спецслужб (Веремєєва, 2019). Ціллю кібератак є зміст повідомлень, приватні та персональні дані тощо. Нині розробники месенджерів масово використовують наскрізне шифрування (end-to-end encryption, E2EE) – спосіб передачі даних, у якому доступ до повідомлень мають тільки користувачі, які беруть участь у спілкуванні, що не дає змоги отримати доступ до криптографічних ключів третім особам (Proton Team, 2020). Водночас Zoom використовує також 256-бітне шифрування AES, що забезпечує додатковий захист даних та більшу стійкість до зломів.

Так, для запобігання кібератакам у 2016 р. Rakuten Viber увів наскрізне шифрування повідомлень і розмов, проте варто враховувати ризики, пов'язані з тим, що частина серверів Viber розміщена на території РФ (Полякова, 2017). Доступна інформація і про інші уразливості, які були виявлені в масових месенджерах. Так у WhatsApp було виявлено слабке місце в сервісі інтернет-телефонії, яке давало змогу інфікувати смартфони через інтернет-дзвінок (Губенко, 2019). У 2019 р. була виявлена уразливість у месенджері Signal, яка давала можливість отримати доступ до мікрофона та здійснити аудіовиклик без відома користувача (Silvanovich, 2019), а у 2020 р. – уразливість Facebook Messenger, яка давала змогу атакуючому здійснювати аудіовиклики й підключатися до вже активних дзвінків без відома абонентів (Нефедова, 2020). У Telegram виявлена уразливість, яка допускає створення підробленого профілю, який маскується під функцію «Вибране» («Saved Messages»), яку користувачі використовують для зберігання важливої інформації, включаючи фотографії та паролі (Касми, 2020). Також були виявлені серйозні уразливості в клієнті для відеоконференцій Zoom, використовуючи які зловмисники могли викрадати персональні дані користувачів (Lawrence, 2020).

У діяльності інформаційно-комунікаційного менеджменту органів публічної влади постає питання визначення номенклатури програмних засобів для обміну миттєвими повідомленнями для створення ефективного комунікативного простору. Для цього насамперед варто визначити сферу комунікативної діяльності для вирішення конкретних завдань – публічні чи внутрішні (корпоративні) комунікації.

У випадку публічних комунікацій основною метою є максимальна доступність та аудиторія реципієнтів, що передбачає застосування масових програмних продуктів (застосунків) для обміну миттєвими повідомленнями з найвищим відсотком охоплення серед користувачів (споживачів інформації).

Водночас для внутрішніх (корпоративних) комунікацій першочерговим є перелік вимог, які ставить внутрішня політика управління інформаційно-комунікаційною підсистемою конкретного органу публічної влади, зокрема кіберзахист, використання спеціальних захищених каналів інформації, інтеграція з іншими програмними продуктами тощо. Так, згідно із внутрішньою корпоративною політикою для забезпечення кібербезпеки Єврокомісія рекомендувала своїм співробітникам перейти на месенджер Signal та анонсувала розробку власного месенджера (Fanta, 2020). Водночас, ураховуючи інформаційні ризики, уряд Німеччини повідомив про перехід на комунікаційне програмне забезпечення компанії Wire Swiss GmbH, а

міністерство оборони Німеччини (бундесвер) повідомило про тестове використання сервісів для обміну миттєвими повідомленнями Stashcat та BW Messenger (Gebauer, 2020).

Висновки та пропозиції щодо подальших досліджень. Стрімкий розвиток цифровізації, нові технологічні підходи й технічні рішення постійно змінюють як технічно-транспортну складову комунікативної підсистеми публічного управління, так і комунікативний ландшафт загалом. З огляду на це в умовах цифрових трансформацій для забезпечення повноцінної комунікативної взаємодії та створення ефективного комунікаційного простору виникає потреба в ефективному управлінні інформацією. Тому для організації, планування й управління процесами комунікацій, контролю та оцінювання ефективності комунікативної діяльності вважаємо за доцільне впровадження інформаційно-комунікаційного менеджменту як системи управління інформаційно-комунікаційною сферою органів публічної влади.

Одним із пріоритетних напрямів підвищення ефективності роботи та забезпечення ефективної комунікативної взаємодії органів публічної влади в реальному часі як для внутрішніх взаємозв'язків, так і в процесі зовнішніх комунікацій має стати повсюдне застосування систем обміну миттєвими повідомленнями. Проте в процесі деталізації оптимальної номенклатури програмних засобів, які мають використовуватись для обміну миттєвими повідомленнями органами публічної влади, варто враховувати сферу їх застосування (зовнішні або внутрішні комунікації), функціональні особливості, у тому числі за типом носіїв інформаційного змісту та протоколом доступу, а також кібербезпекові ризики та загрози.

Подальші наукові дослідження варто спрямувати на вивчення світового досвіду щодо механізмів упровадження цифрових трансформацій у сфері публічного управління та місцевого самоврядування, зокрема на використання в інформаційно-комунікаційних системах органів публічної влади засобів цифрових комунікацій, з огляду на питання кібербезпеки, у тому числі в умовах поширення COVID-19.

Список використаних джерел

Fanta A. EU diplomats to use mystery app for secure messaging. *netzpolitik.org, 27.02.2020*. URL: https://netzpolitik.org/2020/eu-diplomats-to-use-mystery-app-for-secure-messaging/

Gebauer M., Rosenbach M. Bundesregierung setzt verstärkt auf verschlüsselnde Messenger-Apps. *Spiegel, 03.04.2020.* URL: https://www.spiegel.de/netzwelt/apps/coronakrise-bundesregierung-setzt-verstaerkt-auf-verschluesselte-messenger-apps-a-67dece1c-fd11-41fc-bd5a-cba1e7788535.

Kemp S. Digital 2021: Ukraine. 12 February 2021. URL: https://datareportal.com/reports/digital-2021-ukraine

Lawrence A. Zoom Lets Attackers Steal Windows Credentials, Run Programs via UNC Links. *BleepingComputer.* March 31, 2020. URL: https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/.

Lomas, E. (2010). Information governance: information security and access within a UK context. *Records Management Journal.* Vol. 20. N 2. URL: https://doi.org/10.1108/09565691011064322

Proton T. What is end-to-end encryption and how does it work? *ProtonMail.* March 7, 2018. URL: https://protonmail.com/blog/what-is-end-to-end-encryption/

Silvanovich N. Incoming call can be connected without user interaction. Sep. 28, 2019. URL: https://bugs.chromium.org/p/project-zero/issues/detail?id=1943

Бірюков Д. С., Лещенко О. Я. Досвід комунікацій у сфері цивільного захисту в Україні: політичні аспекти. *Запровадження комунікації органів державної влади :* зб. матеріалів наук.-практ. конф. / упоряд. А. В. Баровська. Київ : Фенікс, 2016. 192 с. URL: https://niss.gov.ua/sites/default/files/2016-06/Verstka_ost_ispr-2eea8.pdf

References

Fanta, A. (2020). EU diplomats to use mystery app for secure messaging. *Netzpolitik.org*. Retrieved from: https://netzpolitik.org/2020/eu-diplomats-to-use-mystery-app-for-secure-messaging/

Gebauer, M., Rosenbach, M. (2020). Bundesregierung setzt verstärkt auf verschlüsselnde Messenger-Apps. *Spiegel.* Retrieved from: https://www.spiegel.de/netzwelt/apps/coronakrise-bundesregierung-setzt-verstaerkt-auf-verschluesselte-messenger-apps-a-67dece1c-fd11-41fc-bd5a-cba1e7788535.

Kemp, S. (2021). Digital 2021: Ukraine. 12 February. Retrieved from: https://datareportal.com/reports/digital-2021-ukraine

Lawrence, A. (2020). Zoom Lets Attackers Steal Windows Credentials, Run Programs via UNC Links. *BleepingComputer.* March 31. Retrieved from: https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/.

Lomas, E. (2010). «Information governance: information security and access within a UK context». *Records Management Journal*. Vol. 20. N 2. Retrieved from: https://doi.org/10.1108/09565691011064322

Proton, T. (2018). What is end-to-end encryption and how does it work? *ProtonMail.* March 7. Retrieved from: https://protonmail.com/blog/what-is-end-to-end-encryption/

Silvanovich, N. (2019). Incoming call can be connected without user interaction. Sep. 28. Retrieved from: https://bugs.chromium.org/p/project-zero/issues/detail?id=1943

Biriukov, D. S, Leshchenko, O. Ia. (2017). Dosvid komunikatsii u sferi tsyvilnoho zakhystu v Ukraini: politychni aspekty. *Zaprovadzhennia komunikatsii orhaniv derzhavnoi vlady :* zb. mat-liv nauk.-prakt. konf. Kyiv : Feniks, 2016. 192 p. Retrieved from: https://niss.gov.ua/sites/default/files/2016-06/Verstka_ost_ispr-2eea8.pdf

Будзан Б. Менеджмент в Україні: сучасність і перспективи. Київ : Основи, 2011. 349 с.

Веремєєва Т. Месенджери в Україні: основні гравці, проблеми та перспективи. *Comments.* 2019. 9 груд. URL: https://comments.ua/article/it/technology/641679-messendzhery-v-ukraine-osnovnye-igroki-problemy-i-perspektivy.html

Губенко Д. Через WhatsApp смартфони інфікували шпигунською програмою. *Deutsche Welle.* 2019. 14 трав. URL: https://www.dw.com/uk/через-whatsapp-смартфони-інфікували-шпигунською-програмою/a-48727010

Дрешпак В. М. Комунікації в публічному управлінні : навч. посіб. Київ : ДРІДУ НАДУ, 2015. 168 с. URL: http://biblio.umsf.dp.ua/jspui/bitstream/123456789/3136/1/Комуніації в публічному управлінні.pdf

Дубинський І. Проникнення інтернету в Україні. *InMind Factum Group Ukraine.* 2019. Жовт. URL: https://inau.ua/sites/default/files/file/1910/ dani_ustanovchyh_doslidzhen_iii_kvartal_2019_roku.pdf

Жиленко Д. Рейтинг мобільних додатків за січень 2021. *Kantar Україна.* URL: https://tns-ua.com/news/reyting-mobilnih-dodatkiv-za-sichen-2021

Про електронні комунікації : Закон України від 03.09.2015 № 675-VIII. *Офіц. вісн. України.* 2021. 26 січ. № 6. С. 10, ст. 306, код акта 102665/2021. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

Касми Э. Найден элементарный способ перехвата чужих сообщений в Telegram. *CNews.* 2020. 7 авг. URL: https://www.cnews.ru/news/top/2020-08-07_v_telegram_obnaruzhena_gigantskaya

Нефедова М. Баг в Facebook Messenger для Android позволял подслушивать пользователей. *Хакер.* 2020. *23 нояб.* URL: https://xakep.ru/2020/11/23/facebook-messenger-bug/

Полякова А. Telegram, Viber, WhatsApp, Signal – яким месенджерам можна довіряти. *Економ. правда.* 2017. 15 груд. URL: https://www.epravda.com.ua/publications/2017/12/15/632183/

Цифрове врядування : монографія / О. В. Карпенко [та ін.] ; за ред. О. В. Карпенка. Київ : ІДЕЯ ПРИНТ, 2020. 336 с.

Budzan, B. (2011). Menedzhment v Ukraini : suchasnist i perspektyvy. Kyiv : Osnovy. 349 p.

Veremieieva, T. (2019). Mesendzhery v Ukraini: osnovni hravtsi, problemy ta perspektyvy. *Comments.* 9 hrudnia. Retrieved from: https://comments.ua/article/it/technology/641679-messendzhery-v-ukraine-osnovnye-igroki-problemy-i-perspektivy.html

Hubenko, D. (2019). Cherez WhatsApp smartfony infikuvaly shpyhunskoiu prohramoiu. *Deutsche Welle.* Retrieved from: https://www.dw.com/uk/через-whatsapp-смартфони-інфікували-шпигунською-програмою/a-48727010

Dreshpak, V. M. (2015). Komunikatsii v publichnomu upravlinni : navch. posib. Kyiv : DRIDU NADU. 168 p. Retrieved from: http://biblio.umsf.dp.ua/jspui/bitstream/123456789/3136/1/Комуніації в публічному управлінні.pdf

Dubynskyi, I. (2019). Pronyknennia internetu v Ukraini. Zhovten *InMind Factum Group Ukraine.* Retrieved from: https://inau.ua/sites/default/files/file/1910/ dani_ustanovchyh_doslidzhen_iii_kvartal_2019_roku.pdf

Zhylenko, D., Reitynh mobilnykh dodatkiv za sichen 2021. *Kantar Ukraina.* Retrieved from: https://tns-ua.com/news/reyting-mobilnih-dodatkiv-za-sichen-2021

Zakon Ukrainy Pro elektronni komunikatsiy. *Ofitsiinyi visnyk Ukrainy.* 26.01.2021 – 2021 r., № 6, stor. 10, st. 306, kod akta 102665/2021. Retrieved from: https://zakon.rada.gov.ua/laws/show/1089-20#Text

Kasmi, J. (2020). Najden jelementarnyj sposob perehvata chuzhih soobshhenij v Telegram. *CNews,* 7 avgusta. Retrieved from: https://www.cnews.ru/news/top/2020-08-07_v_telegram_obnaruzhena_gigantskaya

Nefjodova, M. (2020). Bag v Facebook Messenger dlja Android pozvoljal podslushivat' pol'zovatelej. *Haker.* 23 nojabrja. Retrieved from: https://xakep.ru/2020/11/23/facebook-messenger-bug/

Poliakova, A. (2017). Telegram, Viber, WhatsApp, Signal – yakym mesendzheram mozhna doviriaty. *Ekonomichna pravda.* 15 hrudnia. Retrieved from: https://www.epravda.com.ua/publications/2017/12/15/632183/

Tsyfrove vriaduvannia : monohrafiia / O. V. Karpenko [ta in.] ; za. red. O. V. Karpenka. Kyiv : IDEIa PRYNT, 2020. 336 s.

Осьмак Антон Сергійович,
доктор філософії з публічного управління та адміністрування, доцент кафедри національної економіки та публічного управління,
Київський національний економічний університет імені Вадима Гетьмана,
03057, Україна, м. Київ, проспект Перемоги, 54/1

Цитування: Осьмак А. С. Цифрові сервіси обміну миттєвими повідомленнями в публічному управлінні: сутність, класифікація та кібербезпека. *Вісн. НАДУ. Серія «Державне управління».* 2021. № 1 (100). С. 40–45.

Стаття надійшла: 26.02.2021

Схвалено до друку: 01.03.2021

Osmak, Anton S.,
Philosophy Doctor of Public Management and Administration, Associate Professor of Macroeconomics and Public Administration Department,
Kyiv National Economic University named after Vadym Hetman,
54/1 Prospect Peremogy, Kyiv, 03057, Ukraine
E-mail: anton.osmak@gmail.com
http://orcid.org/0000-0002-1960-8353

Citation: Osmak, A. S. (2021). Tsyfrovi servisy obminu myttievymy povidomlenniamy v publichnomu upravlinni: sutnist, klasyfikatsiia ta kiberbezpeka [Digital instant messaging services in public administration: essence, classification and cybersecurity]. *Bulletin of the NAPA. Series «Public Administration».* Is. 1 (100). P. 40–45 [in Ukrainian].

Article arrived: 26.02.2021

Accepted: 01.03.2021