Дослідження, розробки, проекти
з питань публічного управління та адміністрування

УДК 351

Прав Роман Юрійович
кандидат наук з державного управління
Прав Роман Юрьевич
кандидат наук по государственному управлению
Prav Roman
Candidate of Sciences in Public Administration

ПУБЛІЧНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЮ БЕЗПЕКОЮ
ПУБЛИЧНОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ БЕЗОПАСНОСТЬЮ
PUBLIC ADMINISTRATION OF INFORMATION AND COMMUNICATION SECURITY MANAGEMENT

Анотація. *В умовах активного розвитку цифрових технологій та проведення трансформаційних процесів системи публічного управління актуальним є питання ефективного використання інформації з метою розвитку соціально-економічних та суспільних процесів. Роль держави у забезпеченні захисту інформаційних даних та створення ефективних комунікацій є доволі великою. Інформацію у системі публічного управління можна розглядати як вхідний ресурс у системі надання адміністративних послуг, джерело отримання новин та систему отримання нових знань та навичок. У статі проаналізовані тенденції розвитку цифрових технологій, окремо визначено зростання кількості користувачів Інтернет-ресурсів, соціальних мереж, проаналізовано характеристики різних категорій користувачів. В Україні кількість Інтернет-користувачів є високою, а*

доступ до інформації доволі широким. Отже, актуальним є питання забезпечення населення об'єктивною офіційною інформацією та боротьби з фейками. У рамках даного питання у статті запропоновано налагодження системи публічних комунікацій через підвищення рівня інформаційної грамотності населення. В умовах розвитку системи публічного адміністрування важливим питанням є цифровізація процесів надання адміністративних послуг. Для забезпечення цифровізації у системі публічного адміністрування необхідно створення баз даних та робота з великою кількістю даних. Це викликає два блоки ризиків, які були пропрацьовано у дослідженні: ризики нестачі потужності технічних систем для обробки та зберігання даних, а також ризиків витоку персональної чи конфіденційної інформації через недостатній рівень систем захисту. Отже, у статті також було розглянуто питання кібербезпеки на державному рівні. У результаті дослідження було запропоновано організаційні механізми контролю безпеки інформаційних потоків та комунікаційних зав'язків з метою забезпечення безпеки держави та суспільства.

Ключові слова: *публічне управління, інформаційна безпека, комунікації.*

Аннотация. *В условиях активного развития цифровых технологий и проведения трансформационных процессов системы публичного управления актуальным является вопрос эффективного использования информации с целью развития социально-экономических и общественных процессов. Роль государства в обеспечении защиты информационных данных и создание эффективных коммуникаций довольно высока. Информацию в системе публичного управления можно рассматривать как входной ресурс в системе предоставления административных услуг, источник получения новостей и систему получения новых знаний и*

навыков. В статье проанализированы тенденции развития цифровых технологий, отдельно выделен рост количества пользователей Интернет-ресурсов, социальных сетей, проанализированы характерные различия категорий пользователей. В Украине количество Интернет-пользователей высокое, а доступ к информации довольно широк. Итак, актуальным является вопрос обеспечения населения объективной официальной информацией и борьба с фейками. В рамках данного вопроса в статье предложено повысить эффективность системы публичных коммуникаций путем повышения уровня информационной грамотности населения. В условиях развития системы публичного администрирования важным вопросом является цифровизация процессов предоставления административных услуг. Для обеспечения цифровизации в системе публичного администрирования необходимо создание баз данных и работа с большим количеством данных. Это вызывает два блока рисков, которые были проработаны в исследовании: риски нехватки мощности технических систем для обработки и хранения данных, а также риски утечки персональной или конфиденциальной информации из-за недостаточного уровня систем защиты. Итак, в статье также были рассмотрены вопросы кибербезопасности на государственном уровне. В результате исследования было предложено внедрить организационные механизмы контроля безопасности информационных потоков и коммуникаций с целью обеспечения безопасности государства и общества.

Ключевые слова: *публичное управление, информационная безопасность, коммуникации.*

Summary. *In the conditions of active development of digital technologies and carrying out of system of public management transformational processes the question of effective use of the information for the social and economic and*

social processes development purpose is actual. The role of the state in ensuring the protection of information data and the creation of effective communications is quite large. Information in the system of public administration can be considered as an input resource in the system of administrative services, a source of news and a system of acquiring new knowledge and skills. The article analyzes the development trends of digital technologies, separately identifies the growth in the number of users of Internet resources, social networks, analyzes the characteristics of different categories of users. In Ukraine, the number of Internet users is high, and access to information is quite wide. Thus, the issue of providing the population with objective official information and combating fakes is relevant. In the framework of this issue, the article proposes to establish a system of public communications by increasing the level of information literacy of the population. In the context of the development of the system of public administration, an important issue is the digitalization of the processes of providing administrative services. To ensure digitalization in the system of public administration, it is necessary to create databases and work with a large amount of data. This poses two blocks of risks that have been developed in the study: risks of lack of capacity of technical systems for data processing and storage, as well as risks of leakage of personal or confidential information due to insufficient level of security systems. Thus, the article also addressed the issue of cybersecurity at the state level. As a result of the study, organizational mechanisms for controlling the security of information flows and communication links were proposed in order to ensure the security of the state and society.

Key words: *public administration, information security, communication.*

Постановка проблеми. Сучасне суспільство розвивається в умовах великих потоків інформації, які не просто здійснюють інформаційну функцію, але і формують відношення громадськості до певних процесів

суспільного, соціально-економічного, політичного життя держави. Отже, інформація є важливим джерелом забезпечення стабільності розвитку суспільства, в тому числі є фактором національної безпеки. Розвиток цифрових технологій значно збільшує потоки інформації, формуючи систему Big Date – великих інформаційних потоків, які містять акумулювану із певною метою інформацію. Цифрові дані та гаджети для їх використання активно розвиваються. У 2019 році вперше кількість осіб, що використовує у якості джерел інформації цифрові ресурси перевищило 50%, залишивши на другому місці телебачення, що до цього часу лідирувало [1]. За статистикою Організації Об'єднаних Націй у 2020 році було зареєстровано понад 4,5 мільярдів людей на патенті, що є користувачами мережі Інтернет [2], і ця кількість продовжує зростати. Нарощування обсягів інформаційних потоків має позитивні моменти, зокрема, підвищення доступності, прозорості, оперативності їх отримання, проти ставить під загрозу питання збереження конфіденційної інформації, правдивості та відповідності дійсним фактам. Отже, питання захисту інформації в умовах нарощування потоків цифрових даних та спрощення доступу до них лежить у поля обов'язків публічного управління та має високу актуальність.

Аналіз останніх досліджень і публікацій. Питаннями забезпечення інформаційної безпеки та системи ефективних комунікацій на рівні публічного управління у зв'язку із актуальністю та високим практичним значенням розглядалися у роботах багатьох вітчизняних науковців. Відзначимо ті роботи, які були виділені для визначення окремих аспектів проведеного та представленого у статті дослідження, а саме роботи таких авторів: Кукіна І. В., Панченка О. А., Євдоченко Л. О., Варенья Н.М. Проте, активний розвиток цифрових технологій та впровадження трансформаційних процесів ставить перед дослідниками нові завдання розвитку публічних інформаційно-комунікаційних технологій.

Формулювання цілей статті (постановка завдання). Розвиток цифрових технологій та нарощування обсягів інформаційних потоків ставить перед органами державної влади завдання створення систем управління інформаційно-комунікаційними потоками для забезпечення безпеки та сталого розвитку держави. Відповідно до актуальності теми дослідження у статті поставлено за мету розробити шляхи підвищення рівня безпеки інформаційно-комунікаційних технологій у публічному секторі.

Для досягнення поставленої мети було окреслено ряд завдань:

- проаналізувати місце цифрових технологій у житті сучасної людини та у системі публічного управління;
- визначити наявні ресурси цифрової підтримки публічного управління та тенденції подальшого розвитку,
- проаналізувати алгоритми роботи з інформаційними системами на рівні публічного управління: надання адміністративних послуг, оцінки статистичних даних, комунікації, державної інформаційної політики,
- запропонувати організаційні механізми контролю безпеки інформаційних потоків та комунікаційних зав'язків з метою забезпечення безпеки держави та суспільства.

Виклад основного матеріалу. В умовах відкритого доступу до інформації важливим аспектом її сприйняття є підтвердження даних реальними фактами, забезпечення неупередженості, чесності та прозорості джерел, що цю інформацію надають. Великі обсяги інформаційних потоків значно ускладнюють системи контролю виведення в публічний простір інформації, що часто не відповідає дійсності, лобіює інтереси певних політичних та економічних груп, загрожує національній безпеці держави. В умовах переведення основних потоків інформації у цифрові ресурси,

процеси здійснення контролю безпеки інформації та запобігання витокам конфіденційних даних особливо ускладняються.

За даними статистики у світі кількість Інтернет-користувачів складає 4,54 мільярда осіб, у порівнянні із 2019 роком ця цифра виросла на 7%. Тенденції свідчать про продовження зростання кількості юзерів. Одним із найбільш популярних серед користувачів Інтернет-контентом є контент соціальних мереж. Так, на сьогодні різними соціальними мережами користуються 3,8 мільярди осіб на планеті, а зростання цього показника за рік становило 9% (в Україні користувачами соціальних мереж є майже половина населення). Отже, тенденції зростання кількості підписників соціальних мереж є вищими, ніж показники охоплення населення планети всесвітньою мережею, що визначає високу інформаційну роль соціально-мережевого контенту у формуванні ставлення населення до певних питань суспільного характеру, формування суспільної думки, інформатизації та інших процесів комунікативного спрямування [2].

Період часу, який середньостатистична людина проводить у мережі становить приблизно 6 з половиною годин на день, тобто понад ста днів на рік. Це майже третина нашого часу. Інтернет-ресурси використовуються як для роботи, проведення дозвілля, так і для перегляду новин, пошуку експертних думок для допомоги у визначенні людиною власної позиції з того чи іншого питання, отримання релевантної інформації за різними запитами: освіта, медицина, саморозвиток, отримання публічних чи муніципальних послуг тощо [7].

Хоча, варто зазначити, що різні категорії населення мають різні можливості доступу до інформації. За статистикою менша кількість жінок, ніж чоловіків користуються Інтернет-ресурсами, є зворотно пропорційна залежність між віком людей та відсотком користувачів у даній віковій категорії, жителі міст мають ширші можливості доступу, ніж сільські жителі. Понад 40% населення планети взагалі не мають доступу до мережі

Інтернет, більша частина із яких є мешканцями Південної Азії та Африки (31% та 27% відповідно), що свідчить про залежність рівня доступу до мережі та рівня життя і доходів анселення. Географічно кількість осіб, що не мають доступу до мережі за регіонами представлена на рис. 1

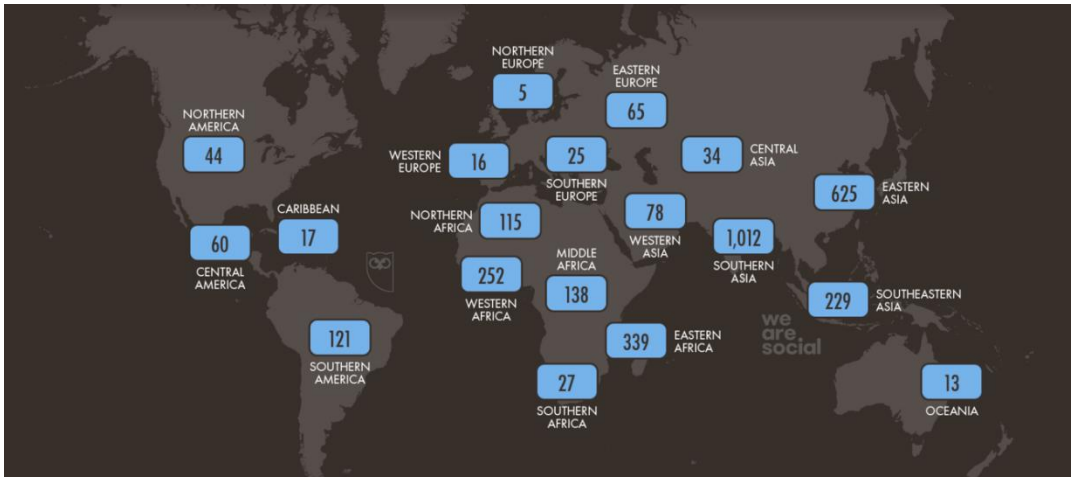

Рис. 1. Кількість осіб, що не мають доступу до мережі Інтернет, *млн. осіб* **[8]**

Україна посідає 29 місце у світі за долею підключених до мережі Інтернет у структурі населення. Це доволі високий показник [9]. При цьому, понад 90% мають можливість використовувати смартфони для доступу до мережі [1]. Ця цифра вказує на велике розповсюдження мобільних пристроїв, що дають додаткові можливості для отримання інформації, зокрема мобільні додатки, месенджери та чат-боти, що є додатковими механізмами розповсюдження інформації та можуть бути використані з метою забезпечення публічного управління комунікаціями.

В Україні з метою управління потоками цифрової інформації на рівні публічної влади було створено Міністерство цифрової трансформації України, яке діє на основі Положення про Міністерство, що визначає його основні функції [10]:

- реалізація державної політики цифровізації всіх сфер життя населення, розвитку економіки, публічного адміністрування,
- розвиток цифрової грамотності населення,

- розвиток національних інформаційних систем та інформаційної інфраструктури,
- сприяння розвитку IT-сектору та цифровізації інших галузей економіки.

Представимо основні проєкти Міністерства, що реалізовані у вигляді наступної схеми – рис. 2

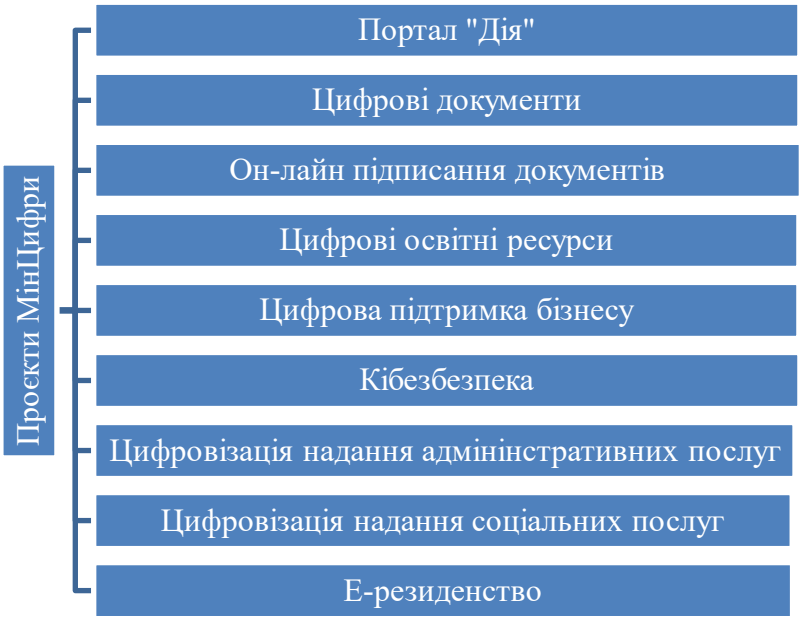

Рис. 2. Проєкти Міністерства цифрової трансформації України

Аналізуючи проєкти, розроблені та впроваджені Міністерством, варто зазначити, що особлива увага уряду приділяється максимальній цифровізації процесів надання адміністративних та соціальних послуг. При цьому, до додатків та програмних продуктів, що створені з метою забезпечення е-адміністрування, приєднуються бази даних із персональною інформацією користувачів. Така система акумулювання інформаційних даних має два великих блоки ризиків:

- ризик неправомірного заволодіння та використання персональними даними користувачів,
- ризик збоїв у роботі програмного забезпечення через високе навантаження та велику кількість даних.

Мінімізація даних ризиків можлива лише за умови впровадження ефективних систем інформаційної безпеки. Для формування практичних підходів до забезпечення кібербезпеки пропонується наступний алгоритм реалізації функцій публічного управління у галузі інформатизації – рис. 3

Рис. 3. Система забезпечення інформаційної безпеки на рівні публічного управління

Отже, у рамках алгоритму забезпечення кібербезпеки та безпеки інформаційних потоків виділено наступні блоки:

- вільний доступ до офіційної інформації та її поширення,
- захист персональних та конфіденційних даних, інформації, що містить державну таємницю,
- робота із кібератаками,
- боротьба із недостовірною інформацією.

Розробка алгоритму управління інформаційної безпекою на публічному рівні дозволила визначити дві складові: технічну та

комунікаційну. Хотілося б більш детально зупинитися саме на комунікаційній складовій інформаційної безпеки.

В умовах політичної нестабільності, соціально-економічної кризи, військової агресії на Сході України та пандемії коронавірусу і інших зовнішніх та внутрішніх факторів ризику розвитку суспільства, важливими аспектом є забезпечення ефективних комунікацій органів публічної влади і населення країни. Аналізуючи систему комунікацій між публічним сектором, приватним сектором, органами місцевої влади та населенням у дослідженні було виділено наступні блоки:

- боротьба з фейковою та недостовірною інформацією,
- попередження інформаційних «вбросів»,
- боротьба з пропагандою,
- створення системи іміджу засобів масової інформації із відповідним формуванням ставлення суспільства до ЗМІ.

Питання безпеки комунікацій публічної влади має таку ж високу актуальність як і питання захисту інформаційних даних. Кількість фейкової інформації у мережі постійно зростає. Інформацію із непідтвердженими даними або даними, що містять суб'єктивні оцінки та висновки використовують навіть провідні вітчизняні ЗМІ. У такі ситуації важливим є забезпечення населення оперативною достовірною інформацією, що засновується на фактах та експертному аналізі, а не чутках, неперевіреній інформації, неправдивих даних чи домислах. Частково така інформація є спеціальним інформаційним «вбросом», що може бути пов'язаний із необхідністю формування через певні групи лобістів громадської думки з приводу питань суспільного розвитку, підготовки цієї думки до певних подій з метою забезпечення погодження тих чи інших дій суспільством. Особливу небезпеку складають такі інформаційні провокації в умовах гібридної війни. Механізмами для попередження негативних явищ у системах комунікації публічного сектору

із громадськістю є забезпечення відповідальності засобів масової інформації за якість надання даних своєю репутацією. Високий рівень інформаційної культури створює передумови для формування негативного ставлення суспільства до тих джерел інформації, які мають погану репутацію або у інформаційних матеріалах яких були виявлені неправдиві, фейкові чи суб'єктивні дані. Формування іміджу інформаційних джерел за рахунок підвищення якісного рівня інформаційного середовища можна досягти лише у інформаційно свідомому суспільстві, коли люди розуміють, як відрізнити фейкову новину від справжньої, де шукати достовірні джерела інформації, як повідомити користувачів інформації, що вона не є достовірною та вивести її із інформаційного поля. Підвищення інформаційної грамотності населення можливо шляхом максимального охоплення людей ресурсами підвищення цифрової грамотності, що сприятиме як забезпеченню більш високого ступеня захисту інформаційних даних, так і створенню об'єктивного комунікаційного простору у системі «публічна влада-населення».

Висновки та пропозиції. Отже, у статі розглянуті питання розвитку інформаційної безпеки та системи комунікацій на рівні публічного управління. Визначено актуальність процесів цифровізації та проаналізовано національний досвід створення цифрових технологій. Серед проблемних аспектів цифровізації визначено ризики при використанні великої кількості даних, безпеки конфіденційної інформації та необхідність створення більш прозорого комунікаційного простору із заміною великої кількості фейкової інформації на достовірні офіційні дані шляхом підвищення якості інформаційного простору та цифрової грамотності населення.

Література

1. Офіційний сайт Української інтернет асоціації. Дослідження Інтернет-аудиторії. URL: https://inau.ua/proekty/doslidzhennya-internet-audytoriyi
2. Офіційний сайт Організації Об'єднаних Націй в Україні. URL: https://ukraine.un.org/uk
3. Кукін І. В. Комплексний механізм публічного управління інформаційною безпекою особистості у сфері національної безпеки та її прикордонному секторі / І. В. Кукін // Публічне управління та митне адміністрування. 2020 . № 4 (27). С. 134-139.
4. Панченко О. А. Роль засобів масової інформації в системі державного управління інформаційною безпекою / О. А. Панченко // Публічне управління та митне адміністрування. 2020. № 1 (24). С. 97-102.
5. Євдоченко Л. О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах умовах глобалізації: автореф. дис. канд. наук з держ. упр. : 25.00.01 // Львівський регіональний інститут державного управління Національної академії державного управління при Президентові України. Львів, 2011. 20 с.
6. Варенья Н.М. Ідеологічне підґрунтя стратегічних комунікацій як форма протидії інформаційної агресії // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.) [Електронне видання]. Київ: Нац. акад. СБУ, 2019. С. 18-20.
7. Офіційний сайт Організації Об'єднаних Націй. Департамент глобальних комунікацій. URL: https://www.un.org/ru/sections/departments/department-global-communications/index.html
8. Офіційний сайт Організації Об'єднаних Націй. Щорічник ООН. URL: https://unyearbook.un.org/

9. Офіційний сайт Урядового порталу України. Питання Міністерства цифрової трансформації. URL: https://www.kmu.gov.ua/npas/pitannya-ministerstva-cifrovoyi-t180919
10. Офіційний сайт Міністерства цифрової трансформації України. URL: https://thedigital.gov.ua/

References

1. Ofitsiinyi sait Ukrainskoi internet asotsiatsii. Doslidzhennia internet-audytorii. URL: https://inau.ua/proekty/doslidzhennya-internet-audytoriyi
2. Ofitsiinyi sait Orhanizatsii Obiednanykh Natsii v Ukraini. URL: https://ukraine.un.org/uk
3. Kukin I. V. Kompleksnyi mekhanizm publichnoho upravlinnia informatsiinoiu bezpekoiu osobystosti u sferi natsionalnoi bezpeky ta yii prykordonnomu sektori / I. V. Kukin // Publichne upravlinnia ta mytne administruvannia. 2020. № 4 (27). S. 134-139.
4. Panchenko O. A. Rol zasobiv masovoi informatsii v systemi derzhavnoho upravlinnia informatsiinoiu bezpekoiu / O. A. Panchenko // Publichne upravlinnia ta mytne administruvannia. 2020. № 1 (24). S. 97-102.
5. Yevdochenko L. O. Udoskonalennia systemy derzhavnoho zabezpechennia informatsiinoi bezpeky Ukrainy v umovakh umovakh hlobalizatsii: avtoref. dys. kand. nauk z derzh. upr. : 25.00.01 // Lvivskyi rehionalnyi instytut derzhavnoho upravlinnia Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy. Lviv, 2011. 20 s.
6. Varenia N.M. Ideolohichne pidhruntia stratehichnykh komunikatsii yak forma protydii informatsiinoi ahresii // Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy: zb. tez nauk. dop. nauk.-prakt. konf. (Kyiv, 4 kvitnia 2019 r.) [Elektronne vydannia]. Kyiv: Nats. akad. SBU, 2019. S. 18-20.

7. Ofitsiinyi sait Orhanizatsii Obiednanykh Natsii. Departament hlobalnykh komunikatsii.URL:https://www.un.org/ru/sections/departments/department-global-communications/index.html
8. Ofitsiinyi sait Orhanizatsii Obiednanykh Natsii. Shchorichnyk OON. URL: https://unyearbook.un.org/
9. Ofitsiinyi sait Uriadovoho portalu Ukrainy. Pytannia Ministerstva tsyfrovoi transformatsii. URL: https://www.kmu.gov.ua/npas/pitannya-ministerstva-cifrovoyi-t180919
10. Ofitsiinyi sait Ministerstva tsyfrovoi transformatsii Ukrainy. URL: https://thedigital.gov.ua/