

7. Robertson R., Church-State Relations: Tensions and Transitions / Robertson R., Robbins T. // Sociology of Religion. – 1987. – vol. 49 (2). –p. 187-188
8. Robertson, R., The Eastern Christian Churches. A brief Survey / Robertson, R., Stancati, S. // Angelicum [Rezension]. Rom., 1990 – 149-151.

**Науменко Ольга Михайлівна**

Доцент кафедри політичних технологій  
Київського національного економічного університету  
імені Вадима Гетьмана,  
кандидат політичних наук, доцент

## **РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ ПОЛІТИЧНОЇ ЕЛІТИ ЗА УМОВ ВІЙНИ**

Сучасні цифрові технології виводять діяльність політичної еліти за умов війни на новий рівень політичної комунікації. Державний сектор, як і бізнес зокрема постали з викликом захисту інформації та унеможливлення щодо неї DDoS-атак. Поширеними стали інформаційно-психологічний тиск на суспільства та кібератаки на державні установи.

За умов інформаційного суспільства роль медіа зростає не лише як посередника між владою і соціумом, а як фактор трансформації політичної системи діяльності політичних еліт, розвитку політичних процесів, формування брендів у суспільній свідомості, комерціалізації та прагматизації соціальних відносин. Дані процеси зумовили появу медіасфери, медіаполітики [1, с. 33]. Вплив медіафактора на діяльність політичних еліт виявляється в формування особистого іміджу та іміджу держави, що за умов воєнного стану набуло посиленого значення через пропаганду та контрпропаганду російсько-української війни.

Медіачинник соціально-політичної мобілізації спрацьовує в інтересах залежності ЗМІ від органів влади: загальнодержавних, центральних, регіональних, олігархічних. Висвітлення подій здійснюється на користь замовника, щодо оповіщення суспільства та громадськості про його позитивні ініціативи, гуманітарні акції, успішні проекти, благодійні внески олігарха та патріотичні програми. Тим самим політична еліта формує позитивний імідж та прогнозовані рейтинги щодо майбутніх виборів в органи публічної влади. Здебільшого електорат сприймає політиків як рекламних об'єктів.

Засоби масової інформації підлаштовують імідж політиків під запити цільової аудиторії. Комерціалізація політиків як товар є прийнятною і зручною для претендентів на високі посади у цілому в державі чи регіонах. Новим топом політичного лідера є цифровий політичний суб'єкт [1, с. 36].

м. Одеса, 23 березня 2023 р.

Матеріали II Всеукраїнської науково-практичної конференції  
«Трансформація українського суспільства в цифрову еру»

До російського вторгнення український уряд працював лише на серверах, які розташовувалися в головних державних будівлях. Дані місця були вразливими до ракетних атак, фізичне знищення яких могло б паралізувати всю роботу вищого керівництва країни. 17 лютого 2022 р. міністр цифрової трансформації України М. Федоров разом з колегами в парламенті ухвалили рішення щодо переміщення локальних серверів в публічну «хмару». Відбулася евакуація критичних державних даних до центрів обробки інформації по всій Європі.

Реалізоване владою України рішення було своєчасне і важливе, локалізуючи вплив і доцільність російських ракетних кібератак та обстрілів. Компанія Microsoft відіграла власну роль щодо збереження стійкості країни, спеціалісти якої надавали доступ до найсучасніших технічних інструментів, що прискорило перенесення важливих даних за межі країни задля збереження операційної діяльності уряду [2].

Хмарні сервіси з початку війни були ключовими інструментами захисту українських держреєстрів, збереження цілісності державного аудиту та підтримки економіки. Наразі центри обробки даних цифрової інфраструктури України, які підтримують усі військові і цивільні операції, розташовані в різних європейських країнах.

Хмарні сервіси дали змогу не лише обминути руйнівні наслідки від російських кібератак та поширити програмне забезпечення, тим самим знешкоджуючи шкідливі програми. І через рік повномасштабного вторгнення чутливими до даних програм є локальні урядові системи, які не є приєднані до «хмар» [2].

DDoS-атака є методом атаки, коли хакери націлюються на сервери та перевантажують їх користувальницьким трафіком. За даних умов сервер не справляється з вхідними запитами, сайт, додаток чи програма, які розміщені на ньому, відключаються чи працюють з низькою продуктивністю.

Для прикладу, після початку повномасштабного вторгнення росії в Україну Міністерство цифрової трансформації України заснувало добровільну кіберармію, що здійснює DDoS-атаки на ресурси країни-окупанта. За досить короткий період IT ARMY of Ukraine поклати сайти російських пропагандистів, органів влади, компаній із держсектора, енергетики, банків, рітейлу, сервіси грошових переказів, бухгалтерської звітності і багато іншого. Все це викликало паніку у місцевого населення [3].

17 лютого 2023 р. було прийнято Верховною Радою України Закон України «Про хмарні послуги» № 2075-IX [4], що встановлює характерні особливості застосування хмарних послуг органами державної влади, органами влади Автономної Республіки Крим, органами місцевого самоврядування, військовими формуваннями, які утворені згідно законів України, державними підприємствами,

установами і організаціями, суб'єктами владних повноважень та іншими суб'єктами, яким делеговані такі повноваження [5].

За умов воєнного стану Постановою Кабінету міністрів України від 12 березня 2022р. державні установи одержали дозвіл на розміщення державних інформаційних ресурсів і публічних електронних реєстрів на хмарних ресурсах в центрах обробки даних чи поза ними, які розміщені за межами України. Це розширило можливості використання хмар за умов воєнного стану, що надало державним організаціям та бізнесу застосовувати всі їх переваги для безперешкодної роботи у складний воєнний період [6].

Роль цифрових технологій за умов війни забезпечує зберігання важливої державної інформації у хмарних сервісах міжнародних компаній в країнах ЄС та США. Діяльність політичної еліти в захисті інформаційних технологій є значною через засоби створення IT-армії, запуск чатборту «Ворог» та використання інтернет-сервісу Starlink від SpaceX, які роздають супутниковий інтернет для забезпечення української армії широкопasmовим зв'язком.

#### Список використаної літератури

1. Дроботун, Д. (2021). Медіафактор у діяльності політичних еліт. *Науковий журнал «Politicus»*. Південноукр. нац. пед. ун-т ім. К. Д. Ушинського ; голов. ред. С. М. Наумкіна. Одеса : Виданичий дім «Гельветика». Випуск 4. 130 с. 33–38.
2. Незламна цифра. Які технології допомогли Україні вистояти під час війни (2023, січень, 24). New Voice. <https://biz.nv.ua/ukr/markets/ukrajina-z-rozvitkom-tehnologiy-vistoyala-pered-atakami-rosiji-shcho-zminilosya-pid-chas-vijni-z-rf-50298276.html>
3. Що таке кібербезпека і як бізнесу захиститися від DDOS-атак (2022, травень, 04). GigaCloud. <https://gigacloud.ua/blog/navchannja/scho-take-kiberbezpeka-i-jak-biznesu-zahistitisja-vid-ddos-atak>
4. Закон України Про хмарні послуги. Верховна Рада України. № 2075-IX (2023). <https://zakon.rada.gov.ua/laws/show/2075-IX#Text>
5. Прийнято Закон України «Про хмарні послуги» (2023, лютий, 17). Верховна Рада України. Офіційний вебпортал парламенту України. <https://www.rada.gov.ua/news/Novyny/219626.html>
6. Підгайна Є. (2022, березень, 29) Тримаємо стрій: добірка корисних хмарних сервісів для відновлення роботи бізнесу в умовах війни. Як облаштувати робочі місця у будь-якій точці світу та убезпечити корпоративні дані. MIND.UA. <https://mind.ua/publications/20238662-trimaemo-strij-dobirka-korisnih-hmarnih-servisiv-dlya-vidnovlennya-roboti-biznesu-v-umovah-vijni>