**ОЦІНКА ГОТОВНОСТІ ОРГАНІЗАЦІЙ ДО ГІБРИДНОГО ТА ДИСТАНЦІЙНОГО УПРАВЛІННЯ**

**Нестерук В.А.**

здобувач наукового ступеня доктора філософії

Науковий керівник: **Середа Г.В.**

к.е.н., доцент

*Донецький національний університет імені Василя Стуса*

У сучасних умовах, коли Україна стикається з численними викликами післявоєнного відновлення, організації змушені шукати ефективні моделі управління, які відповідають новим реаліям. Гібридні та дистанційні моделі управління стають одним із найважливіших інструментів адаптації. Втім для успішного впровадження цих моделей необхідно проводити детальну оцінку готовності організації до їхнього застосування, враховуючи технологічні, управлінські, соціальні та безпекові аспекти. Такий підхід дозволяє уникнути помилок при переході на нові моделі роботи та забезпечує стабільність і ефективність процесів в організації.

Першим кроком у процесі оцінювання готовності організації до переходу на гібридні та дистанційні моделі управління є перевірка стану її цифрової інфраструктури. Успішне впровадження гібридної або дистанційної роботи потребує наявності надійної інфраструктури, яка включає високошвидкісний інтернет, цифрові платформи для комунікації та зберігання даних, а також засоби для управління проєктами. Наприклад, платформи на кшталт Microsoft Teams або Zoom дозволяють командам підтримувати зв’язок, незалежно від їхнього фізичного місцезнаходження. Однак важливо оцінити, чи відповідає інфраструктура організації потребам нових робочих умов, особливо в післявоєнній Україні, де значна частина технічних ресурсів може бути пошкоджена або зруйнована. Організації повинні мати не лише технологічні засоби, але й резервні канали Інтернет зв'язку та альтернативні джерела електроенергії в умовах воєнних загроз та стихійних лих на випадок можливих збоїв, що дозволить уникнути простоїв у роботі [1].

Другий ключовий аспект готовності організації до переходу на гібридні моделі стосується персоналу. Оцінка готовності працівників до роботи в нових умовах повинна враховувати їхній технічний рівень, здатність адаптуватися до цифрових інструментів, а також психологічну готовність до змін. Не всі працівники мають достатні навички для ефективної роботи з цифровими платформами, тому важливим елементом впровадження є проведення навчальних програм, які допоможуть підвищити їхню цифрову грамотність. Крім того, важливо розуміти, що психологічний стан працівників, особливо в умовах післявоєнної реабілітації, відіграє значну роль у їхній продуктивності. Війна створила нові виклики для психічного здоров’я, тому організації мають розробляти програми підтримки, орієнтовані на адаптацію персоналу до роботи в нових умовах [2].

Також необхідно звернути увагу на управлінські практики в організації, які безпосередньо впливають на успішність переходу на гібридні та дистанційні моделі. Традиційні управлінські підходи, де продуктивність оцінювалася за кількістю часу, проведеного в офісі, стають малоефективними в нових умовах. Організації повинні перейти до орієнтованих на результат моделей оцінки, де головним критерієм успішності є прогрес у досягненні встановлених цілей, а не фізична присутність на робочому місці. Це передбачає створення системи ключових показників ефективності, які допоможуть об’єктивно вимірювати результати роботи кожного співробітника, незалежно від його робочого місця [3].

Не менш важливою складовою оцінки готовності є організаційна гнучкість. У контексті переходу на гібридні моделі особливого значення набуває здатність організації швидко адаптувати свої процеси під нові умови. Це стосується як комунікації між командами, що працюють у різних форматах (віддалено або в офісі), так і інтеграції різних відділів у єдину ефективну систему управління. Гнучкість дозволяє організації не тільки успішно впроваджувати нові моделі роботи, але й адаптуватися до можливих змін у зовнішньому середовищі. Наприклад, в умовах післявоєнної нестабільності організаціям потрібно бути готовими до швидких змін в економічній і політичній ситуаціях, що впливає на їхню діяльність [4].

Водночас кібербезпека також відіграє ключову роль у забезпеченні успішного переходу на гібридні моделі управління. Перехід на віддалену роботу підвищує ризики кіберзагроз, пов’язаних з використанням віддалених доступів та хмарних платформ. Організаціям потрібно забезпечити належний захист своїх даних та інформаційних систем, включаючи впровадження надійних механізмів автентифікації, шифрування даних та моніторингу безпеки. Крім того, необхідно навчати персонал основам кібербезпеки, щоб мінімізувати ризики людських помилок, які можуть призвести до витоку конфіденційної інформації [5]. У післявоєнний період, коли ресурси організацій можуть бути обмеженими, ризики кіберзагроз збільшуються, тому необхідно особливо ретельно оцінювати готовність компаній до забезпечення кібербезпеки в умовах гібридної роботи.

Вищеперелічені категорії цілком доцільно розглядати в комплексі як складові інтегральної готовності організації до гібридного та дистанційного управління, що детальніше проілюстровано з перспективи складових внутрішнього середовища організації (зокрема: цілей, структури, технологій, персоналу та організаційної культури) і через проміжні елементи готовності та їхні зв’язки, продемонстровані на відповідній схемі (рис. 1).



Рисунок 1 – Схема складових інтегральної готовності організації до гібридного та дистанційного управління

Загалом, комплексна оцінка готовності організації до переходу на моделі гібридного або дистанційного управління за всіма ключовими складовими зовнішнього середовища формує передумови необхідних внутрішніх трансформацій та змін. Тільки глибокий аналіз технологічної інфраструктури, готовності персоналу, адаптивності управлінських практик та безпеки дозволить забезпечити ефективність нових моделей роботи та адаптувати організацію до змінних умов зовнішнього середовища. Така підготовка створює основу для більш стійкого та гнучкого розвитку організацій України в умовах післявоєнного відновлення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. S. Robertson, S. Baror, H. Venter. «Enhancing Metaward: Integrating Digital Forensic Readiness in the Metaverse.» European Conference on Cyber Warfare and Security, 2024. URL: https://papers.academic-conferences.org/index.php/eccws/article/view/2320.
2. C. De la Cruz, N. Furto, M. Lentejas. «Artificial Intelligence (AI) Application in Government Department Hybrid Work Environment: A Holistic Study and Policy Implications.» SSRN Papers, 2023. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=4590556.
3. M. Lentejas, C. De la Cruz, N. Furto. «Artificial Intelligence Application in Government Department Hybrid Work Environment: A Holistic Study and Policy Implications.» ResearchGate, 2023. URL: https://www.researchgate.net/profile/Ma-Juvy-Lentejas/publication/375142848\_ARTIFICIAL\_INTELLIGENCE\_APPLICATION\_IN\_GOVERNMENT\_DEPARTMENT\_HYBRID\_WORK\_ENVIRONMENT\_A\_HOLISTIC\_STUDY\_AND\_POLICY\_IMPLICATIONS/links/65424c640426ef6369f5279e/ARTIFICIAL-INTELLIGENCE-APPLICATION-IN-GOVERNMENT-DEPARTMENT-HYBRID-WORK-ENVIRONMENT-A-HOLISTIC-STUDY-AND-POLICY-IMPLICATIONS.pdf.
4. S. Robertson, S. Baror, H. Venter. «Enhancing Metaward: Integrating Digital Forensic Readiness in the Metaverse.» European Conference on Cyber Warfare and Security, 2024. URL: https://papers.academic-conferences.org/index.php/eccws/article/view/2320.
5. J. L. Flores, E. Cohen, M. Mansour. «Integrating Cybersecurity into Hybrid Work Environments.» Cybersecurity Review Journal, 2023. URL: https://www.cybersecurityreviewjournal.com/integrating-cybersecurity-into-hybrid-work.