

ОРГАНІЗАЦІЯ КОМАНДНОЇ РОБОТИ В УМОВАХ ГЛОБАЛЬНИХ ВИКЛИКІВ У КОНТЕКСТІ ЦИФРОВОЇ ТА КАДРОВОЇ БЕЗПЕКИ¹

Глебова Алла Олександрівна*, кандидат економічних наук, доцент,
доцент кафедри менеджменту і логістики
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

*ORCID 0000-0002-7030-948X



© Глебова А.О., 2025

Стаття отримана: 10.11.2025

Стаття прийнята: 11.12.2025

Стаття опублікована: 26.12.2025

Вступ. Глобальні виклики сучасності: цифровізація, пандемія COVID-19, глобалізація, дефіцит водних ресурсів, штучний інтелект, гібридні формати зайнятості, зростання кількості кіберзагроз, посилення процесів міждержавної міграції тощо, впливають на організацію роботи не тільки організації, але і управлінської діяльності. Зростає роль комунікацій, командної роботи, змінюються підходи до організації бізнес-процесів та управління продуктивністю й ефективністю організації. В умовах високої турбулентності зовнішнього середовища ефективність організації як і управлінської діяльності змінюється, як і ключові фактори успіху. Однак, незмінним фактором організаційного розвитку й ефективності залишається персонал, який здатний забезпечити як стрімкий розвиток, так й банкрутство. Стрімкий розвиток цифрових платформ, хмарних сервісів, систем аналітики й інструментів віддаленої колаборації створює нову архітектуру робочого середовища. Цифрові комунікації стають не просто засобом обміну інформацією, а ключовим елементом підтримки продуктивності, прозорості процесів, координації завдань і згуртованості команди незалежно від її географічної дислокації. Водночас зростаюча цифровізація зумовлює появу нових ризиків: витік конфіденційних даних, маніпуляція інформацією, кібератаки, а також внутрішніх загроз, пов'язаних із поведінковими девіаціями та низьким рівнем цифрової компетентності працівників. У цих умовах кадрова безпека формується як складний багатокомпонентний інститут, що поєднує технологічні, організаційні та поведінкові механізми забезпечення надійності персоналу. Її значення суттєво посилюється, оскільки порушення безпекових політик у цифровому середовищі здатні не лише ускладнити командну взаємодію, а й створити загрози стратегічній стійкості організації. Таким чином, дослідження специфіки організації командної роботи в умовах глобальних викликів через призму цифрових комунікацій і кадрової безпеки є надзвичайно актуальним. Воно дозволяє ідентифікувати ключові фактори ризику, оцінити вплив цифрових інструментів на надійність командної взаємодії та сформулювати комплекс управлінських рішень для забезпечення ефективного й безпечного функціонування команд у цифрову епоху.

Аналіз останніх досліджень і публікацій. Сучасні глобальні виклики, які обумовлені цифровізацією, гібридними формами зайнятості, зростанням кіберзагроз і трансформацією соціально-економічних процесів, суттєво змінюють характер організації командної роботи та моделі комунікацій у цифровому середовищі. У цих умовах особливої актуальності набуває питання забезпечення кадрової безпеки як базового елементу надійності командної взаємодії та стратегічної стійкості організації. Незважаючи на наявність численних досліджень щодо цифрових комунікацій Осокіна М. [1], Бережко О. [2], Баченко Л. [3]; управління командами Баркова К. [4], Такман Б. [5], Сміт Д. [6] та ризиків у цифровому робочому просторі Філоненко С. [7], Малюга В. [8] недостатньо опрацьованими залишаються інтегра-

¹ Публікацію підготовлено в межах виконання науково-дослідних робіт за фінансування МОН України: «Прогнозування властивостей мультикомпонентних біодеградуючих скафолдів для лікування і корекції травм кісткової тканини» (№ ДР 0125U000447) та «Вивчення механічних і біологічних властивостей полімер-нано-гідроксиапатитних біодеградуючих 3D скафолдів в умовах in vitro та in vivo» (№ ДР 0125U001429)

ційні аспекти поєднання цифрових інструментів комунікації з механізмами кадрової безпеки в роботі сучасних команд.

Метою статті є дослідження теоретико-практичних аспектів процесу інтеграції цифрових комунікацій і механізмів кадрової безпеки в управлінні сучасними командами та визначення напрямів мінімізації репутаційних ризиків та втрат від несанкціонованого доступу до інформації та дисфункцій командної взаємодії.

Основний матеріал і результати. Сучасні умови цифрової трансформації висувають принципово нові вимоги до організації командної роботи, зумовлюючи потребу у науково обґрунтованих підходах до формування та управління командами, але з урахуванням цифрової та кадрової безпеки. Динамічне цифрове середовище, що характеризується високою швидкістю обміну інформацією, поширенням дистанційних форматів зайнятості не тільки в Україні, Європі (табл. 1) та світі, зростанням кількості цифрових платформ і комунікаційних сервісів, потребує від керівників не лише технологічної компетентності, а й здатності враховувати психологічні, емоційні та інтелектуальні особливості членів команди під час обрання моделі командоутворення.

Таблиця 1

Аналіз кількості зайнятих осіб, які працюють вдома, у відсотках від загальної зайнятості, за статтю, віком та професійним статусом (%) за даними Євростату у 2020–2024 роках

Країна	2020	2021	2022	2023	2024	Відхилення від 2024 року			
						2020	2021	2022	2023
Бельгія	17,2	26,2	16,4	14,3	13,8	17,2	26,2	16,4	14,3
Болгарія	1,2	2,8	1,6	1	1,2	1,2	2,8	1,6	1
Чехія	7,2	7,2	6,3	6,1	6,6	7,2	7,2	6,3	6,1
Данія	17	18,1	11,8	7,9	7,8	17	18,1	11,8	7,9
Німеччина	13,6	17,2	14,5	12,8	12,9	13,6	17,2	14,5	12,8
Естонія	12,2	14,9	12,4	12	13,1	12,2	14,9	12,4	12
Ірландія	21,5	32,2	25,4	21,4	20,6	21,5	32,2	25,4	21,4
Греція	7	6,7	2,5	1,9	2,7	7	6,7	2,5	1,9
Іспанія	10,9	9,4	7,5	7,1	7,8	-3,1	-1,6	0,3	0,7
Франція	15,7	17	12,4	10,8	11,1	-4,6	-5,9	-1,3	0,3
Хорватія	3,2	4,8	4,9	4,8	4,5	1,3	-0,3	-0,4	-0,3
Італія	12,2	8,3	5,2	4,4	3,7	-8,5	-4,6	-1,5	-0,7
Кіпр	4,9	6,8	4,5	3,9	4	-0,9	-2,8	-0,5	0,1
Латвія	4,5	11	8,8	8,1	8,4	3,9	-2,6	-0,4	0,3
Литва	5,4	9,1	6,1	5,6	5,2	-0,2	-3,9	-0,9	-0,4
Люксембург	23,1	28,1	17,7	12,7	13	-10,1	-15,1	-4,7	0,3
Угорщина	3,5	4,6	2,8	3,7	4	0,5	-0,6	1,2	0,3
Мальта	14,8	14,8	12	11,5	12,1	-2,7	-2,7	0,1	0,6
Нідерланди	17,8	20,4	15,6	12,7	12,2	-5,6	-8,2	-3,4	-0,5
Австрія	18,1	15,9	12,9	10,9	10,8	-7,3	-5,1	-2,1	-0,1
Польща	9	7	5	5,4	5,5	-3,5	-1,5	0,5	0,1
Португалія	13,8	14,4	8	7,7	8,7	-5,1	-5,7	0,7	1
Фінляндія	25,1	24,8	23,2	21,7	19,6	-5,5	-5,2	-3,6	-2,1
Норвегія	4,7	16,4	8,2	6,5	6	1,3	-10,4	-2,2	-0,5
Швейцарія	4,9	16	10,6	8,3	7,8	2,9	-8,2	-2,8	-0,5
Швеція		26,9	18,1	14,4	13,4	13,4	-13,5	-4,7	-1
Європейський Союз (27 країн)	12,1	13,3	10	8,9	8,9	12,1	13,3	10	8,9
Європейська зона (20 країн з 2023 року)	13,6	14,8	11,2	9,9	9,9	13,6	14,8	11,2	9,9

Джерело: складено і проаналізовано на основі [9]

Проведений аналіз статистичних даних (табл. 1) свідчить, що після завершення пандемії COVID-19 відбулася корекція ринку праці. Якщо у 2021 році частка дистанційної зайнятості в ЄС сягала піку (13,3%), то станом на 2024 рік вона стабілізувалася на рівні 8,9%. І підтвердився висновок, що саме пандемія, яка стала глобальним викликом обумовила активне впровадження та використання дистанційних технологій. Однак, варто зазначити, що для країн-лідерів економічного розвитку (Ірландія, Фінляндія, Нідерланди)

цей показник залишається стабільно високим (від 12% до 20%). Стабільність показників 2023–2024 років підтвердила, дистанційні технології та цифрові комунікації стали невід'ємною частиною архітектури сучасного бізнесу, що вимагає довгострокових рішень щодо захисту даних та управління лояльністю віддаленого персоналу, а питання інтеграції механізмів кадрової безпеки в цифрове середовище переходить із розряду ситуативних завдань у площину стратегічного менеджменту.

Другим викликом, який продемонстрував роль і значення цифрових комунікацій, інформаційно-комунікаційних та дистанційних технологій стало повномасштабне вторгнення Російської Федерації в Україну, яке тримає до цього часу. В умовах високого рівня небезпеки, екстремально невизначених умовах саме цифрові комунікації та технології продемонстрували можливості не тільки для задоволення життєвоважливих потреб населення, але і можливості організації діяльності як державних установ, так і бізнесу.

Станом кінець 2024 року в Україні на єдиному порталі державних послуг «Дія» можна отримати понад 130 електронних послуг та сервісів, у мобільному застосунку «Дія» – близько 30 [10]. У 2024 році 64% громадян отримували державні сервіси онлайн. За три роки кількість користувачів порталу та застосунку зросла з 13% у 2020 році до 51% на початок жовтня 2023 року. Майже 80% оцінили свій досвід як радше або дуже позитивний [11]. У 2024 році через ЦНАПи надано понад 20 млн послуг. Найпопулярнішими серед них стали: реєстрація місця проживання – 6,6 млн; послуги соціального характеру – 3,3 млн; реєстрація нерухомості – 3 млн; паспортні послуги – 1,1 млн; земельні послуги – 562 тис.; реєстрація ВПО – 277 тис.; послуги для ветеранів – 219 тис. [12]. На платформі Дія. Центр у 2024 році з'явилася можливість здійснити попередній запис до 553 ЦНАПів. Також за рік отримано понад 70 тисяч відгуків про роботу ЦНАПів та запущено оновлену оцінку якості послуг. Вже 871 ЦНАП використовує в роботі інформаційні системи, зокрема систему Вулик, а кількість користувачів платформи Дія. Центр уже досягла 640 тисяч. Крім того, у Дія.Центрах запрацювали публічні послуги «Нафтогаз України». Минуло року ЦНАПи пройшли тест на стійкість, актуалізувавши за два місяці дані близько 2 млн військовозобов'язаних [12].

Таким чином, цифровізація в умовах війни перетворилася з інструменту комфорту на базову умову виживання та безпеки, забезпечивши безперервність надання послуг навіть в екстремальних умовах. Інформаційно-комунікаційні технології, цифровізація, мережа ЦНАПів стали критично важливим елементом національної безпеки та соціальної стабільності. Відповідно такі тенденції впливають і на процес управлінської діяльності та організацію бізнес-процесів та потребу у активному розвитку цифрових компетенцій не тільки в технічних працівників, але і управлінського персоналу. Тому що цифровізація відбувається не тільки в секторі державних послуг, але і бізнесі. У бізнесі, пандемія та цифровізація стали каталізаторами розвитку ринку e-commerce, який на початку повномасштабного вторгнення становив 0%, але вже в квітні 2022 року цей показник був вищим, ніж в лютому і січні. Інтернет-магазинам

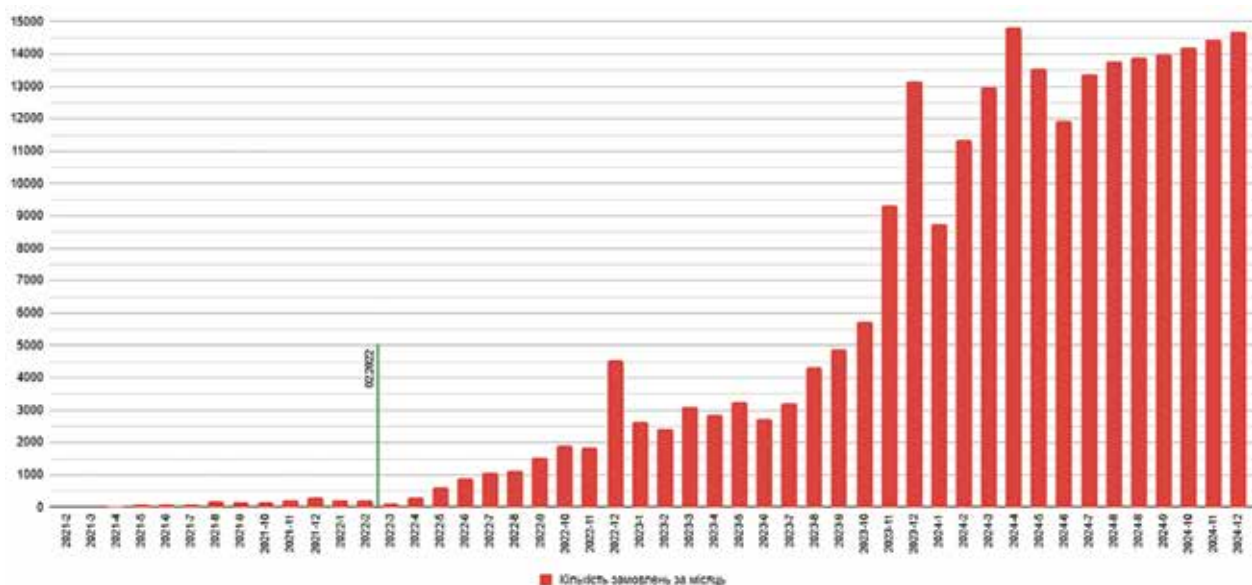


Рис. 1. Кількість замовлень у Інтернет-магазинах в Україні з 2021 по 2024 рік (помісячно)

Джерело: [13]

вистачило буквально 1–2 місяці, щоб наростити і збільшити кількість замовлень, які були до початку вторгнення [13]. Отже, в умовах глобальних викликів (пандемія, війна) саме цифровізація продемонструвала можливості не тільки для того, щоб вистояти, але і розвиватися. Водночас, саме цифровізація стала також глобальним викликом не тільки для бізнесу, але держави та всього суспільства. Динамічний розвиток великих мовних моделей (ШІ) призвів не тільки до нових можливостей, але і загроз.

Так, великі мовні моделі (LLMs), відкрили безпрецедентні можливості для автоматизації складних інтелектуальних завдань, оптимізації процесів та створення персоналізованих сервісів, які супроводжуються зростанням кількості фейків, дипфейків, кібератак, віртуальних шахрайств. У результаті, такий технологічний прорив супроводжується низкою глобальних викликів для управлінців.

1) Кібербезпека та інформаційна загроза. ШІ значно спростив створення високоякісного дезінформаційного контенту (deepfakes), що ускладнює верифікацію даних і становить пряму загрозу національній безпеці та суспільній довірі, особливо в умовах інформаційної війни.

2) Етичні та правові питання. Невизначеність щодо авторських прав на контент, створений ШІ, а також проблема алгоритмічної упередженості (bias), закладеної в навчальні дані, вимагають негайного правового регулювання на державному рівні. Це стосується як бізнес-середовища, так і державного сектору (наприклад, ухвалення рішень у соціальній сфері чи правосудді).

3) Трансформація ринку праці. Масштабна автоматизація, викликана ШІ, створює ризик скорочення робочих місць у сферах, пов'язаних із рутинною інтелектуальною працею (контент-менеджмент, початкове програмування, клієнтська підтримка). Це вимагає від держави та освітньої системи розробки стратегій для масового перекваліфікації робочої сили та розвитку у громадян критичного мислення й «людських» компетенцій, які не підлягають автоматизації.

Саме тому, динамічний розвиток технологій та поява комплексних викликів, пов'язаних із впровадженням ШІ та кіберзахистом, вимагає не просто підвищення кваліфікації окремих фахівців, а формування нових міждисциплінарних команд. В умовах високої невизначеності та необхідності швидкого ухвалення рішень, командна робота стає не додатковою перевагою, а ключовим фактором стійкості та інноваційності. Ефективна команда, що поєднує технічні знання, управлінські навички та розуміння етичних норм, є єдиним механізмом, здатним швидко інтегрувати нові цифрові інструменти та одночасно мінімізувати пов'язані з ними ризики. Ця посилена залежність від цифрових систем та командної взаємодії, зокрема в умовах гібридного або віддаленого формату роботи, створює нові критичні точки вразливості.

Людський фактор залишається найбільш уразливою ланкою в системі кіберзахисту. Відповідно, питання кадрової безпеки виходить на перший план і набуває стратегічного значення (табл.2).

Таблиця 2

**Особливості формування кадрової політики
в умовах змін та глобальних викликів у контексті цифрової безпеки**

Критерій (ознака)	Кадрова політика в умовах змін	Кадрова політика в умовах глобальних викликів
1	2	3
Ключові фактори ризику	Стандартні бізнес-ризик, економічна нестабільність, внутрішня корупція.	Екстремальні зовнішні виклики: пандемія (віддалена робота), повномасштабне вторгнення (військово-політичний ризик), прискорений розвиток ШІ.
Модель організації	Переважно офісна, централізована	Гібридна/віддалена (децентралізована). Розмиття меж між робочим та особистим простором.
Основний фокус загроз	Ненавмисні помилки (низька компетенція), матеріальна шкода (крадіжки, шахрайство).	Інформаційна шкода: репутаційні ризики, колабораціонізм/шпигунство, витік критичних даних через незахищені канали зв'язку, втрата персональних даних,
Периметр безпеки	Чіткий, фізичний: контрольований доступ до приміщень, мереж та обладнання.	Віртуальний, рухомий: периметр переноситься на домашні роутери, особисті пристрої та хмарні сервіси.
Вимоги до персоналу	Відповідність професійним навичкам. Базова комп'ютерна грамотність.	Стійкість (резильєнтність), цифрова гігієна (безпека акаунтів, VPN), медіаграмотність (протиіда ПІСО), цифрова компетентність (базова (A1,A2), середня (B1,B2), висока (C1,C2)).
Навчання персоналу	Регламентоване, періодичне, фокус на правилах трудової дисципліни.	Безперервне, адаптивне, сценарне навчання (фішинг, соціальна інженерія). Фокус на психологічній стійкості.

Продовження таблиці 2

1	2	3
Управління ризиками	Фокус на фізичній та майново-фінансовій безпеці.	Фокус на безпеці даних, репутаційних ризиках в умовах високого рівня невизначеності.
Найм працівників	Оцінка Hard Skills (жорсткі навички). Очні інтерв'ю. Кадрові перевірки фокусуються на минулому досвіді.	Оцінка Soft Skills (гнучкість, стресостійкість) та цифрової компетенції. Пріоритет віддаленим/відео інтерв'ю. Обов'язкова перевірка цифрового сліду та іноді політичної лояльності.
Оцінка ефективності	Базується на присутності на робочому місці (нормо-години) та формальних KPI. Періодичні (річні/піврічні) атестації.	Базується на кінцевому результаті (Output) незалежно від місця. Використання OKR/Agile-методологій. Оцінка впливу на стійкість організації.
Соціальні відносини	Фізично орієнтована корпоративна культура (спільні обіди, офісні заходи, ієрарх.відносини).	Віртуально підтримувана культура. Необхідність постійної цифрової комунікації та управління соціальною ізоляцією персоналу. Зростання значення горизонтальних зв'язків.
Мотивація	Переважно матеріальна (фінансові бонуси, премії, відчутні соціальні пакети – абонементи, транспорт).	Домінування нематеріальної мотивації: свобода вибору місця роботи, гнучкий графік, психологічна підтримка (ментальне здоров'я), відчуття місії та причетності до спільної справи/ стійкості держави.

Джерело: складено автором

Це охоплює не лише перевірку доброчесності персоналу, але й систематичне навчання щодо виявлення фішингу, протидії соціальній інженерії та усвідомлення важливості захисту конфіденційної інформації. Адже, за 18 місяців повномасштабної війни, із січня 2022 року, кількість втручань у роботу сайтів та реєстрів органів державної влади збільшилася у 15 разів проти трьох попередніх років [14]. Зокрема, за період із 2019 по 2021 роки на державний сектор було здійснено 28 352 882 кібератак, тоді як за період із січня 2022 року по 31 серпня 2023 року – 422 063 020 кібератак [14]. Таким чином, доцільно зробити висновок, що глобальні виклики (пандемії, війна, цифровізація, штучний інтелект) у 2020–2024 роках перетворюють кадрову безпеку в потужний інструмент забезпечення стратегічної стійкості організації. Водночас, саме глобальні виклики демонструють потребу у змінах в управлінських концепціях щодо організації діяльності сучасних соціально-економічних систем. Зокрема, у формуванні нових навичок у всіх категорій працівників (технічних, виробничих, управлінських) – «кібергігієни» та «командної роботи». Коли в екстремальних умовах та високого рівня небезпеки потрібно забезпечувати взаємодію, що дозволить досягати поставлених цілей. Оскільки саме цифровізація продемонструвала, які вигоди може отримувати організація від використання командної роботи в організації управлінської діяльності варто наголосити на кількох ключових аспектах.

По-перше, цифрові інструменти забезпечили принципово новий рівень прозорості та швидкості обміну інформацією, що сприяло формуванню команд з високим рівнем взаємодії та оперативності ухвалення рішень. Це дозволило організаціям скорочувати часові витрати на координацію, підвищувати керованість процесів та оперативно реагувати на зміни зовнішнього середовища.

По-друге, цифровізація відкрила можливість ефективно формувати крос-функціональні, проектні та віртуальні команди, що працюють у різних часових поясах і професійних контекстах, але об'єднані спільними цілями та єдиним інформаційним простором. Завдяки цьому компанії змогли більш продуктивно використовувати інтелектуальний потенціал працівників, збільшувати інноваційність рішень та знижувати ризики, пов'язані з фрагментацією управлінських функцій.

По-третє, розвиток цифрових платформ для спільної роботи (Microsoft Teams, Google Workspace, Slack, Jira, Notion, Miro тощо) змінив підходи до організації командної взаємодії, зробивши її більш структурованою, контрольованою та підзвітною. Інструменти аналітики та моніторингу дозволяють керівникам відстежувати прогрес, оцінювати внесок кожного члена команди, оперативно усувати бар'єри та формувати культуру відповідальності. У цілому цифровізація стала каталізатором переходу від традиційних команд до гнучких, мережевих, самоорганізованих команд, для яких характерними є високий рівень взаємної довіри, спільна відповідальність та орієнтація на результат. Таким чином, командна робота в цифровому середовищі не лише підвищує ефективність управлінських процесів, але й створює передумови для розвитку стійкої, адаптивної організаційної структури, здатної функціонувати в умовах невизначеності та швидких технологічних змін. Саме глобальні виклики створили передумови для формування навичок командної роботи у всіх працівників (управлінських, виробничих, технічних) одночасно з цифровими компетенціями.

Однак, у світовій практиці в організації управління сучасними організаціями використовуються різні види команд : традиційні, віртуальні, проєктні, гібридні (поєднання онлайн і офлайн), крос-культурні, креативні, команди змін тощо. Тому виникає необхідність змін у кадровій політиці сучасних організацій в умовах глобальних змін та впровадженні технологій командної роботи, щоб мінімізувати наслідки від втрат репутаційних ризиків та даних, що може призвести до зниження стійкості організацій у довгостроковій перспективі, знижуватимуть рівень конкурентоспроможності організації та її вартість. Тому доцільно проаналізувати особливості формування кадрової політики з використанням різних видів команд (табл.2), які потребують врахування у процесі їх формування, щоб зменшити кількість загроз та втрат вигід при використанні різних підходів до організації роботи в організації. Отже, глобальні виклики (пандемії, війна, цифровізації) обумовлюють потребу у зміні кадрової політики сучасної організації, яка стає одним із важливих інструментів управління сучасних управлінців, оскільки зростання зовнішньої та внутрішньої міграції населення призводить до браку кваліфікованих кадрів, значних змін у соціальних, вікових структурах колективів та населення громади та країни в цілому. Зростання ролі значення фізичної безпеки працівників, а в умовах повномасштабного вторгнення стає першочерговою задачею.

Таблиця 3

**Особливості формування кадрової політики
в умовах глобальних викликів для різних видів команд**

Критерій командної роботи	Традиційна команда	Проектні команди	Віртуальні команди	Гібридні команди
1. Модель роботи/ Структура	Жорстка, ієрархічна. Централізований офіс.	Гнучка, міжфункціональна. Тимчасовий склад, орієнтація на дедлайн.	Географічно розподілена. Повна залежність від асинхронної комунікації.	Комбінована: ротація між офісом та віддаленою роботою.
2. Найм працівників	Фокус на спеціалізації та фізичній присутності.	Фокус на експертних знаннях та здатності до швидкої інтеграції.	Пріоритет на цифровій грамотності та навичках самоорганізації.	Акцент на адаптивності та здатності ефективно працювати в обох режимах.
3. Оцінка ефективності	Базується на нормо-годинах та індивідуальних KPI.	Базується на оцінці результаті проєкту та досягненні колективних KPI.	Базується виключно на кінцевому результаті (Output).	Збалансована оцінка: індивідуальний внесок + загальні критерії фізичної присутності та роботи.
4. Мотивація	Переважно матеріальна (бонуси, кар'єрний ріст).	Визнання досягнень, можливість працювати над стратегічними цілями.	Автономія, гнучкий графік, психологічна підтримка.	Гнучкість + приналежність до певної соціальної групи. Акцент на спільній місії.
5. Навчання персоналу	Фокус на трудовій дисципліні та профільних знаннях.	Фокус на кросс-функціональному навчанні та командному вирішенні проблем.	Обов'язкове навчання цифрової гігієни (VPN, шифрування, ШП-ризик).	Поєднання навичок співпраці в офісі з протоколами цифрової безпеки вдома.
	Цифрова компетентність та кібергігієна (базовий рівень)	Цифрова компетентність та кібергігієна (просунутий рівень)		
6. Вимоги до персоналу (КБ)	Чітке дотримання фізичних інструкцій.	Висока лояльність та комунікативна дисципліна.	Самодисципліна, стресостійкість, медіаграмотність.	Адаптивність та проактивне дотримання протоколів безпеки.

Джерело: складено автором

В цих умовах командна робота і цифрові технології стають невід'ємними елементами процесу управління персоналом, а навички командної роботи та цифрової компетентності дозволяє вирішувати

професійні завдання. Тому виникає потреба у впровадженні гнучких, адаптивних та людино-центричних підходах у кадровій політиці з урахуванням безпекових аспектів. Коли кадрова політика: по-перше, повинна враховувати та бути орієнтованою на розвиток нових компетенцій як на рівні працівників, так і керівників. Зокрема, для працівників: вимоги виходять за рамки *hard skills*; критично важливими стають *soft/digital skills*: самоорганізація (*time management*), цифрова гігієна, ефективна письмова комунікація та резильєнтність (стресостійкість). Для керівників: адміністративний контроль поступається місцем лідерству через довіру, управлінню асинхронною командою та забезпеченню психологічної підтримки, а також вмінню балансувати ресурсами та приймати кризові рішення.

По-друге, враховувати зміни у структурі та моделі управління. Зокрема, фокус при наймі на роботу зміщується від вузької спеціалізації до експертних знань, цифрової грамотності, самоорганізації та адаптивності. Мотивація еволюціонує від суто матеріальної до визнання автономії, гнучкого графіка та приналежності до спільної місії, що підкреслює зростання важливості психологічних факторів.

По-третє, зростає роль і значення цифрових комунікацій у процесі управління[15], що потребує врахування у програмах навчання, професійного розвитку та формування посадових інструкцій для працівників на різних рівнях управління.

По-четверте, кадрова політика повинна враховувати зміни у інформаційній й цифровій безпеці (табл. 4), оскільки основний фокус загроз зміщується від внутрішнього шахрайства до зовнішніх кібератак, соціальної інженерії (фішинг), а також витоку даних через вразливість домашніх мереж та різницю в рівнях захисту. Це актуалізує обов'язкове навчання персоналу психологічній стійкості та протоколам цифрової гігієни.

Таблиця 4

**Особливості формування кадрової політики в умовах глобальних викликів
та використання різних видів команд (безпековий аспект)**

Критерій командної роботи	Традиційна команда	Проектні команди	Віртуальні команди	Гібридні команди
1.Периметр безпеки	Фізичний, контроль робочого устаткування.	Фізичний та віртуальний контроль. Складна гібридна безпека. Необхідність управління різними політиками доступу. Висока вразливість домашніх мереж.		
2.Основний фокус загроз	Ненавмисні помилки та внутрішнє шахрайство.	Втрата даних через неякісну деактивацію прав. Кібератаки, методи соціальної інженерії (фішинг, вішинг тощо), шкідливе програмне забезпечення тощо, які спрямовані на особисті та робочі облікові записи працівників. Колабораціонізм/ шпигунство та витік даних через різницю в рівнях захисту.		
3.Управління ризиками КБ	Контроль доступу, моніторинг робочого часу.	Жорстке управління доступом (JIT – Just-in-Time Access) та швидке відкликання прав.	Комплексний моніторинг активності та обов'язкове навчання психологічній стійкості.	Впровадження технологій нульової довіри (Zero Trust) та аудит політик доступу до хмарних ресурсів.
4.Ключові компетенції (працівник)	Профільні <i>hard skills</i> , Дотримання інструкцій.	Багатозадачність, кросфункціональність, взаємозамінність.	Самоорганізація (<i>Time Management</i>), Цифрова гігієна, ефективна письмова комунікація.	Гнучкість графіка, Вміння перемикатися між онлайн/ офлайн комунікацією, стресостійкість/ Резильєнтність.
5.Ключові компетенції (Керівник)	Адміністративний контроль, Технічна експертиза.	Управління дедлайнами, Ресурсний менеджмент, Ефективне делегування.	Лідерство через довіру, Управління асинхронною командою, забезпечення психологічної підтримки.	Управління справедливістю, Балансування ресурсами, Кризове прийняття рішень.
6. Види ризиків	Операційні ризики (саботаж, залежність від фізичної інфраструктури). Ризик корупції.	Ризик знань (втрата експертизи після розпуску). Ризик дедлайну (<i>failure to meet temporary goals</i>). Кіберризик (через часту зміну прав доступу).	Кіберризик (фішинг, небезпечні мережі). Психологічний ризик (вигорання, ізоляція, втрата лояльності).	Ризик нерівності (<i>proximity bias</i>). Комунікаційні розриви (втрата інформації між режимами). Складність безпеки (управління подвійним доступом).

Джерело: складено автором

Таким чином, ефективна кадрова політика в умовах глобальних викликів повинна бути адаптивною, технологічно інтегрованою та цілісною, здатна балансувати гнучкість і безпеку. Вона має не лише підтримувати цифровізацію та крос-функціональність.

Висновки. Глобальні виклики 2020–2024 років – пандемія, війна, цифровізація та розвиток ІІІ – суттєво змінили підходи до управління персоналом підприємства. Цифрові комунікації та дистанційні технології стали основою безперервності роботи, але водночас посилили ризики кіберзагроз і витоку даних, репутаційних втрат. Продemonстрували потенційні можливості використання командної роботи, яка є інтегрованою у сучасні цифрові комунікації (цифрові платформи, соціальні мережі, цифрові додатки тощо) і дозволяє формувати стійкість організації. Це, в свою чергу, обумовлює потребу у трансформації кадрової політики, яка повинна враховувати сучасні тенденції та потребу врахування цифрової компетентності та навичок кібергігієни, що є прямою відповіддю на загрози соціальної інженерії, дезінформації та посилення ІІІ. Це дозволить формувати адаптивність системи управління до глобальних викликів та мінімізувати наслідки цих впливів, формувати стійкість у довгостроковій перспективі.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ:

1. Осокін М., Осокіна А. Цифрові комунікації в системі управління бізнесом. *Економіка та суспільство*, 2024. № 64. DOI: <https://doi.org/10.32782/2524-0072/2024-64-31>
2. Berezko O., Maksymovych S. International and intercultural communication in the globalizing society. *Інформація, комунікація, суспільство 2013* : матеріали 2-ої Міжнародної наукової конференції ІКС-2013, 16–19 травня 2013 року, Україна, Львів, Славське / Національний університет «Львівська політехніка», Кафедра соціальних комунікацій та інформаційної діяльності, Кафедра інформаційних систем і мереж. Львів : Видавництво Львівської політехніки, 2013. С. 112–113.
3. Баценко Л., Галенін Р. Роль цифрових комунікацій в управлінні цифровою трансформацією організації: бачення організаційного адміністрування. *Вісник Київського інституту бізнесу і технологій*, № 51 (2), 2024. С. 10–25. URL: <https://www.herald.kibit.edu.ua/index.php/visnyk/article/view/1793/156>
4. Баркова К. О. Командоутворення як складова формування успішного корпоративного середовища. *Український журнал прикладної економіки та техніки*. 2023. Т. 8. № 4. С. 194–199.
5. Tuckman B. Bruce Tuckman's Team Development Model. 1965. URL: <https://lfhe.ac.uk/download.../3C6230CF-61E8-4C5E-9A0C1C81DCDEDA2>
6. Douglas K. Smith. The Wisdom of Teams: Creating the High-performance Organization. Harvard Business School Press, 1993. 291pp.
7. Філоненко, С. Ф., Мужик І. М., Німченко Т. В. Система попередження витоку персональних даних мережевими каналами. *Ukrainian Scientific Journal of Information Security*. 2014. Vol. 20, № 3. Р. 279–285.
8. Малюга В., Кузьменко М. Проблема кадрової безпеки у сучасних наукових дослідженнях. *Вісник Національного університету оборони України*, 2021, 63(5). с. 70–79. DOI: <https://doi.org/10.33099/2617-6858-2021-63-5-70-79>
9. Eurostat (2025), “Employed persons working from home as a percentage of the total employment, by sex, age and professional status (%)”, available at: https://ec.europa.eu/eurostat/databrowser/view/LFSA_EHOMP/default/table?lang=en
10. У Мінцифри пояснили, чому на порталі «Дія» у чотири рази більше послуг, ніж у застосунку. URL: <https://www.ukrinform.ua/rubric-society/3952337-na-portali-dia-mozna-otrimati-ponad-130-elektronnih-poslug-u-zastosunku-blizko-30.html>
11. Понад 60% українців отримують держпослуги онлайн: результати дослідження. URL: <https://testbed.diia.org.ua/platform/t-news/details?id=16>
12. Близько 5 тисяч точок та 20 мільйонів послуг у ЦНАПах – головні досягнення 2024 року. URL: <https://thedigital.gov.ua/news/progress/blizko-5-tisyach-tochok-ta-20-milyoniv-poslug-u-tsnapakh-golovni-dosyagnennya-2024-roku>
13. Алла Петриченко. Як українські інтернет-магазини працювали у 2021–2024 роках: e-commerce статистика і прогнози. URL: <https://shop-express.ua/ukr/blog/ecommerce-statistics/>
14. Вдовенко О. Війна у цифровому вимірі та права людини. Підсумковий звіт із 24 лютого 2022 року по 31 серпня 2023 року. Київ: ГО «Платформа прав людини», 2023. 84 с.
15. Глебова А. О., Кравченко В. В. Розвиток цифрових комунікацій в умовах діджиталізації економіки України: проблеми та можливості. *Ефективна економіка*. 2021. № 9. URL: <http://www.economy.nayka.com.ua/?op=1&z=9277>

REFERENCES:

1. Osokin M., Osokina A. (2024) Tsyfrovi komunikatsii v systemi upravlinnia biznesom [Digital communications in business management]. *Ekonomika ta suspilstvo*, no. 64. DOI: <https://doi.org/10.32782/2524-0072/2024-64-31>
2. Berezko O., Maksymovych S. (2013) International and intercultural communication in the globalizing society. *Informatsiia, komunikatsiia, suspilstvo 2013*: materialy 2-oi Mizhnarodnoi naukovoï konferentsii IKS-2013, 16–19 travnia 2013 roku, Ukraina, Lviv, Slavske. Lviv: Vydavnytstvo Lvivskoi politekhniki, pp. 112–113.

3. Batsenko L., Halenin R. (2024) Rol cyfrovych komunikatsii v upravlinni cyfrovoi transformatsiiei orhanizatsii: bachennia orhanizatsiinoho administruvannia [The role of digital communications in managing digital transformation of an organization]. *Visnyk Kyivskoho instytutu biznesu i tekhnologii*, no. 51(2), pp. 10–25. Available at: <https://www.herald.kibit.edu.ua/index.php/visnyk/article/view/1793/156>
4. Barkova K. O. (2023) Komandoutvorennia yak skladova formuvannia uspishnogo korporatyvnoho seredovysha [Team building as a component of creating a successful corporate environment]. *Ukrainskyi zhurnal prykladnoi ekonomiky ta tekhniky*, vol. 8, no. 4, pp. 194–199.
5. Tuckman B. (1965) Bruce Tuckman's Team Development Model. Available at: <https://www.lfhe.ac.uk/download/3C6230CF-61E8-4C5E-9A0C1C81DCDEDC42>
6. Smith D. K. (1993) The Wisdom of Teams: Creating the High-performance Organization. Harvard Business School Press, 291 pp.
7. Filonenko S. F., Muzhyk I. M., Nimchenko T. V. (2014) Systema poperedzhennia vytoku personalnykh danykh merezhevymy kanalamy [System of preventing personal data leakage through network channels]. *Ukrainian Scientific Journal of Information Security*, vol. 20, no. 3, pp. 279–285.
8. Maliuha V., Kuzmenko M. (2021) Problema kadrovoi bezpeky u suchasnykh naukovykh doslidzhenniakh [The problem of personnel security in modern research]. *Visnyk Natsionalnoho universytetu oborony Ukrainy*, no. 63(5), pp. 70–79. DOI: <https://doi.org/10.33099/2617-6858-2021-63-5-70-79>
9. Eurostat (2025) Employed persons working from home as a percentage of the total employment, by sex, age and professional status (%). Available at: https://ec.europa.eu/eurostat/databrowser/view/LFSA_EHOMP/default/table?lang=en
10. U Mintsyfyri poiasnyly, chomu na portali “Diia” u chotyry razy bilshe posluh, nizh u zastosunku [The Ministry of Digital Transformation explained why the Diia portal has four times more services than the app]. Available at: <https://www.ukrinform.ua/rubric-society/3952337-na-portali-dia-mozna-otrimati-ponad-130-elektronnih-poslug-u-zastosunku-blizko-30.html>
11. Ponad 60% ukraintsiv otrymuyut derzhposluhy online: rezultaty doslidzhennia [Over 60% of Ukrainians receive public services online: research results]. Available at: <https://testbed.diia.org.ua/platform/t-news/details?id=16>
12. Blyzko 5 tysiach tochok ta 20 milioniv posluh u TsNAPakh – holovni dosiagnennia 2024 roku [About 5,000 service points and 20 million services in ASCs – key achievements of 2024]. Available at: <https://thedigital.gov.ua/news/progress/blizko-5-tisyach-tochok-ta-20-milyoniv-poslug-u-tsnapakh-golovni-dosyagnennia-2024-roku>
13. Petrychenko A. (2024) Yak ukrainski internet-mahazyny pratsiuvaly u 2021–2024 rokakh: e-commerce statystyka i prohnozy [How Ukrainian online stores operated in 2021–2024: e-commerce statistics and forecasts]. Available at: https://shop-express.ua/ukr/blog/ecommerce-statistics/?utm_source=chatgpt.com
14. Vdovenko O. (2023) Viina u tsyfrovomu vymiri ta prava liudyny. Pidsumkovyi zvit iz 24 liutoho 2022 roku po 31 serpnia 2023 roku [War in the digital dimension and human rights. Final report from February 24, 2022 to August 31, 2023]. Kyiv: Platforma prav liudyny, 84 p.
15. Hliebova A. O., Kravchenko V. V. (2021) Rozvytok tsyfrovych komunikatsii v umovakh didzhitalizatsii ekonomiky Ukrainy: problemy ta mozhlyvosti [Development of digital communications in the context of Ukraine's digitalization: problems and opportunities]. *Efektivna ekonomika*, no. 9. Available at: <http://economy.nayka.com.ua/?op=1&z=9277>

УДК 658.3: 351/354

JEL J24, M12, M15

Глєбова Алла Олександрівна, кандидат економічних наук, доцент, доцент кафедри менеджменту і логістики, Національний університет «Полтавська політехніка імені Юрія Кондратюка». **Організація командної роботи в умовах глобальних викликів у контексті цифрової та кадрової безпеки.**

У статті досліджено особливості організації командної роботи в умовах глобальних викликів та відображення її у кадровій політиці організації. Встановлено, що глобальні виклики 2020–2024 років – пандемія COVID-19, повномасштабна війна в Україні, прискорена цифровізація, гібридні форми зайнятості та стрімкий розвиток штучного інтелекту – кардинально трансформували вимоги до організації командної роботи та кадрової політики сучасних організацій. Цифрові комунікації, дистанційні технології та хмарні сервіси стали структуротворчими елементами управлінської діяльності, визначаючи нову архітектуру взаємодії між працівниками та керівниками. Водночас цифрове середовище посилює ризики витоку даних, кібератак, соціальної інженерії та інформаційних маніпуляцій, що висуває підвищені вимоги до кадрової безпеки. Відповідно, це обумовлює потребу у трансформації кадрової політики організації та її орієнтації на впровадження нових підходів до організації процесів із управління персоналом на основі врахування цифрової компетентності та навичок кібергігієни, що є прямою відповіддю на загрози соціальної інженерії, дезінформації та посилення ШІІ.

Ключові слова: кадрова безпека, цифрова компетентність, цифрова безпека, кадрова політика, менеджмент, управління змінами.

UDC 658.3: 351/354

JEL J24, M12, M15

Alla Hliebova, Candidate of Economic Sciences, Docent, Associate Professor at the Department of Management and Logistics, National University “Yuri Kondratyuk Poltava Polytechnic”. **Organization of teamwork in the context of global challenges in the context of digital and personnel security.**

The article examines the peculiarities of organizing teamwork in the context of global challenges and its reflection in the organization's personnel policy. It has been established that the global challenges of 2020–2024 – the COVID-19 pandemic, full-scale war in Ukraine, accelerated digitalization, hybrid forms of employment, and the rapid development of artificial intelligence–have radically transformed the requirements for teamwork organization and personnel policy in modern organizations. Digital communications, remote technologies, and cloud services have become structural elements of management activities, defining a new architecture of interaction between employees and managers. At the same time, the digital environment has increased the risks of data leaks, cyberattacks, social engineering, and information manipulation, which places increased demands on personnel security. Accordingly, this necessitates the transformation of an organization's personnel policy and its focus on implementing new approaches to the organization of personnel management processes based on digital competence and cyber hygiene skills, which is a direct response to the threats of social engineering, disinformation, and the rise of AI. The study identifies the characteristics of human resource policy that is being shaped in the context of change and global challenges affecting the stability of organizations. Analysis of EU and Ukrainian statistics has demonstrated the steady growth of remote work and digital services as prerequisites for ensuring the continuity of business processes, public administration, and social infrastructure even in conditions of extreme uncertainty. The study emphasizes that digitalization is not only a tool for increasing productivity, but also a factor in the formation of new competencies necessary for effective team interaction: digital literacy, psychological resilience, and the ability to work in virtual, project-based, hybrid, and interdisciplinary teams. Therefore, the author analyzed the peculiarities of forming personnel policy regarding the practice of using different types of teams. A comparison of different team models has shown that HR policy must evolve from traditional administrative control to flexible, people-centered, and security-oriented approaches. The importance of assessing digital competencies, self-organization skills, the ability to work in asynchronous digital environments, and the willingness to adhere to cyber hygiene protocols is growing. For managers, leadership through trust, managing the psychological resilience of the team, crisis decision-making, and ensuring information security are becoming key. The study substantiates that effective team management in the face of global challenges is only possible if digital communications and personnel security are integrated into a single management system. This approach ensures the strategic stability of the organization, improves the quality of team interaction, minimizes the risks of data leaks and reputational damage, and contributes to the formation of modern human resources capable of working in highly turbulent conditions. At the same time, digitalization and the development of teamwork are key tools for adapting socio-economic systems to the new conditions of global instability.

Key words: personnel security, digital competence, digital security, personnel policy, management, change management.