Ірина П. Мігус*

ЕКОНОМІЧНА БЕЗПЕКА ІТ-ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВОЇ КОМАНДНОЇ ВЗАЄМОДІЇ

У статті досліджено економічну безпеку ІТ-підприємств в умовах цифрової командної взаємодії. Обґрунтовано, що для підприємств ІТ-сфери командна робота є не лише організаційною формою виконання проєктів, а й важливим чинником формування, підтримання або послаблення економічної безпеки. Визначено, що цифрова командна взаємодія охоплює комунікацію, координацію завдань, управління знаннями, розподіл ролей, спільну розробку програмних продуктів, контроль доступу до інформаційних ресурсів, захист інтелектуальної власності та підтримання продуктивності в умовах дистанційної, гібридної або розподіленої роботи. Розкрито особливості цифрової командної взаємодії в ІТ-підприємствах, зокрема залежність від цифрових платформ, високий рівень автономії працівників, проєктний характер діяльності, міжфункціональність команд, значення швидкості комунікації, ризики втрати знань, кіберзагрози та потребу в захисті комерційної таємниці. Систематизовано типи командної взаємодії та типи команд, характерні для ІТ-підприємств, а також визначено їх вплив на фінансову, кадрову, інформаційну, інтелектуальну, організаційну, технологічну та репутаційну складові економічної безпеки. Доведено, що цифрова командна взаємодія може одночасно посилювати економічну безпеку через підвищення гнучкості, продуктивності, швидкості ухвалення рішень і прозорості процесів, а також створювати додаткові ризики, пов'язані з інформаційними витоками, неузгодженістю дій, залежністю від цифрових сервісів, емоційним вигоранням, кадровою нестабільністю та втратою контролю над знаннями. Запропоновано розглядати управління цифровою командною взаємодією як складову системи економічної безпеки ІТ-підприємства.

Ключові слова: *економічна безпека; ІТ-підприємство; цифрова командна взаємодія; командна робота; інформаційна безпека; інтелектуальна власність; кадрова безпека; цифрове управління; проєктні команди.*

Табл. 4. Рис. 1. Літ. 11.

DOI: 10.32752/1993-6788-2026-1-296-442-455

ORCID: https://orcid.org/0000-0001-6939-9097

Iryna Mihus

ECONOMIC SECURITY OF IT ENTERPRISES IN THE CONDITIONS OF DIGITAL TEAM INTERACTION

The article examines the economic security of IT enterprises in the conditions of digital team interaction. The relevance of the study is determined by the fact that IT enterprises operate in a highly dynamic environment where economic results depend not only on financial resources, technologies, and market positioning, but also on the quality of teamwork, digital communication, knowledge exchange, and protection of intellectual assets. The article argues that digital team interaction should be considered not only as an organizational form of project implementation, but also as an important element of the economic security system of IT enterprises. Digital team interaction includes communication, task coordination, knowledge management, role distribution, joint software development, access control, protection of confidential information, and productivity support in remote, hybrid, and distributed work formats. The methodological basis of the study includes a systematic approach, structural analysis, logical generalization, comparison, and synthesis of theoretical provisions concerning economic security, team management, digital work,

* "KROK" University. Ukraine. Scientific Center of Innovative Research. Estonia.

information security, and project management. The main results of the study include the systematization of types of digital team interaction and types of teams typical for IT enterprises. The article identifies the influence of digital team interaction on the financial, personnel, information, intellectual, organizational, technological, and reputational components of economic security. It is substantiated that digital team interaction can strengthen economic security by increasing flexibility, productivity, transparency, speed of decision-making, and adaptability of IT enterprises. At the same time, it may create additional risks related to data leakage, cyber threats, dependence on digital platforms, loss of tacit knowledge, weak coordination, employee burnout, staff turnover, and uncontrolled access to intellectual property. The practical value of the study lies in the development of an integrated approach to managing digital team interaction as a component of the economic security system of IT enterprises.

Keywords: *economic security; IT enterprise; digital team interaction; teamwork; information security; intellectual property; personnel security; digital management; project teams.*

Peer-reviewed, approved and placed: *12.02.2026*

Постановка проблеми. IT-сфера є однією з найбільш динамічних галузей сучасної економіки, у якій конкурентоспроможність підприємств визначається не лише рівнем технологічної експертизи, фінансовими ресурсами або доступом до ринків, а й здатністю ефективно організовувати командну роботу. Для IT-підприємств команда виступає базовою одиницею створення цінності, оскільки саме через взаємодію розробників, тестувальників, бізнес-аналітиків, дизайнерів, менеджерів проєктів, DevOps-фахівців, спеціалістів із кібербезпеки та інших учасників формується кінцевий програмний продукт або цифрова послуга. У цьому контексті командна взаємодія є не допоміжним організаційним процесом, а ключовим елементом функціонування IT-підприємства.

Поширення дистанційної, гібридної та розподіленої роботи суттєво змінило характер командної взаємодії в IT-сфері. Якщо раніше значна частина комунікації, координації та контролю здійснювалася в межах фізичного офісного простору, то нині командна робота дедалі більше реалізується через цифрові платформи, системи управління проєктами, корпоративні месенджери, відеоконференції, хмарні сервіси, репозиторії коду, таск-трекери та інструменти спільної розробки. Така трансформація створює нові можливості для гнучкості, масштабування, залучення фахівців із різних країн і прискорення проєктної роботи. Водночас вона формує нові ризики для економічної безпеки підприємства.

Економічна безпека IT-підприємства охоплює захист фінансових, кадрових, інформаційних, інтелектуальних, технологічних, організаційних і репутаційних ресурсів від внутрішніх і зовнішніх загроз. В умовах цифрової командної взаємодії ці складові стають особливо взаємопов'язаними. Наприклад, слабкий контроль доступу до репозиторіїв коду може призвести не лише до інформаційних втрат, а й до втрати інтелектуальної власності, фінансових збитків і репутаційних наслідків. Неефективна комунікація в команді може спричинити затримки у виконанні проєкту, перевитрати бюджету, конфлікти з клієнтами та зниження якості продукту. Висока плинність кадрів може призвести до втрати унікальних знань, порушення строків розробки та зниження інноваційного потенціалу підприємства.

Проблема забезпечення економічної безпеки ІТ-підприємств в умовах цифрової командної взаємодії полягає в тому, що традиційні підходи до економічної безпеки часто зосереджуються на фінансовому контролі, захисті інформації, кібербезпеці або правових аспектах діяльності. Однак вони не завжди враховують управлінську роль командної взаємодії, яка безпосередньо впливає на продуктивність, якість продукту, збереження знань, захист інтелектуальної власності, лояльність працівників і стійкість бізнес-процесів. Тому цифрова командна взаємодія має розглядатися не лише як інструмент організації роботи, а як окрема управлінська площина забезпечення економічної безпеки ІТ-підприємства.

Актуальність дослідження посилюється тим, що ІТ-підприємства часто працюють у проєктному форматі, мають високу залежність від людського капіталу, інтелектуальної власності, даних, цифрової інфраструктури та довіри клієнтів. У таких умовах будь-яке порушення командної взаємодії може швидко трансформуватися в економічні втрати. Саме тому виникає необхідність комплексного аналізу типів цифрової командної взаємодії, типів команд в ІТ-підприємствах, особливостей їх функціонування та впливу на різні складові економічної безпеки.

Аналіз останніх досліджень і публікацій. Проблематика економічної безпеки підприємств розглядається у науковій літературі як система захисту життєво важливих ресурсів, інтересів і потенціалу підприємства від внутрішніх та зовнішніх загроз. У класичних і сучасних підходах до економічної безпеки акцент робиться на фінансовій стійкості, ресурсній забезпеченості, конкурентоспроможності, інформаційній захищеності, кадровій стабільності та здатності підприємства адаптуватися до змін зовнішнього середовища [1; 2]. Для ІТ-підприємств ці положення мають специфічне значення, оскільки основними об'єктами захисту є не лише фінансові активи, а й знання, програмний код, цифрова інфраструктура, клієнтські дані, компетентності персоналу, інноваційні рішення та репутація.

Окремий напрям досліджень пов'язаний із командною роботою та організацією взаємодії в проєктних командах. У працях, присвячених командному менеджменту, підкреслюється, що результативність команди залежить від чіткого розподілу ролей, якості комунікації, довіри, спільного розуміння цілей, психологічної безпеки, компетентності учасників і здатності до координації дій [3; 4]. Для ІТ-сфери ці положення є особливо важливими, оскільки більшість завдань має комплексний характер і потребує узгодженої роботи фахівців із різними функціональними ролями. Розробка програмного продукту не може бути ефективною без взаємодії технічних і нетехнічних спеціалістів, зокрема розробників, аналітиків, тестувальників, дизайнерів і менеджерів.

Значна увага в сучасних дослідженнях приділяється цифровій трансформації командної роботи. Поширення дистанційної та гібридної зайнятості посилило значення цифрових платформ, хмарних сервісів, систем управління проєктами, корпоративних месенджерів і репозиторіїв коду [5; 6]. Дослідники наголошують, що цифрова взаємодія підвищує гнучкість команд, дозволяє залучати фахівців незалежно від географічного розташування,

прискорює обмін інформацією та створює умови для масштабування бізнесу. Водночас вона може посилювати ризики фрагментації комунікації, інформаційного перевантаження, втрати неформальних знань, зниження командної згуртованості та ускладнення контролю за виконанням завдань [5; 7].

У контексті ІТ-підприємств важливе місце посідають дослідження agile-підходів, Scrum, Kanban, DevOps і продуктових команд. Ці підходи передбачають високий рівень автономії команд, ітеративну розробку, короткі цикли планування, постійний зворотний зв'язок, швидку адаптацію до змін вимог і тісну взаємодію між учасниками процесу [8; 9]. З одного боку, такі підходи сприяють підвищенню продуктивності, гнучкості й інноваційності. З іншого боку, вони потребують зрілої культури відповідальності, прозорої комунікації, цифрової дисципліни та належного управління знаннями. За відсутності цих передумов гнучкі методології можуть не знижувати, а посилювати організаційні ризики.

Питання інформаційної та кібербезпеки також широко представлені в наукових і практичних джерелах. Міжнародні стандарти управління інформаційною безпекою та кіберризиками акцентують увагу на управлінні доступом, захисті інформаційних активів, оцінюванні ризиків, контролі постачальників, кібергігієні персоналу та безперервності діяльності [10; 11]. Для ІТ-підприємств ці положення набувають особливого значення в умовах цифрової командної взаємодії, коли працівники можуть мати доступ до критичних даних із різних локацій, використовувати різні цифрові пристрої, працювати з хмарними сервісами та брати участь у кількох проєктах одночасно.

Разом із тим, попри значну кількість досліджень з економічної безпеки, командного менеджменту, цифрової трансформації та кібербезпеки, низка питань залишається недостатньо опрацьованою. По-перше, у науковій літературі економічна безпека ІТ-підприємств часто розглядається переважно через фінансові, інформаційні або технічні ризики, тоді як управління командною взаємодією не завжди виділяється як самостійний елемент системи безпеки. По-друге, недостатньо досліджено вплив різних типів цифрової командної взаємодії на окремі складові економічної безпеки, зокрема кадрову, інтелектуальну, організаційну та репутаційну.

По-третє, невирішеною залишається проблема систематизації типів команд в ІТ-підприємствах із позиції їхнього впливу на економічну безпеку. Наприклад, продуктова команда, проєктна команда, DevOps-команда, команда кібербезпеки або віддалена міжнародна команда мають різні ризики, різний рівень доступу до критичних ресурсів і різну залежність від цифрових інструментів. По-четверте, потребує подальшого вивчення питання збереження знань і захисту інтелектуальної власності в умовах високої мобільності ІТ-фахівців. По-п'яте, недостатньо розкрито зв'язок між психологічною безпекою, цифровою культурою, командною довірою та економічною безпекою підприємства. Отже, наукова проблема полягає в необхідності комплексного обґрунтування ролі цифрової командної взаємодії в системі економічної безпеки ІТ-підприємств.

Метою статті є обґрунтування ролі цифрової командної взаємодії в забезпеченні економічної безпеки ІТ-підприємств, систематизація типів

командної взаємодії та типів команд, характерних для ІТ-сфери, а також визначення їх впливу на складові економічної безпеки підприємства.

Для досягнення поставленої мети визначено такі завдання: уточнити зміст економічної безпеки ІТ-підприємств в умовах цифрової командної взаємодії; охарактеризувати особливості цифрової командної роботи в ІТ-сфері; систематизувати типи командної взаємодії та типи команд в ІТ-підприємствах; визначити вплив цифрової командної взаємодії на фінансову, кадрову, інформаційну, інтелектуальну, організаційну, технологічну та репутаційну безпеку; запропонувати управлінську логіку забезпечення економічної безпеки ІТ-підприємств через ефективне управління цифровою командною взаємодією.

Основні результати дослідження. Економічна безпека ІТ-підприємства в умовах цифрової командної взаємодії може бути визначена як стан захищеності фінансових, інформаційних, кадрових, інтелектуальних, технологічних, організаційних і репутаційних ресурсів підприємства, за якого командна робота забезпечує стабільність бізнес-процесів, збереження критичних знань, захист даних, результативність проєктів і здатність підприємства створювати довгострокову вартість. Таке розуміння дозволяє відійти від вузького трактування економічної безпеки як фінансового контролю або захисту від втрат і розглядати її як інтегровану управлінську систему [1; 2; 10].

Для ІТ-підприємств особливе значення має те, що основний результат діяльності створюється не матеріальними активами, а інтелектуальним капіталом, програмним кодом, цифровими продуктами, даними, алгоритмами, технічною експертизою та здатністю команд швидко перетворювати знання на ринкову цінність. Саме тому командна взаємодія безпосередньо впливає на економічну безпеку. Якщо команда працює узгоджено, підприємство отримує вищу продуктивність, кращу якість продукту, нижчі транзакційні витрати, швидший вихід на ринок і кращу репутацію перед клієнтами. Якщо командна взаємодія порушена, виникають затримки, дублювання завдань, конфлікти, технічні помилки, витоки інформації, втрата знань і фінансові збитки [3; 4; 8].

Цифрова командна взаємодія в ІТ-підприємствах має низку специфічних ознак. По-перше, вона здійснюється переважно через цифрове середовище, тобто платформи управління проєктами, системи контролю версій, корпоративні месенджери, відеоконференції, хмарні сховища, CRM-системи, ERP-системи та системи кіберзахисту. По-друге, вона має високий рівень документованості, оскільки значна частина комунікацій, завдань, рішень і технічних змін фіксується в цифрових інструментах. По-третє, вона характеризується підвищеною залежністю від якості цифрової культури, оскільки працівники мають не лише володіти технічними навичками, а й дотримуватися правил інформаційної безпеки, цифрової етики, кібергігієни та відповідального використання даних [5; 10; 11].

По-четверте, цифрова командна взаємодія часто відбувається в умовах географічної розподіленості працівників. ІТ-команда може об'єднувати фахівців із різних міст, країн і часових поясів, що посилює гнучкість

підприємства, але одночасно ускладнює координацію, контроль, підтримання довіри та управління конфліктами. По-п'яте, така взаємодія має високий рівень залежності від неформальних знань, які не завжди фіксуються в документації. У разі звільнення ключового працівника або втрати комунікації між учасниками команда може втратити важливу частину знань про архітектуру продукту, клієнтські вимоги, технічні рішення або внутрішні процеси [6; 7].

З огляду на це доцільно систематизувати основні типи цифрової командної взаємодії, характерні для IT-підприємств.

Таблиця 1. **Типи цифрової командної взаємодії в IT-підприємствах,** *сформовано автором на основі [3; 5; 8; 10; 11]*

Тип цифрової командної взаємодії	Зміст	Основні цифрові інструменти	Значення для економічної безпеки
Комунікаційна взаємодія	Обмін інформацією, обговорення завдань, уточнення вимог, проведення зустрічей	Slack, Microsoft Teams, Google Meet, Zoom, корпоративні месенджери	Зменшує ризики непорозумінь, але потребує правил інформаційної безпеки та контролю конфіденційності
Координаційна взаємодія	Розподіл завдань, контроль строків, синхронізація дій між учасниками	Jira, Trello, Asana, ClickUp, Monday.com	Підвищує керованість проєктів, знижує ризики затримок і перевитрат бюджету
Техніко-розробницька взаємодія	Спільна робота над кодом, тестування, рев'ю, управління версіями	GitHub, GitLab, Bitbucket, CI/CD-платформи	Впливає на захист інтелектуальної власності, якість продукту та безперервність розробки
Аналітична взаємодія	Аналіз вимог, даних, поведінки користувачів, бізнес-процесів	BI-системи, CRM, аналітичні платформи, системи звітності	Підвищує якість управлінських рішень і знижує ризики помилкових стратегічних дій
Документаційна взаємодія	Створення, збереження та оновлення технічної, управлінської та проєктної документації	Confluence, Notion, Google Workspace, SharePoint	Зменшує ризики втрати знань і залежності від окремих працівників
Безпекова взаємодія	Узгодження доступів, реагування на інциденти, дотримання політик безпеки	IAM-системи, SIEM, VPN, DLP, системи моніторингу	Захищає дані, код, клієнтську інформацію та критичні цифрові активи
Соціально-командна взаємодія	Підтримання довіри, залученості, командної культури та психологічної безпеки	Внутрішні платформи, онлайн-зустрічі, HRM-системи	Знижує кадрові ризики, вигорання, конфлікти та плинність персоналу

Як видно з таблиці 1, цифрова командна взаємодія не є однорідним процесом. Вона охоплює різні напрями діяльності, кожен із яких по-своєму впливає на економічну безпеку ІТ-підприємства. Комунікаційна взаємодія забезпечує швидкість обміну інформацією, але водночас може стати джерелом витоку конфіденційних даних. Координаційна взаємодія підвищує керованість проєктів, але за відсутності прозорих правил може призводити до перевантаження працівників або дублювання завдань. Техніко-розробницька взаємодія прямо пов'язана із захистом інтелектуальної власності, оскільки саме в репозиторіях коду та середовищах розробки зосереджуються ключові активи ІТ-підприємства. Документаційна взаємодія має особливе значення для збереження знань і забезпечення безперервності роботи.

Не менш важливою є систематизація типів команд, які функціонують в ІТ-підприємствах. Кожен тип команди має власну логіку організації, рівень автономії, характер доступу до інформації та специфічні ризики для економічної безпеки.

Таблиця 2. **Типи команд в ІТ-підприємствах та їх особливості з позиції економічної безпеки,** *сформовано автором на основі [6; 8; 9; 10]*

Тип команди	Основне призначення	Особливості цифрової взаємодії	Потенційні ризики для економічної безпеки
Проєктна команда	Виконання конкретного ІТ-проєкту в межах строків, бюджету та вимог клієнта	Активне використання таск-трекерів, комунікаційних платформ і систем звітності	Перевищення бюджету, затримки, неузгодженість вимог, конфлікти з клієнтом
Продуктова команда	Розвиток цифрового продукту протягом тривалого життєвого циклу	Постійна робота з аналітикою, backlog, користувацьким досвідом і технічними змінами	Втрата продуктових знань, помилки стратегічного розвитку, зниження якості продукту
Agile-команда	Ітеративна розробка з високою адаптивністю до змін	Регулярні спринти, daily meetings, ретроспективи, цифрові дошки завдань	Формалізація agile без реальної відповідальності, хаотичність змін, перевантаження команди
DevOps-команда	Забезпечення зв'язку між розробкою, тестуванням і експлуатацією	Використання CI/CD, автоматизації, моніторингу та хмарної інфраструктури	Збої релізів, порушення безперервності сервісів, технічні інциденти
Команда кібербезпеки	Захист цифрових активів, виявлення загроз, реагування на інциденти	Моніторинг подій безпеки, контроль доступів, аналіз інцидентів	Несвоєчасне реагування на атаки, витоки даних, репутаційні збитки
Віддалена команда	Виконання завдань працівниками з різних локацій	Повна залежність від цифрових каналів комунікації та хмарних сервісів	Втрата контролю, слабка згуртованість, ризики кібергігієни, складність координації

Закінчення табл. 2.

Тип команди	Основне призначення	Особливості цифрової взаємодії	Потенційні ризики для економічної безпеки
Міжнародна розподілена команда	Співпраця фахівців із різних країн і часових поясів	Асинхронна комунікація, різні культурні та правові контексти	Комунікаційні бар'єри, правові ризики, складність захисту даних
Аутсорсингова команда	Надання послуг зовнішньому клієнту	Постійна взаємодія з клієнтськими системами, вимогами та документацією	Ризики конфіденційності, залежність від клієнта, репутаційна відповідальність
R&D-команда	Створення нових технологічних рішень, прототипів і дослідницьких продуктів	Інтенсивний обмін знаннями, експериментальні середовища, робота з новими технологіями	Втрата інтелектуальної власності, невизначеність результатів, високі інноваційні ризики

Представлена систематизація свідчить, що не існує універсальної моделі командної роботи, яка однаково підходила б для всіх IT-підприємств. Проєктна команда потребує жорсткішого контролю строків, бюджету та вимог клієнта. Продуктова команда потребує збереження довгострокових знань про продукт і користувачів. DevOps-команда має особливе значення для технологічної безпеки та безперервності цифрових сервісів. Команда кібербезпеки прямо впливає на інформаційну та репутаційну безпеку. Віддалені й міжнародні команди створюють нові можливості для масштабування бізнесу, але потребують посилених правил доступу, цифрової дисципліни та управління культурними відмінностями.

Особливістю цифрової командної взаємодії є те, що її вплив на економічну безпеку може бути як позитивним, так і негативним. З одного боку, цифрові інструменти підвищують прозорість завдань, пришвидшують ухвалення рішень, дозволяють контролювати хід проєктів, зберігати історію комунікації та забезпечувати доступ до знань. З іншого боку, вони створюють залежність від цифрової інфраструктури, збільшують кількість точок доступу до конфіденційної інформації, ускладнюють контроль поведінки працівників і можуть сприяти інформаційному перевантаженню [5; 7; 10].

Вплив цифрової командної взаємодії на економічну безпеку IT-підприємства доцільно розглядати через основні складові економічної безпеки.

З таблиці 3 видно, що цифрова командна взаємодія є подвійним явищем з позиції економічної безпеки. Вона здатна суттєво підвищувати ефективність IT-підприємства, але лише за умови належного управління. Якщо цифрова взаємодія не регламентована, вона може призводити до втрати контролю над бізнес-процесами, розпорошення відповідальності, зниження якості комунікації та підвищення ризиків для інформаційних активів. Тому управління цифровою командною взаємодією має включати не лише

організацію робочих процесів, а й правила безпеки, політики доступу, механізми документування знань, процедури реагування на інциденти та систему підтримки персоналу.

Таблиця 3. **Вплив цифрової командної взаємодії на складові економічної безпеки ІТ-підприємства,** *сформовано автором на основі [1; 2; 5; 10; 11]*

Складова економічної безпеки	Позитивний вплив цифрової командної взаємодії	Потенційні загрози
Фінансова безпека	Підвищення продуктивності, контроль строків, скорочення витрат на офісну інфраструктуру, швидше виконання проєктів	Перевитрати через слабку координацію, затримки релізів, неефективне планування ресурсів
Кадрова безпека	Можливість залучення фахівців незалежно від локації, гнучкість роботи, підвищення автономії	Плинність кадрів, вигорання, слабка залученість, втрата командної згуртованості
Інформаційна безпека	Централізація доступів, фіксація дій, можливість моніторингу цифрових процесів	Витоки даних, слабкі паролі, неконтрольований доступ, використання незахищених пристроїв
Інтелектуальна безпека	Спільне створення знань, документування рішень, збереження технічної історії проєкту	Втрата коду, порушення прав інтелектуальної власності, залежність від окремих фахівців
Організаційна безпека	Прозорий розподіл ролей, керованість завдань, швидка адаптація до змін	Хаотична комунікація, дублювання функцій, слабкий контроль відповідальності
Технологічна безпека	Автоматизація процесів, контроль версій, моніторинг систем, підтримка безперервності сервісів	Технічні збої, залежність від платформ, неправильне налаштування доступів
Репутаційна безпека	Підвищення якості сервісу, швидша реакція на клієнтські запити, прозорість виконання проєктів	Невиконання строків, витоки клієнтських даних, низька якість продукту, публічні конфлікти
Правова безпека	Фіксація домовленостей, цифрові сліди рішень, контроль виконання контрактних зобов'язань	Порушення NDA, недотримання вимог щодо персональних даних, неврегульованість дистанційної роботи

Особливого значення для економічної безпеки ІТ-підприємств набуває питання управління знаннями. У традиційних підприємствах значна частина активів може бути матеріально зафіксована, тоді як в ІТ-сфері критично важливі знання часто належать працівникам або командам. Це знання про архітектуру продукту, особливості коду, логіку інтеграцій, очікування клієнтів, історію технічних рішень і причини вибору певних підходів. Якщо ці знання не документуються або не передаються всередині команди, підприємство стає залежним від окремих фахівців. У разі їх звільнення або переходу до конкурентів виникає ризик втрати частини інтелектуального капіталу [3; 6; 8].

Для зниження таких ризиків ІТ-підприємству необхідно формувати систему управління знаннями, яка включає технічну документацію, бази знань, стандарти кодування, процедури code review, регулярні внутрішні навчання, наставництво, документування архітектурних рішень і контроль оновлення проєктної інформації. Водночас важливо забезпечити баланс між відкритістю знань усередині команди та захистом конфіденційної інформації. Надмірне обмеження доступу може уповільнювати роботу команди, тоді як надмірна відкритість створює ризики витоку даних і порушення прав інтелектуальної власності [10; 11].

Іншою важливою проблемою є кадрова безпека. ІТ-підприємства значною мірою залежать від кваліфікованих фахівців, а конкуренція за таланти залишається високою. Цифрова командна взаємодія відкриває можливість залучати працівників із різних регіонів і країн, але водночас підвищує ризики слабкої залученості, професійного вигорання, ізоляції, втрати відчуття належності до команди та швидкої зміни місця роботи. У таких умовах економічна безпека залежить не лише від контрактних умов, а й від якості командної культури, психологічної безпеки, прозорості комунікації, справедливого розподілу навантаження та можливостей професійного розвитку [4; 7].

Психологічна безпека команди має прямий зв'язок з економічною безпекою підприємства. Якщо працівники не бояться повідомляти про помилки, ризики, технічні проблеми або порушення процедур, підприємство має більше шансів своєчасно виявити загрози. Якщо ж у команді домінує страх, замовчування проблем або надмірний тиск, помилки можуть накопичуватися й перетворюватися на серйозні фінансові, технологічні або репутаційні втрати. Для ІТ-підприємств це особливо важливо, оскільки невчасно виявлена технічна помилка або вразливість у коді може мати масштабні наслідки для клієнтів і самого підприємства [3; 4; 10].

Інформаційна безпека в умовах цифрової командної взаємодії потребує особливої уваги. Учасники команд можуть працювати з різних пристроїв, підключатися до корпоративних систем із різних мереж, використовувати хмарні сервіси, обмінюватися файлами, брати участь у спільній розробці та мати доступ до клієнтських даних. Це означає, що кожен учасник команди стає потенційною точкою ризику. Тому економічна безпека ІТ-підприємства залежить від контролю доступів, багатофакторної автентифікації, сегментації прав, моніторингу активності, політик використання пристроїв, навчання працівників кібергігієні та регулярного перегляду прав доступу [10; 11].

Важливо також враховувати правову складову економічної безпеки. ІТ-підприємства часто працюють із міжнародними клієнтами, укладають договори про нерозголошення, обробляють персональні дані, передають права на програмні продукти або створюють рішення на замовлення. У цифровій командній взаємодії правові ризики можуть виникати через несанкціоноване поширення інформації, використання сторонніх інструментів без погодження, порушення умов ліцензування програмного забезпечення, невизначеність прав на результати роботи фрілансерів або зовнішніх підрядників. Тому правові аспекти командної роботи мають бути

відображені у внутрішніх політиках, трудових договорах, NDA, угодах із підрядниками та правилах використання цифрових інструментів [2; 10].

Для забезпечення економічної безпеки ІТ-підприємств цифрова командна взаємодія має управлятися системно. Доцільно виділити кілька управлінських рівнів такого забезпечення.

Таблиця 4. **Управлінські рівні забезпечення економічної безпеки ІТ-підприємств через цифрову командну взаємодію,** *сформовано автором на основі [1; 5; 10; 11]*

Управлінський рівень	Зміст управлінських дій	Очікуваний результат для економічної безпеки
Стратегічний рівень	Визначення ролі командної взаємодії в бізнес-моделі, політиці безпеки та стратегії розвитку	Узгодження командної роботи з цілями підприємства та системою економічної безпеки
Організаційний рівень	Формування структури команд, ролей, відповідальності, правил комунікації та координації	Зниження хаотичності, дублювання функцій і ризиків неузгодженості
Технологічний рівень	Вибір цифрових платформ, контроль доступів, автоматизація процесів, моніторинг активності	Захист цифрових активів, підвищення прозорості та безперервності роботи
Кадровий рівень	Навчання працівників, розвиток цифрової культури, підтримка залученості, профілактика вигорання	Зниження кадрових ризиків, підвищення відповідальності та лояльності
Інформаційний рівень	Управління знаннями, документацією, конфіденційною інформацією та клієнтськими даними	Збереження інтелектуального капіталу та зниження ризиків витоку інформації
Контрольний рівень	Аудит доступів, оцінювання ефективності команд, аналіз інцидентів, перегляд політик	Своєчасне виявлення загроз і коригування управлінських рішень

Запропонована систематизація свідчить, що управління цифровою командною взаємодією не може бути завданням лише HR-відділу, проєктного менеджера або фахівців із кібербезпеки. Воно потребує міжфункціонального підходу, у якому беруть участь керівництво підприємства, менеджери проєктів, технічні лідери, HR-фахівці, юристи, фахівці з інформаційної безпеки та фінансові менеджери. Лише така інтеграція дозволяє забезпечити узгодження продуктивності команди, захисту інформації, контролю витрат, збереження знань і дотримання договірних зобов'язань.

У практичному вимірі забезпечення економічної безпеки ІТ-підприємства через цифрову командну взаємодію має включати такі елементи: розроблення політики цифрової командної роботи; визначення правил використання корпоративних платформ; запровадження матриці доступів; регулярний перегляд прав доступу; документування технічних і управлінських рішень; захист репозиторіїв коду; проведення code review; навчання працівників кібергігієні; формування культури відповідального обміну інформацією; оцінювання командної продуктивності; профілактику

професійного вигорання; контроль виконання NDA та інших договірних зобов'язань.

Окремо слід наголосити, що цифрова командна взаємодія має бути не лише контрольованою, а й гнучкою. Надмірна бюрократизація командної роботи може знижувати швидкість розробки, демотивувати працівників і ускладнювати інноваційну діяльність. Водночас надмірна свобода без правил безпеки може створити загрози для даних, коду, клієнтських зобов'язань і репутації підприємства. Тому завдання управління полягає у пошуку балансу між автономією команд і контролем безпеки. Для IT-підприємств такий баланс є одним із ключових критеріїв зрілості управлінської системи.

Узагальнюючи викладене, можна запропонувати текстову логіку забезпечення економічної безпеки IT-підприємств в умовах цифрової командної взаємодії (Рис. 1).

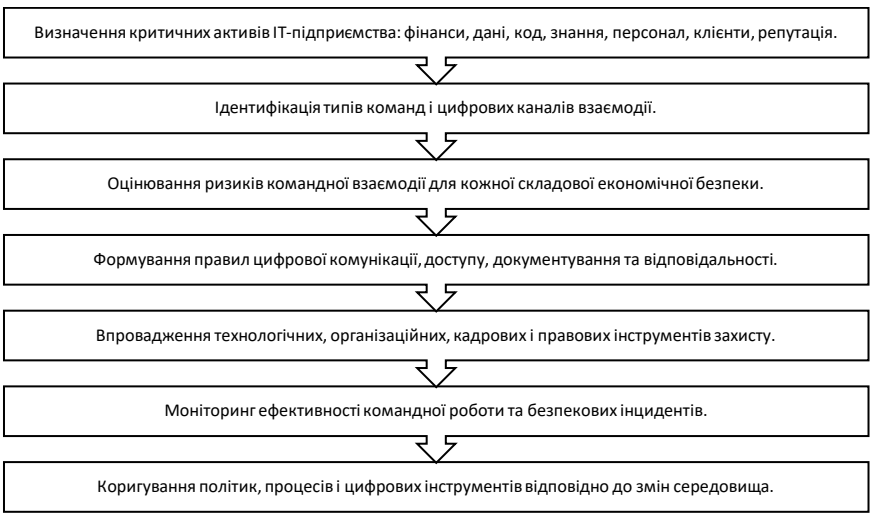

Рис. 1. **Логіка забезпечення економічної безпеки IT-підприємства через управління цифровою командною взаємодією,** *сформовано автором*

Таким чином, цифрова командна взаємодія має розглядатися як важлива управлінська площина економічної безпеки IT-підприємств. Вона впливає на фінансові результати, якість продукту, захист інформації, збереження інтелектуальної власності, кадрову стабільність, технологічну надійність і репутацію підприємства. Ефективне управління такою взаємодією дозволяє не лише зменшити ризики, а й створити додаткові переваги для розвитку IT-підприємства в умовах цифрової економіки.

Висновки. У статті обґрунтовано, що економічна безпека IT-підприємств в умовах цифрової командної взаємодії має розглядатися як комплексна система захисту фінансових, кадрових, інформаційних, інтелектуальних, технологічних, організаційних і репутаційних ресурсів. На відміну від

традиційних підходів, які зосереджуються переважно на фінансових або інформаційних аспектах безпеки, запропонований підхід акцентує увагу на командній взаємодії як важливому управлінському чиннику економічної безпеки.

Визначено, що цифрова командна взаємодія в IT-підприємствах охоплює комунікаційні, координаційні, техніко-розробницькі, аналітичні, документаційні, безпекові та соціально-командні процеси. Кожен із цих типів взаємодії має власне значення для економічної безпеки. Комунікаційна взаємодія впливає на швидкість і точність обміну інформацією, координаційна взаємодія визначає керованість проєктів, техніко-розробницька взаємодія пов'язана із захистом коду й інтелектуальної власності, документаційна взаємодія забезпечує збереження знань, а безпекова взаємодія спрямована на захист критичних цифрових активів.

Систематизовано типи команд, характерні для IT-підприємств, зокрема проєктні, продуктові, agile-команди, DevOps-команди, команди кібербезпеки, віддалені, міжнародні, аутсорсингові та R&D-команди. Доведено, що кожен тип команди має специфічний вплив на економічну безпеку, оскільки відрізняється характером доступу до інформації, рівнем автономії, обсягом відповідальності, тривалістю роботи та залежністю від цифрових інструментів.

Встановлено, що цифрова командна взаємодія може одночасно посилювати й послаблювати економічну безпеку IT-підприємства. Її позитивний вплив проявляється у підвищенні продуктивності, гнучкості, прозорості процесів, швидкості ухвалення рішень, можливості залучення фахівців незалежно від локації та збереженні цифрових слідів управлінських рішень. Водночас потенційні загрози пов'язані з витоками даних, втратою інтелектуальної власності, слабкою координацією, інформаційним перевантаженням, кадровою нестабільністю, професійним вигоранням, залежністю від цифрових платформ і порушенням конфіденційності.

Практичне значення дослідження полягає в обґрунтуванні необхідності інтегрувати управління цифровою командною взаємодією в систему економічної безпеки IT-підприємства. Для цього доцільно поєднувати стратегічні, організаційні, технологічні, кадрові, інформаційні, правові та контрольні інструменти. Перспективи подальших досліджень доцільно пов'язати з розробленням методики оцінювання впливу цифрової командної взаємодії на рівень економічної безпеки IT-підприємств, формуванням індикаторів безпечної командної роботи та побудовою інтегрального індексу командної безпеки в IT-сфері.

1. Edmondson, A. C. (2019). The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth. Wiley. https://www.researchgate.net/publication/359340045_Amy_C_Edmondson_The_fearless_organization_Creating_psychological_safety_in_the_workplace_for_learning_innovation_and_growth_New_Jersey_John_Wiley_Sons_Inc_2019_256_pages_1749_hardcover

2. Eurofound. (2020). Telework and ICT-based mobile work: Flexible working in the digital age. Publications Office of the European Union. https://www.eurofound.europa.eu/en/publications/2020/telework-and-ict-based-mobile-work-flexible-working-digital-age

3. Illiashenko, O. (2016). Economic security of enterprise: Theoretical and methodological foundations. National Academy of Management.

4. ISO/IEC. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. International Organization for Standardization. https://www.iso.org/standard/27001

5. Katzenbach, J. R., & Smith, D. K. (1993). The wisdom of teams: Creating the high-performance organization. Harvard Business School Press.

6. McKinsey & Company. (2020). What's next for remote work: An analysis of 2,000 tasks, 800 jobs, and nine countries. https://www.mckinsey.com/featured-insights/future-of-work/whats-next-for-remote-work-an-analysis-of-2000-tasks-800-jobs-and-nine-countries

7. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework 2.0. https://www.nist.gov/cyberframework

8. OECD. (2021). The digital transformation of SMEs. OECD Publishing. https://doi.org/10.1787/bdb9256a-en

9. Project Management Institute. (2017). Agile practice guide. Project Management Institute.

10. Schwaber, K., & Sutherland, J. (2020). The Scrum guide. https://scrumguides.org/scrum-guide.html

11. Spataro, J. (2021). The future of work: The good, the challenging and the unknown. Microsoft WorkLab. https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work

---

1. Edmondson, A. C. (2019). The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth. Wiley. https://www.researchgate.net/publication/359340045_Amy_C_Edmondson_The_fearless_organization_Creating_psychological_safety_in_the_workplace_for_learning_innovation_and_growth_New_Jersey_John_Wiley_Sons_Inc_2019_256_pages_1749_hardcover

2. Eurofound. (2020). Telework and ICT-based mobile work: Flexible working in the digital age. Publications Office of the European Union. https://www.eurofound.europa.eu/en/publications/2020/telework-and-ict-based-mobile-work-flexible-working-digital-age

3. Illiashenko, O. (2016). Economic security of enterprise: Theoretical and methodological foundations. National Academy of Management.

4. ISO/IEC. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. International Organization for Standardization. https://www.iso.org/standard/27001

5. Katzenbach, J. R., & Smith, D. K. (1993). The wisdom of teams: Creating the high-performance organization. Harvard Business School Press.

6. McKinsey & Company. (2020). What's next for remote work: An analysis of 2,000 tasks, 800 jobs, and nine countries. https://www.mckinsey.com/featured-insights/future-of-work/whats-next-for-remote-work-an-analysis-of-2000-tasks-800-jobs-and-nine-countries

7. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework 2.0. https://www.nist.gov/cyberframework

8. OECD. (2021). The digital transformation of SMEs. OECD Publishing. https://doi.org/10.1787/bdb9256a-en

9. Project Management Institute. (2017). Agile practice guide. Project Management Institute.

10. Schwaber, K., & Sutherland, J. (2020). The Scrum guide. https://scrumguides.org/scrum-guide.html

11. Spataro, J. (2021). The future of work: The good, the challenging and the unknown. Microsoft WorkLab. https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work