ISSN: 3083-7782
Електронний науковий журнал «ЕКОНОМІЧНА ПАРАДИГМА»

УДК 004.738.5:004.056:005.95/.96

Нагаєв Віктор Михайлович
доктор педагогічних наук, професор, професор кафедри менеджменту, бізнесу і адміністрування
Державний біотехнологічний університет
ORCID: 0000-0002-3130-6112

Чалий Ігор Вільович
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій, кібернетики та захисту інформації
Державний біотехнологічний університет
ORCID: 0000-0003-4896-133X

Гіржева Ольга Миколаївна
доктор економічних наук, професор, професор кафедри менеджменту, бізнесу і адміністрування
Державний біотехнологічний університет
ORCID: 0000-0003-4548-3512

Назарова Світлана Олександрівна
кандидат економічних наук, доцент, професор кафедри мультимедійних систем і технологій
Харківський національний економічний університет імені Семена Кузнеця
ORCID: 0009-0007-2229-423X

Вашечко Сергій Сергійович
аспірант кафедри менеджменту, бізнесу і адміністрування
Державного біотехнологічного університету
ORCID: 0009-0007-6087-2328

DOI: 10.25313/economics-2026-3-107-12

Авторське право © Автор(и).
Це стаття з відкритим доступом, що розповсюджується відповідно до умови ліцензії Creative Commons Attribution Ліцензія 4.0 (https://creativecommons.org/licenses/by/4.0/)

ХМАРНІ ТЕХНОЛОГІЇ WEB 3.0 ТА WEB 4.0 ЦИФРОВОГО ЛІДЕРСТВА ТА КІБЕРЗАХИСТУ У ПРОФЕСІЙНОМУ СТАНОВЛЕННІ СУЧАСНОГО МЕНЕДЖЕРА

Анотація. *Вступ. Глобальна цифровізація економічних відносин та перехід до мережецентричного суспільства зумовлюють докорінну перебудову парадигми сучасного менеджменту, висуваючи нові вимоги до професійних компетенцій управлінців. Стрімкий розвиток хмарних технологій поколінь Web 3.0 та Web 4.0 виступає визначальним чинником трансформації бізнес-середовища, що пов'язано з переходом від централізованих ієрархічних структур до децентралізованих екосистем та інтелектуальних симбіотичних систем. У цьому процесі виняткового значення набувають питання адаптації науково обґрунтованих стратегій цифрового лідерства та інтеграції інструментарію децентралізованих автономних організацій (DAO), смарт-контрактів і предиктивної аналітики в управлінську практику, з обов'язковим забезпеченням належного кіберзахисту всієї інфраструктури. Становлення менеджера нового покоління розглядається як основа формування стійких адаптивних бізнес-моделей, що здатні ефективно функціонувати в умовах високої волатильності технологічного простору.*

Мета дослідження полягає у теоретико-практичному обґрунтуванні ролі хмарних технологій Web 3.0 та Web 4.0 у професійному становленні сучасного менеджера, а також у розробці концептуальних засад механізмів кіберзахисту в умовах децентралізації та інтелектуалізації цифрового менджменту.

Матеріали і методи. Матеріалами дослідження є: 1) міжнародні стандарти та регламенти з хмарної безпеки (зокрема ISO/IEC 27017, звіти CSA та NIST); 2) джерельна база наукових праць вітчизняних та зарубіжних фахівців у галузі блокчейн-технологій, штучного інтелекту, кібербезпеки та професійної підготовки управлінців. В процесі дослідження було використано наступні наукові методи: історико-логічний та системний аналіз (для характеристики етапів розвитку Web-технологій та їхнього впливу на менеджмент); моделювання (для опису когнітивного управління та предиктивних бізнес-процесів у Web 4.0); проектування (для визначення структури цифрових компетенцій менеджера); логічного узагальнення (для формування висновків та практичних рекомендацій щодо підвищення кіберстійкості організацій).

Результати. Обґрунтовано перехід від ієрархічних до децентралізованих моделей цифрового менеджменту, що ґрунтуються на використанні смарт-контрактів та алгоритмічної довіри. Визначено структуру сформованості професійних компетенцій менеджера, яка в умовах Web 4.0 доповнюється навичками цифрового лідерства та здатності до симбіотичної взаємодії з ШІ-агентами. Доведено, що кібербезпека в умовах Web 3.0/4.0 має бути представлена не лише технічними засобами захисту, а й стратегічним рівнем «Cyber-Security Awareness» керівної ланки. Це включає впровадження криптографічних стандартів, постквантових алгоритмів захисту та механізмів предиктивного моніторингу загроз у хмарному середовищі з метою забезпечення безперервності бізнес-процесів та високої довіри стейкголдерів.

Перспективи. В контексті перспектив подальших досліджень вважаємо за доцільне розробити прикладні методики оцінювання кіберризиків у децентралізованих хмарних системах та обґрунтувати ситуаційну модель цифрового лідерства, що базується на використанні інтелектуальних когнітивних сервісів. Це дозволить оптимізувати управлінські комунікації та підвищити ефективність стратегічного планування в умовах глобального цифрового менеджменту.

Ключові слова: *хмарні технології, Web 3.0, Web 4.0, кібербезпека, циффровий менеджмент, цифрове лідерство, цифрова компетентність, менеджмент персоналу, діджиталізація, інформаційні технології, кадровий розвиток, децентралізовані автономні організації (DAO), управлінські комунікації, блокчейн, професійне становлення менеджера.*

Постановка проблеми. Питання трансформації управлінських парадигм у контексті впровадження хмарних технологій поколінь Web 3.0 та Web 4.0, а також забезпечення кіберстійкості та цифрового лідерства в системі корпоративного та публічного управління, є сьогодні однією з найактуальніших проблем розвитку глобальної економічної системи. Ця проблематика інтерпретується особливістю сучасного розвитку соціально-економічної інфраструктури в умовах четвертої та п'ятої промислових революцій, де децентралізовані мережі, семантична павутина та штучний інтелект складають основу функціонування суспільства. У такому середовищі комунікаційні та управлінські процеси зазнають радикальних цифрових трансформацій за принципом переходу від централізованих платформ до автономних інтелектуальних екосистем [1; 2].

Питання кібербезпеки як стабілізуючого чинника професійного становлення менеджера інтегрує в собі необхідність захисту децентралізованих активів, управління цифровою ідентичністю та забезпечення цілісності даних у симбіотичних мережах Web 4.0. Саме здатність менеджера виступати гарантом цифрової довіри відіграє критичну роль у прийнятті стратегічних рішень, які мають фундаментальне значення для життєздатності будь-якої організації в умовах гібридних загроз [3].

Аналіз останніх досліджень і публікацій. В умовах глобалізації та інтенсивної розбудови децентралізованого інформаційного суспільства традиційні методи управління корпоративними активами та людським капіталом стають недостатньо ефективними. Для створення нових, архітектурно гнучких методів управління бізнес-процесами та доступу до даних все частіше застосовуються хмарні технології поколінь Web 3.0 та Web 4.0, які являють собою сукупність децентралізованих протоколів, семантичних алгоритмів та інтелектуальних агентів, що забезпечують обробку та зберігання інформації в умовах повної суверенності цифрового контенту [1]. Так Г. Гілдер стверджує, що ера централізованих хмар (Google, Amazon) закінчується через проблеми з безпекою та приватністю. Він прогнозує перехід до Web 3.0, де архітектура безпеки базується на блокчейні, а не на паролях чи центральних серверах. За сучасною науковою концепцією, Web 3.0 (Semantic Web) являє собою форму організації цифрового простору, яка сприяє підвищенню прозорості та безпеки діяльності через використання блокчейн-технологій для формування нового типу управлінської взаємодії, орієнтованої на усунення посередників та автоматизацію довіри [2, с. 88].

Можливість обробки даних інтелектуальними хмарними сервісами Web 4.0 забезпечить впровадження технологій «Cognitive Management», що відіграє вирішальну роль у підвищенні ефективності управлінських комунікацій та сприятиме переходу до предиктивного моделювання бізнес-процесів [3]. У межах сучасних стратегій цифрової трансформації, які розглядаються як пріоритетні для професійного становлення менеджера, слід відзначити концепцію «Edge Computing», сутність якої полягає у розподіленій обробці даних безпосередньо в місцях їх виникнення. Інструменти, що використовуються для реалізації цього підходу, включають децентралізовані хмарні мережі (IPFS), смарт-контракти, мобільні блокчейн-термінали та програмне забезпечення у вигляді децентралізованих додатків (dApps) [4].

Питанням еволюції інформаційного суспільства та прогнозуванням технологічних хвиль присвячено фундаментальні праці провідних мислителів та футурологів, таких як: Е. Тоффлер, Д. Белл, М. Кастельс, Ф. Фукуяма, а також представників сучасної цифрової філософії: Ю.Н. Харарі, Н. Бострома, К. Шваба та ін.

Дослідженням цільової функції, змісту та сутності децентралізованих систем, блокчейн-інфраструктур та кібербезпеки в системі менеджменту займалися такі науковці, як: Андрущенко В., Бурячок В., Бутерін В., Гнатенко О., Данилик М., Жиляєв І., Корченко О., Лазарєв М., Плескач В., Савченко О., Скрипник В., Толубко В., Шеломенцев В., Юрченко О. та ін. [1–10; 15; 18].

Фундаментальні засади семантичної павутини, закладені Т. Бернерсом-Лі [5], стали концептуальною основою для розвитку сучасних хмарних технологій Web 3.0, де дані отримують чітко визначене значення, зрозуміле для автоматизованих систем. Поряд із впровадженням хмарних інновацій, питання кіберзахисту та цифрового лідерства в системі професійного становлення менеджера сьогодні є ключовими для забезпечення стійкості організацій. В умовах експансії кіберзагроз та використання штучного інтелекту для атак на інформаційні периметри, роль та функції управлінського лідерства зазнали принципових змін у бік «Cyber-Security Awareness». Це потребує перегляду технологій підготовки персоналу [11], форм моніторингу безпеки [7; 10] та методів захисту інтелектуальної власності [8]. Найбільш важливі аспекти, пов'язані з тематикою управлінської компетентності у сфері IT-безпеки та лідерології в цифрову епоху,

висвітлені в роботах дослідників: П. Друкер, С. Сінек, Д. Тапскотт, В. Гейтс, а також вітчизняних фахівців: Бакаєва О., Бєляков О., Гевко О., Дубас О., Козак Ю., Нижник Н., Ситник Я., Соснін О. та ін.

Водночас вважаємо, що віддаючи належне сучасним науковим досягненням, слід приділити особливу увагу системним концепціям формування синергії між хмарними компетенціями Web 3.0/4.0 та навичками предиктивного кіберзахисту як єдиного генезису професійного становлення сучасного менеджера, що потребує подальших поглиблених напрацювань у контексті концептуальних засад стратегічного управління.

Мета дослідження полягає у теоретико-практичному обґрунтуванні ролі хмарних технологій Web 3.0 та Web 4.0 у професійному становленні сучасного менеджера, а також у розробці концептуальних засад механізмів кіберзахисту в умовах децентралізації та інтелектуалізації управлінських процесів.

Виклад основного матеріалу дослідження. Трансформація сучасних управлінських моделей від ієрархій Web 2.0 до децентралізованих екосистем Web 3.0 передбачає еволюцію хмарних технологій, що докорінно змінює архітектуру управлінських комунікацій. Якщо ера Web 2.0 базувалася на централізованих хмарних платформах, де менеджер виконував роль ієрархічного контролера інформаційних потоків, то перехід до Web 3.0 вимагає відмови від моделі «центр–периферія». Концепція семантичної павутини, закладена Т. Бернерсом-Лі [5], стала каталізатором переходу до середовища, де дані отримують чітко визначене значення, зрозуміле для автоматизованих систем. Для сучасного управлінця це означає кінець епохи «інформаційного хаосу»: дані стають структурованими, що дозволяє делегувати рутинний аналіз інтелектуальним агентам. Проте справжня революція в менеджменті відбувається завдяки впровадженню технології блокчейн. Як зазначає Д. Тапскотт [15], ми переходимо від «інтернету інформації» до «інтернету цінності». У цій парадигмі блокчейн виступає як глобальний «протокол довіри», що дозволяє будувати управлінські зв'язки без участі посередників. Це підриває традиційну бюрократичну ієрархію, замінюючи її горизонтальними мережами.

Ключовим інструментом менеджера нової генерації стають децентралізовані автономні організації (DAO), які керуються кодом, а не радою директорів. Для менеджера це означає перехід від авторитарного стилю до управління на основі консенсусу. Згідно з візією В. Бутеріна [14], DAO дозволяють реалізувати управління через алгоритми, де правила взаємодії зафіксовані в програмному коді. Використання смарт-контрактів, технічну логіку яких детально описав Г. Вуд [4], дозволяє автоматизувати виконання контрактних зобов'язань та фінансових операцій без ризику людської помилки чи корупційного втручання.

Таким чином, у середовищі Web 3.0 професійне становлення менеджера зміщується з площини «адміністрування персоналу» у площину «архітектури протоколів». Менеджер перестає бути контролером і стає модератором децентралізованої екосистеми, де довіра забезпечується криптографічними методами, а ефективність — прозорістю блокчейн-реєстрів (табл. 1). Це створює надійне підґрунтя для переходу до наступного етапу — когнітивного управління у хмарах Web 4.0. Для глибшого розуміння трансформації управлінської діяльності проаналізуємо зміну інструментарію, який використовує сучасний менеджер. Перехід до Web 3.0 супроводжується заміною централізованих сервісів на децентралізовані протоколи. Комунікаційні середовища (Slack проти Discord/Matrix). Якщо Slack є класичним корпоративним месенджером з централізованим керуванням та закритим кодом, то Discord став стандартом для DAO завдяки гнучкій системі ролей та інтеграції з ботами. Matrix, у свою чергу, пропонує повну децентралізацію та наскрізне шифрування, де право володіння даними належить користувачеві, а не корпорації.

Традиційний менеджер при аналізі даних покладається на локальні звіти в Excel або хмарні таблиці, які заповнюються вручну та схильні до людських помилок. Тоді як On-chain Analytics (наприклад, Dune

Таблиця 1

Порівняльна характеристика управлінських інструментів Web 2.0 та Web 3.0

Параметр порівняння	Менеджмент Web 2.0 (централізований)	Менеджмент Web 3.0 (децентралізований)
Комунікації	Slack / Microsoft Teams (корпоративний контроль, закриті дані)	Discord / Matrix (гнучкі ролі, токен-гейтинг, суверенність даних)
Аналітика та звітність	Excel / BI-системи (локальні бази, ризик маніпуляцій, ручне введення)	On-chain Analytics (транспарентність блокчейну, автоматизація, «single source of truth»)
Управління кадрами	HR-відділ (бюрократія, суб'єктивізм, трудові книжки)	Алгоритмічний рекрутинг / DAO (смарт-контракти, репутація в блокчейні, оплата за результат)
Прийняття рішень	Накази керівництва (вертикальна ієрархія)	On-chain Voting (голосування токенами, демократичний консенсус)
Зберігання активів	Корпоративні банківські рахунки (залежність від банків-посередників)	Multi-sig гаманці (криптографічний контроль, відсутність посередників)

Джерело: систематизовано авторами на основі [12]

Analytics, Nansen) дозволяє менеджеру Web 3.0 отримувати дані безпосередньо з блокчейну в реальному часі. Це забезпечує 100% достовірність та прозорість бізнес-показників без можливості їх маніпуляції.

Симбіотичний менеджмент Web 4.0: когнітивні хмари та предиктивне моделювання. На сучасному етапі цифровізації менеджменту ми стаємо свідками народження нової парадигми управлінської діяльності. Якщо Web 3.0 забезпечив менеджменту прозорість та децентралізацію, то наступна ітерація — Web 4.0 (Symbiotic Web) — переводить управлінські процеси у площину когнітивної взаємодії між людиною та машиною. Згідно з концепцією Ф. Алмейди [13], Web 4.0 характеризується як «симбіотична павутина», де інтелектуальні агенти стають не просто інструментами, а повноцінними партнерами управлінця в прийнятті рішень.

Фундаментом Web 4.0 є технологія «когнітивних хмар» — систем, що не просто зберігають дані, а здатні до самостійного навчання та логічного виводу. Ключовим елементом цієї трансформації є впровадження технологій «Cognitive Management». Як обґрунтовують А. Коціу та співавтори [3], когнітивні системи здатні обробляти величезні масиви неструктурованих даних (Big Data), які є недоступними для стандартного людського аналізу, у реальному часі, імітуючи процеси людського мислення, але з набагато вищою продуктивністю.

Предиктивне моделювання бізнес-процесів у середовищі Web 4.0 базується на здатності алгоритмів штучного інтелекту прогнозувати ризики та можливості ще до їх фактичного прояву. Менеджер у такому середовищі перестає бути «аналітиком минулого» і стає «проектувальником майбутнього». Використання інтелектуальних агентів, як підкреслює Д. Беланше [6], дозволяє суттєво підвищити персоналізацію управлінських послуг та точність стратегічного планування завдяки здатності ШІ передбачати поведінкові реакції споживачів та ринкові флуктуації.

Когнітивний HR-менеджмент та управління людськими ресурсами. Використання нейромереж для моніторингу емоційного стану та когнітивного навантаження команди через інтерфейси взаємодії з робочим середовищем. Система сигналізує менеджеру про ризик вигорання ключового розробника на основі зміни стилю його кодування та швидкості реакцій у хмарних сервісах. Професійне становлення менеджера за І. Сурай [11] у цьому контексті передбачає розвиток емпатичного лідерства, підсиленого предиктивною аналітикою.

Симбіотичне прийняття рішень. Менеджер працює в режимі «доповненого інтелекту». Хмара виступає як зовнішня когнітивна структура, що забезпечує миттєвий доступ до світового досвіду в конкретній ніші. При розробці стратегії виходу на новий ринок, менеджер використовує когнітивний запит до хмари, яка за секунди синтезує досвід усіх аналогічних кейсів за останні 10 років, відсікаючи помилкові стратегії. Для професійного становлення менеджера це означає необхідність опанування нових методів взаємодії з «когнітивними хмарами». Управлінець у Web 4.0 має володіти навичками: інтерпретації прогнозних моделей, генерованих ШІ; коригування алгоритмічних рішень на основі етичних та соціальних контекстів; управління симбіотичними командами, що складаються з людей та автономних програмних агентів.

Кіберзахист та формування обізнаності у сфері кібербезпеки (Cyber-Security Awareness) як базової компетенції менеджера. У світі Web 3.0 та Web 4.0 атаки стають «інтелектуальними» та блискавичними. Тепер під загрозою не лише сервери, а й сама логіка прийняття рішень (смарт-контракти) та довіра до цифрової особистості. В умовах децентралізації Web 3.0 та інтелектуалізації Web 4.0 традиційні периметри захисту розмиваються. Хмарна інфраструктура стає динамічною, що вимагає від менеджера не лише знання технічних інструментів, а й глибокого розуміння природи цифрових загроз. Як підкреслюється у звіті Cloud Security Alliance [12], більшість інцидентів у хмарах пов'язані не з недоліками технологій, а з помилками в конфігурації та управлінні доступом, що робить людський фактор критичною вразливістю.

Системний підхід до побудови кіберзахисту, обґрунтований в роботах О. Корченка [8], передбачає розгляд безпеки як цілісної методологічної екосистеми. Для управлінця це означає необхідність інтеграції заходів контролю, визначених стандартом ISO/IEC 27017 [7], у щоденні бізнес-процеси. Проте, згідно з технічними засадами захисту в автоматизованих системах, розробленими В. Толубком [9], технічні засоби є ефективними лише за умови високої професійної підготовки персоналу.

Особливого значення у професійному становленні менеджера набуває концепція «Cyber-Security Awareness». Це не просто обізнаність, а активна компетенція, що включає [17]: спроможність до оцінки ризиків та розуміння динаміки сучасних загроз у децентралізованих мережах; стратегічне планування захисту, а саме врахування майбутніх викликів, таких як загроза квантових обчислень, що вимагає поступового впровадження постквантової криптографії згідно з рекомендаціями NIST; етичне управління даними, а саме забезпечення конфіденційності та цілісності інформації в умовах симбіозу з ШІ-агентами.

Симбіоз менеджера з когнітивними хмарами Web 4.0 створює не лише можливості, а й безпрецедентні ризики. Якщо раніше об'єктом атаки були бази даних, то сьогодні метою стає маніпуляція алгоритмами та компрометація децентралізованої логіки. Як зазначає Cloud Security Alliance [12], у хмарних середовищах нового покоління з'являються загрози, які менеджер минулого десятиліття навіть не міг прогнозувати. Розглянемо найбільш показові кейси сучасних атак на бізнес-системи.

Отруєння даних (Data Poisoning) та софістиковані атаки на ШІ. Зловмисники вносять викривлені дані в навчальну вибірку когнітивної хмари, щоб змусити систему приймати хибні рішення. Це може бути наприклад, маніпуляція алгоритмами предиктивної аналітики в логістиці, що змушує компанію закуповувати надлишковий товар або штучно створює дефіцит на певних напрямках. Саме тому згідно з рекомендаціями NIST [17], менеджер має забезпечувати «чистоту» вхідних даних та використовувати методи адверсаріального навчання (Adversarial ML) для захисту інтелектуальних агентів.

Атаки на ланцюги постачань (Supply Chain Attacks) у хмарному середовищі. Зловмисники атакують не саму компанію, а одного з її постачальників хмарних послуг або розробників програмних компонентів. Оскільки сучасний менеджер використовує сотні сторонніх модулів (API, плагіни), компрометація одного з них автоматично дає доступ до всієї системи. Як приклад масштабна атака на SolarWinds або вразливість Log4j, що дозволили хакерам роками залишатися непоміченими всередині урядових та корпоративних мереж. У контексті Web 4.0 це може бути компрометація навчальних моделей ШІ через «отруєння» оновлень бібліотек. Згідно з принципами ISO/IEC 27017 [7], менеджер повинен забезпечувати аудит безпеки не лише своєї компанії, а й усіх партнерів у «цифровій екосистемі». Використання блокчейну для перевірки цілісності програмного коду (Software Bill of Materials — SBOM) стає обов'язковим стандартом.

Хмарний Ransomware 2.0 та «Подвійне вимагання». У Web 2.0 віруси-шифрувальники просто блокували дані. У Web 3.0/4.0 хакери застосовують стратегію «подвійного вимагання»: вони не лише шифрують дані, а й погрожують їх публікацією або маніпуляцією смарт-контрактами компанії, що призводить до повної втрати репутації. Це можуть бути атаки на великі хмарні сховища, де зловмисники вимагають викуп у криптовалюті, погрожуючи змінити логіку автоматизованих виплат у DAO. Це паралізує роботу менеджера, оскільки він втрачає контроль над фінансовими потоками в реальному часі. Відповідно до методології О. Корченка [8], захист має базуватися на принципі «неможливості видалення».

Аналіз цих прикладів доводить, що професійне становлення сучасного управлінця не може обмежуватися лише «м'якими навичками» (soft skills). На основі праць В. Толубка [9] та В. Бурячка [10], ми можемо виділити п'ять ключових аспектів цифрової управлінської компетентності: 1) криптографічна гігієна. Розуміння того, як працюють цифрові підписи та шифрування, є таким самим базовим вмінням, як колись — знання діловодства. Менеджер має розуміти структуру своїх хмарних активів, щоб швидко ідентифікувати «точки відмови» в ланцюгу постачань; 3) стійкість до когнітивного тиску. Здатність приймати рішення в умовах діпфейк-атак та шантажу, спираючись на верифіковані блокчейн-дані, а не на емоційні стимули; 4) технологічний перехід до превентивної HR кадрової політики (використання когнітивних систем для виявлення аномалій у поведінці користувачів та контрактів до того, як станеться інцидент); 5) Zero Trust Architecture (Архітектура нульової довіри). Жоден суб'єкт (людина чи ШІ-агент) не має автоматичної довіри всередині системи. Кожна дія має бути підтверджена блокчейн-підписом.

Враховуючи ці приклади, також стає очевидним, що «цифрове лідерство» за І. Сурай [11] тепер невід'ємне від «кіберстійкості». Сучасний менеджер у процесі свого професійного становлення має трансформувати підхід до захисту: «Ефективне управління в епоху Web 4.0 — це здатність лідера балансувати між відкритістю симбіотичних систем та радикальною захищеністю когнітивних процесів [8]». «Таким чином, кібербезпека перестає бути сервісною функцією ІТ-відділу. Вона стає стрижнем лідерства, навколо якого формується здатність організації виживати та розвиватися в умовах симбіотичних мереж Web 4.0 [11]». Формування такої компетенції дозволяє керівнику перейти від пасивної ролі користувача до ролі активного архітектора безпечного цифрового простору. Кібербезпека в умовах цифрового лідерства стає фундаментом управлінської довіри, забезпечуючи надійність комунікацій та стійкість організації до деструктивних впливів у глобальних хмарних мережах.

Професійна підготовка менеджера майбутнього: від статичних знань до когнітивних симуляцій. Традиційна освітня модель, заснована на лінійному накопиченні знань, виявляється нерелевантною в умовах експоненціального розвитку технологій Web 3.0 та Web 4.0. Професійне становлення сучасного управлінця перетворюється на безперервний процес адаптації, де замість пасивного засвоєння теорії використовується глибоке занурення в інтелектуальні технологічні середовища. Наприклад, адаптивні хмарні VR/AR-тренажери — лабораторії лідерства Web 4.0.

Хмарні алгоритми генерують у VR-середовищі аватарів-опонентів, кожен з яких має унікальний психотип (від агресивного переговорника до пасивно-деструктивного підлеглого). Менеджер відпрацьовує навички вирішення конфліктів в умовах, максимально наближених до реальності. Когнітивні сервіси аналізують міміку, тембр голосу та біометричні показники менеджера під час симуляції, надаючи миттєвий аналіз його стресостійкості та переконливості. Це реалізує концепцію «ситуаційного лідерства», де управлінець вчиться змінювати стиль керівництва залежно від динамічної реакції інтелектуального середовища [11].

Мікронавчання на основі блокчейну: концепція «Живого резюме». У світі Web 3.0 сертифікат про освіту перестає бути паперовим документом і стає динамічним цифровим активом. Кожна засвоєна навичка (наприклад, «Управління DAO» або «Аудит смарт-контрактів») миттєво конвертується в NFT-сертифікат або

SBT (Soulbound Tokens, непередавані токени). Це створює незмінний запис у блокчейні, який неможливо підробити. Резюме менеджера трансформується у «живий» блокчейн-профіль (Proof-of-Skill (підтвердження навички). Роботодавець або DAO бачать не просто перелік курсів, а верифіковану історію успішних кейсів та виконаних проектів. Освітня траєкторія автоматично коригується смарт-контрактом: щойно менеджер опановує базовий рівень, система розблоковує доступ до складніших модулів, базуючись на його реальних успіхах у симуляторі (динамічне навчання).

Такий підхід до навчання має стратегічне значення для формування лідера нового покоління вирішує три ключові проблеми сучасного цифрового менеджменту: 1) подолання розриву між теорією та практикою. Менеджер отримує «досвід без ризику», відпрацьовуючи складні рішення в хмарі, перш ніж застосувати їх до реальних капіталів; 2) глобальна верифікація талантів. Блокчейн-портфоліо дозволяє менеджеру миттєво інтегруватися в міжнародні проекти Web 3.0, де довіра базується на криптографічних доказах компетенції; 3) еволюція Cyber-Security Awareness. Навчання через VR-кейси атак (наприклад, симуляція фішингу або діпфейк-дзвінка) формує навичку розпізнавання загроз на підсвідомому рівні, що значно ефективніше за традиційні інструктажі.

Навчання менеджера сучасної цифрової генерації — це безперервний тюнінг когнітивних та цифрових компетенцій у симбіозі з інтелектуальним хмарним середовищем [13, 16]. Для підготовки менеджера Web 3.0/4.0 необхідно не лише створювати нові курси, а й фундаментально оновити зміст класичних управлінських дисциплін до інтелектуальних сервісів. Ми пропонуємо розділити цей процес на два напрями: модернізація базових дисциплін та впровадження спеціалізованих інноваційних курсів.

1. Оновлення класичних управлінських дисциплін. Традиційні предмети мають бути доповнені модулями, що відображають цифрову реальність: менеджмент організацій. Додавання розділу про DAO. Замість вивчення лише ієрархічних структур, студенти мають опановувати принципи «горизонтального» управління, де роль статуту виконує програмний код, а роль наказів — результати голосування токенів; управління персоналом (HR-менеджмент). Впровадження тем щодо «Цифрової репутації» та «Proof-of-Contribution» [17–20]. Майбутній менеджер повинен розуміти принципи роботи смарт-контрактів для автоматизації виплат, управління ліквідністю у криптовалютних пулах та бюджетування через мультисіг-гаманці; стратегічне управління. Замість SWOT-аналізу, що базується на минулому досвіді, студенти вчаться працювати з когнітивними хмарами для моделювання сценаріїв майбутнього у реальному часі [21].

2. *Впровадження інноваційних фахових дисциплін*, що формують професійний профіль менеджера цифрової кометентності (табл. 2).

Освітній процес має базуватися на методі «Lab-to-DAO», де кожна академічна група функціонує як прототип реального DAO. Студенти самостійно розробляють токеноміку своєї навчальної групи, приймають рішення щодо розподілу завдань через он-чейн голосування, отримують оцінки у вигляді NFT-сертифікатів, що формують їхнє підсумкове блокчейн-портфоліо. Така трансформація освіти дозволяє менеджеру сформувати високий рівень цифрового лідерства у межах професійної компетентнсоті, що базується на практичному досвіді взаємодії з когнітивними та децентралізованими системами [22–24].

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. У сучасних умовах система професійної підготовки менеджерів повинна бути адаптована до потреб глобального цифрового середовища, в якому технології Web 3.0 та Web 4.0 стають невід'ємною складовою цифрового лідерства. Комунікаційні та технологічні інновації в менеджменті повинні мати комплексний характер, узгоджено поєднуючи в собі децентралізовані алгоритми, когнітивні сервіси та соціально-психологічні чинники в системі інтелектуального управління.

Таблиця 2

Інноваційні фахові дисципліни

Назва дисципліни	Характеристика та ключові компетенції
Архітектура цуфрового менеджменту	Вивчення принципів симбіозу з ШІ. Навчання формуванню складних запитів до когнітивних хмар (Prompt Engineering для управлінців) та інтерпретації ШІ-прогнозів.
Криптографічна етика та кібербезпека	Дисципліна на стику права, етики та технічного захисту. Формує навички захисту від діпфейк-атак, маніпуляцій даними та етичного використання персональної інформації у Web 4.0.
Токеноміка та управління блокчейн-спільнотами	Розробка економічних моделей для DAO. Студенти вчаться створювати системи стимулів (incentives) через токени та моделювати поведінку децентралізованих спільнот.
Управління цифровою ідентичністю (Identity Management)	Навчання роботі з децентралізованими ідентифікаторами (DID) та Soulbound-токенами. Формування стратегії розвитку власного «цифрового бренду» в екосистемах Web 3.0.

Джерело: узагальнено авторами на основі [13; 16]

Пріоритетними напрямами розвитку стратегій цифрового менеджменту, кібербезпеки та лідерства в умовах трансформації хмарних технологій можна вважати наступні: 1) розбудова децентралізованої інфраструктури управління на основі блокчейн-протоколів та смарт-контрактів; 2) впровадження когнітивних систем предиктивного аналізу для мінімізації управлінських ризиків; 3) формування нової етики відповідальності («on-chain reputation») в умовах прозорості Web 3.0; 4) впровадження багаторівневих механізмів кібербезпеки, включаючи постквантову криптографію та захист від когнітивних маніпуляцій (діпфейків); 5) трансформація освітнього простору через впровадження VR-симуляторів та блокчейн-верифікації компетенцій; 6) цифровізація механізмів лідерства через симбіотичну взаємодію людини та штучного інтелекту.

Модель процесу формування лідерських навичок фахівця нового покоління базується на реалізації концепції «Cognitive Management» і включає такі етапи: 1) ціннісне орієнтування здобувача на децентралізовані моделі управління та алгоритмічну довіру; 2) організація симуляційного цифрового середовища для відпрацювання навичок лідерства у VR/AR-просторі; 3) залучення фахівців до управління реальними цифровими активами та смарт-контрактами; 4) формування верифікованого цифрового портфоліо на основі блокчейн-технологій.

Ефективне цифрове лідерство відіграє ключову роль у забезпеченні кібербезпеки та зміцненні довіри стейкголдерів до інтелектуальних хмарних сервісів. Інвестування в Cyber-Security Awareness управлінської ланки є необхідною умовою виживання бізнесу в епоху Web 4.0. Це дозволить організаціям будувати стійкі симбіотичні екосистеми, сприяючи розвитку глобальної цифрової економіки.

В контексті перспективи досліджень даного напряму вважаємо за доцільне обґрунтувати критерії та механізми когнітивного лідерства за ситуаційною моделлю та визначити параметри оптимізації взаємодії людини з ШІ-агентами у практиці цифрового менеджменту. Це дасть змогу розробити прикладні рекомендації щодо захисту управлінських процесів від новітніх кіберзагроз та забезпечити високу конкурентоспроможність фахівців у майбутньому цифровому просторі.

ДОДАТКОВА ІНФОРМАЦІЯ

ВНЕСОК АВТОРІВ: Усі автори зробили внесок порівну.
ФІНАНСУВАННЯ: Автори не отримували фінансування для цього дослідження.
ЗАЯВА ПРО ДОСТУПНІСТЬ ДАНИХ: Не застосовується.
КОНФЛІКТ ІНТЕРЕСІВ: Автори заявляють про відсутність конфлікту інтересів.

Література

1. Gilder G. Life After Google: The Fall of Big Data and the Rise of the Blockchain Economy. Regnery Gateway, 2018. 256 p.

2. Tapscott D. The Digital Economy Anniversary Edition: Rethinking promise and peril in the age of networked intelligence, McGrawHill; 2014. 448 p.

3. Kotsiou A., et al. From Web 3.0 to Web 4.0: The Future of Cognitive Systems in Business Management. *Journal of Business and Technology*. 2020. Vol. 12, No. 2. P. 145–160.

4. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Yellow Paper. 2025. URL: https://ethereum.github.io/yellowpaper/paper.pdf (дата звернення: 14.01.2026).

5. Berners-Lee T., Hendler J., Lassila O. The Semantic Web. *Scientific American*. 2001. Vol. 284, № 5. P. 34–43.

6. Belanche D., Casaló L. V., Flavián C. Artificial Intelligence and Public Management: Lessons learned from the use of chatbots in public services. *Government Information Quarterly*. 2019. Vol. 36, № 3. P. 428–439.

7. ISO/IEC 27017:2015. Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. International Organization for Standardization. 2015. 30 p.

8. Корченко О. Г. Побудова систем кібербезпеки: методологічні аспекти: монографія. Київ : НАУ, 2012. 412 с.

9. Толубко В. Б., Хорошко В. О., Гайдур Г. І. Методи та засоби захисту інформації : підручник. Київ : ДУТ, 2017. 484 с.

10. Бурячок В. Л., Толубко В. Б., Хорошко В. О. Інформаційний та кіберзахист : підручник. Київ : ДУТ, 2015. 640 с.

11. Сурай І. Г. Професійна підготовка та розвиток управлінських кадрів: теорія і практика : монографія. Київ : НАДУ, 2015. 348 с.

12. Top Threats to Cloud Computing: The Pandemic Eleven. Cloud Security Alliance. 2022. 54 p. URL: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-the-pandemic-eleven/ (дата звернення: 15.01.2026).

13. Almeida F. Concept and Dimensions of Web 4.0. *International Journal of Computers & Technology*. 2017. Vol. 16, № 7. P. 7040–7046.

14. Buterin V. DAOs, DACs, DAs and More: An Incomplete Terminology Guide. *Ethereum Foundation Blog*. 2014. URL: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/ (дата звернення: 15.01.2026).

15. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. *Portfolio / Penguin.* 2016. 368 p.

16. Vuorikari R., Kluzer S., Punie Y. DigComp 2.2: The Digital Competence Framework for Citizens — With new examples of knowledge, skills and attitudes. Luxembourg: Publications Office of the European Union. 2022. 134 p. URL: https://data.europa.eu/doi/10.2760/115376 (дата звернення: 15.01.2026).

17. Chen L., Jordan S., Liu Y.-K., Moody D., Peralta R., Perlner R., Smith-Tone D. Report on Post-Quantum Cryptography. NIST Internal Report 8105. *National Institute of Standards and Technology*. 2016. 15 p. URL: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (дата звернення: 15.01.2026).

18. Жиляєв І. Б. Цифрова трансформація: виклики та можливості для України : монографія. Київ : ІТ-архітектор, 2019. 280 с.

19. Buterin V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. *White Paper.* 2014. URL: https://ethereum.org/en/whitepaper/ (дата звернення: 25.01.2026).

20. Цифрові трансформації в Україні: чи відповідають вітчизняні інституційні умови зовнішнім викликам та європейському порядку денному? *Українська національна платформа Форуму громадянського суспільства Східного партнерства.* URL: http://eap-csf.org.ua/wpcontent/uploads/2021/04/Research_DT_PF_WG2_ua-1.pdf (дата звернення: 23.01.2026).

21. Сопівник Р. В., Сопівник І. В., Варивода Н. А., Смоляк П. О. Лідерологія : навчальний посібник. Видання доповнене і перевидане. К. : «Компринт», 2019. 488 с.

22. Нагаєв В. М., Гіржева О. М., Чалий І. В., Міненко С. І. Digital трансформації публічних комунікацій, кібербезпеки та цифрового лідерства в системі електронного урядування. *Публічне адміністрування та національна безпека.* 2024. № 4 (45). С. 78–89.

23. Нагаєв В., Земляна Л., Вашечко С. Формування лідерських навичок персоналу аграрних формувань в умовах цифрової економіки. Цифрові трансформації та інноваційні технології в економіці: збірник матеріалів Міжнародної науково-практичної інтернет-конференції, Ломжа-Харків : Видавництво: MANS в Ломжі, Частина 2. 2024. С. 63–71. DOI: https://doi.org/10.58246/ITOM5383

24. Кубарева І. В., Тарлєв В. В. Цифрове лідерство як інструмент посилення ринкових позицій підприємства: корпоративний та особистісний контекст. Стратегія економічного розвитку України. 2023. № 51. С. 120–138. DOI: https://doi.org/10.33111/sedu.2022.51.120.138.

References

1. Gilder, G. (2018). *Life after Google: The fall of big data and the rise of the blockchain economy*. Regnery Gateway.

2. Tapscott, D. (2014). The digital economy anniversary edition: Rethinking promise and peril in the age of networked intelligence. McGraw-Hill.

3. Kotsiou, A., et al. (2020). From Web 3.0 to Web 4.0: The future of cognitive systems in business management. *Journal of Business and Technology, 12*(2), 145–160.

4. Wood, G. (2025). *Ethereum: A secure decentralised generalised transaction ledger* (Yellow paper). https://ethereum.github.io/yellowpaper/paper.pdf

5. Berners-Lee, T., Hendler, J., & Lassila, O. (2001). The semantic web. *Scientific American, 284*(5), 34–43.

6. Belanche, D., Casaló, L. V., & Flavián, C. (2019). Artificial intelligence and public management: Lessons learned from the use of chatbots in public services. *Government Information Quarterly, 36*(3), 428–439.

7. ISO/IEC. (2015). ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. International Organization for Standardization.

8. Korchenko, O. H. (2012). Pobudova system kiberbezpeky: Metodolohichni aspekty [Building cybersecurity systems: Methodological aspects]. NAU.

9. Tolubko, V. B., Khoroshko, V. O., & Haidur, H. I. (2017). *Metody ta zasoby zakhystu informatsii* [Methods and means of information protection]. DUT.

10. Buriachok, V. L., Tolubko, V. B., & Khoroshko, V. O. (2015). *Informatsiinyi ta kiberzakhyst* [Information and cyber protection]. DUT.

11. Surai, I. H. (2015). Profesiina pidhotovka ta rozvytok upravlinskykh kadriv: Teoriia i praktyka [Professional training and development of managerial staff: Theory and practice]. NADU.

12. Cloud Security Alliance. (2022). Top threats to cloud computing: The pandemic eleven (54 p.). https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-the-pandemic-eleven/

13. Almeida, F. (2017). Concept and dimensions of Web 4.0. *International Journal of Computers & Technology, 16*(7), 7040–7046.

14. Buterin, V. (2014a). *DAOs, DACs, DAs and more: An incomplete terminology guide*. Ethereum Foundation Blog. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

15. Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. Portfolio/Penguin.

16. Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The digital competence framework for citizens*. Publications Office of the European Union. https://data.europa.eu/doi/10.2760/115376

17. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (NIST IR 8105). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

18. Zhyliaiev, I. B. (2019). *Tsyfrova transformatsiia: Vyklyky ta mozhlyvosti dlia Ukrainy* [Digital transformation: Challenges and opportunities for Ukraine]. IT-arkhitektor.

19. Buterin, V. (2014b). *Ethereum: A next-generation smart contract and decentralized application platform* (White paper). https://ethereum.org/en/whitepaper/

20. Ukrainian National Platform of the Eastern Partnership Civil Society Forum. (2021). Digital transformations in Ukraine: Do domestic institutional conditions meet external challenges and the European agenda? Retrieved April 23, 2024, from http://eap-csf.org.ua/wpcontent/uploads/2021/04/Research_DT_PF_WG2_ua-1.pdf

21. Sopivnyk, R. V., Sopivnyk, I. V., Varyvoda, N. A., & Smoliak, P. O. (2019). *Liderolohiia* [Leaderology]. Komprint.

22. Nahaiev, V. M., Hirzheva, O. M., Chalyi, I. V., & Minenko, S. I. (2024). Digital transformations of public communications, cybersecurity and digital leadership in the e-government system. *Publichne administruvannia ta natsionalna bezpeka, 4*(45), 78–89.

23. Nahaiev, V., Zemliana, L., & Vashechko, S. (2024). Formation of leadership skills of agricultural personnel in the digital economy. In *Digital transformations and innovative technologies in economy* (Part 2, pp. 63–71). MANS. https://doi.org/10.58246/ITOM5383

24. Kubareva, I. V., & Tarliev, V. V. (2023). Tsyfrove liderstvo yak instrument posylennia rynkovykh pozytsii pidpryiemstva: Korporatyvnyi ta osobystisnyi kontekst. *Stratehiia ekonomichnoho rozvytku Ukrainy, 51*, 120–138. https://doi.org/10.33111/sedu.2022.51.120.138

Дата першого надходження статті до видання: 02.02.2026
Дата прийняття статті до друку після рецензування: 05.03.2026
Дата публікації: 10.03.2026

Nagayev Viktor
Doctor of Pedagogical Sciences, Professor,
Professor of the Department of Management,
Business and Administration
State Biotechnology University

Chaly Igor
Candidate of Technical Sciences,
Associate Professor,
Associate Professor of the Department of
Information Technologies, Cybernetics and
Information Protection
State Biotechnology University

Girzheva Olga
Doctor of Economic Sciences, Professor,
Professor of the Department of Management,
Business and Administration
State Biotechnology University

Nazarova Svitlana
Candidate of Economic Sciences,
Associate Professor,
Professor of the Department of Multimedia
Systems and Technologies
Semen Kuznets Kharkiv National University
of Economics

Vashechko Serhii
postgraduate student of the Department of
Management, Business and Administration
State Biotechnology University

CLOUD TECHNOLOGIES WEB 3.0 AND WEB 4.0 OF DIGITAL LEADERSHIP AND CYBER SECURITY IN THE PROFESSIONAL DEVELOPMENT OF A MODERN MANAGER

Summary. *Introduction. The global digitalization of economic relations and the transition to a network-centric society are leading to a radical restructuring of the paradigm of modern management, putting forward new requirements for the professional competencies of managers. The rapid development of cloud technologies of the Web 3.0 and Web 4.0 generations is a determining factor in the transformation of the business environment, which is associated with the transition from centralized hierarchical structures to decentralized ecosystems and intelligent symbiotic systems. In this process, the issues of adapting scientifically based digital leadership strategies and integrating the tools of decentralized autonomous organizations (DAO), smart contracts and predictive analytics into management practice are of exceptional importance, with the mandatory provision of proper cyber protection of the entire infrastructure. The formation of a new generation manager is considered as the basis for the formation of sustainable adaptive business models that are able to function effectively in conditions of high volatility of the technological space.*

The purpose of the study is to theoretically and practically substantiate the role of cloud technologies Web 3.0 and Web 4.0 in the professional development of a modern manager, as well as to develop conceptual foundations for cyber protection mechanisms in the context of decentralization and intellectualization of digital management.

Materials and methods. The research materials are: 1) international standards and regulations on cloud security (in particular ISO/IEC 27017, CSA and NIST reports); 2) a source database of scientific works by domestic and foreign specialists in the field of blockchain technologies, artificial intelligence, cybersecurity and professional training of managers. The following scientific methods were used in the research process: historical-logical and systems analysis (to characterize the stages of development of Web technologies and their impact on management); modeling (to describe cognitive management and predictive business processes in Web 4.0); design (to determine the structure of the manager's digital competencies); logical generalization (to form conclusions and practical recommendations for increasing the cyber resilience of organizations).

Results. The transition from hierarchical to decentralized models of digital management based on the use of smart contracts and algorithmic trust is substantiated. The structure of the formation of the manager's professional competencies is determined, which in the conditions of Web 4.0 is supplemented by digital leadership skills and the ability to symbiotically interact with AI agents. It is proven that cybersecurity in the conditions of Web 3.0/4.0 should be represented not only by technical means of protection, but also by the strategic level of "Cyber-Security Awareness" of the management level. This includes the implementation of cryptographic standards, post-quantum protection algorithms and mechanisms for predictive threat monitoring in the cloud environment in order to ensure the continuity of business processes and high trust of stakeholders.

Prospects. In the context of the prospects of further research, we consider it advisable to develop applied methods for assessing cyber risks in decentralized cloud systems and to substantiate a situational model of digital leadership based on the use of intelligent cognitive services. This will allow optimizing management communications and increasing the efficiency of strategic planning in the context of global digital management.

Key words: *cloud technologies, Web 3.0, Web 4.0, cybersecurity, digital management, digital leadership, digital competence, personnel management, digitalization, information technology, human resource development, decentralized autonomous organizations (DAO), management communications, blockchain, professional development of a manager.*