УДК 658.6:004
DOI: https://doi.org/10.26642/jen-2019-3(89)-30-34

А.О. Наторіна, к.е.н.
ДНУ «Інститут освітньої аналітики»

Синкретичність менеджменту цифрових ризиків та інформаційної безпеки

Детерміновано роль цифровізації бізнесу у контексті перманентних змін маркетингового середовища. Ідентифіковано та інтерпретовано ключові блоки цифровізації бізнесу, що дозволяють швидко та своєчасно реагувати на ринкові запити, потреби онлайн-покупців, задоволення яких, є важливою складовою успішної діяльності в онлайн-просторі. Доведено залежність конкурентоспроможності цифрового бізнесу від здатності раціонально імплементувати інноваційні технологічні підходи на практиці. Обґрунтовано значущість коректної імплементації інноваційних технологічних бізнес-підходів для стабільного розвитку цифрового бізнесу у сучасних реаліях. При формуванні вибірки прийнятних альтернативних адміністративних рішень автором запропоновано п'ять контурів адаптації та/або секвестування комплексу маркетингових програм і заходів. Надано рекомендації щодо врахування відповідних референцій при аргументації та обґрунтуванні візії цифрового бізнесу, що сприятиме проектуванню цифрової ендогенної екосистеми та забезпечить довгостроковий успішний розвиток бізнесу. Визначено, що гарантування інформаційного захисту є партисипативним пріоритетним завданням під час розвитку цифрового бізнесу. Обґрунтовано, що цифровий бізнес компліментарно розглядає застосування гетерогенних способів імплементації інноваційних технологій, що обумовлюють різноспрямованість IT-потоків. Сформульовано директиви менеджменту цифрових ризиків та інформаційної безпеки, які є уніфікованими для реалізації у нестабільних умовах цифрової трансформації. Реалізація на практиці цих директив передбачає готовність цифрового бізнесу адаптуватися до зміни маркетингового середовища та сприяє не лише інтернальній трансформації цифрового бізнесу, але й залученню нових інвестицій для здійснення ефективного менеджменту цифрових ризиків та інформаційної безпеки.

Ключові слова: *цифровий бізнес; менеджмент; цифровий ризик; інформаційна безпека*.

Актуальність теми. У реаліях сьогодення цифровізація бізнесу стимулювала появу нових способів надання послуг підприємцями в онлайн-просторі та, як наслідок, призвела до появи цифрових ризиків, і, цим самим, підвищила цінність інформаційної безпеки. Адже персонал, постачальники та стейкхолдери працюють з конфіденційною інформацією, втрата якої може призвести до негативних наслідків для бізнесу, у тому числі до значних фінансових витрат. У свою чергу, високий рівень загроз, обумовлених цифровими ризиками, вимагає фокусування уваги на розробці програми заходів щодо забезпечення інформаційної безпеки, які передбачають симультанну реалізацію традиційних та інноваційних бізнес-процесів, а також проведення додаткових бек-тестів у межах імплементації аналітичних підходів.

Аналіз останніх досліджень та публікації, на які спирається автор. З огляду на значущість та актуальність цифровізації діяльності підприємств, що функціонують в онлайн-просторі, різні аспекти ведення цифрового бізнесу у сучасних умовах висвітлено у працях зарубіжних та вітчизняних вчених, економістів, фахівців у сфері онлайн-торгівлі. Зокрема, особливості онлайн-діяльності підприємств в умовах цифрової трансформації, а також специфіку взаємодії з онлайн-покупцями вивчали: І.Бурачек [6], Р.Воллан [3], П.Говінду [5], Ф.Девіс [3], Дж.Діліон [2], Ф.Енжеліс [3], С.Каннан [5], К.Квайрін [3], О.Макфілі [2], А.Раманасан [5]. Підходи щодо ефективного ведення маркетингової онлайн-діяльності у бізнес-середовищі з використанням практичних методів запропоновано: Р.Єном [9], М.Істваніком, З.Карпіком [1], Дж.Ліварі, Н.Ліварі [10], Д.Міліком [1]. Не зменшуючи значення зазначених наукових здобутків, доцільно зазначити, що питання менеджменту цифрових ризиків та інформаційної безпеки потребує подальшого дослідження.

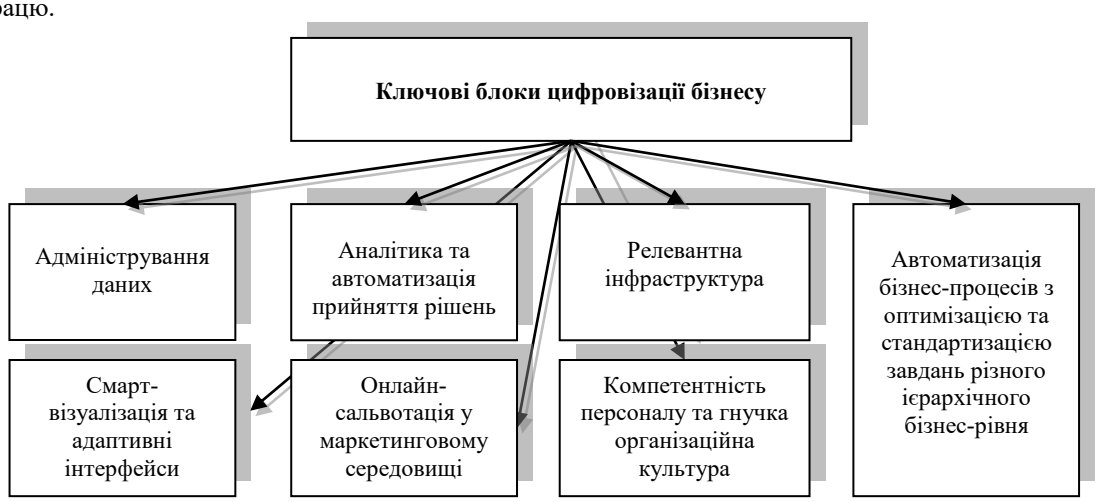
Метою статті є ідентифікація ролі цифровізації бізнесу у сучасному контексті та її впливу на розвиток цифрового бізнесу, а також розробка теоретичних і практичних засад менеджменту цифрових ризиків й інформаційної безпеки як невід'ємної складової успішного ведення цифрового бізнесу.

Викладення основного матеріалу. Сьогодні цифровізація радикально змінила спосіб ведення бізнесу у мінливому з безпрецедентною швидкістю середовищі, розширюючи сфери комунікування з онлайн-покупцями, де головними перевагами є зручність, миттєве отримання відповіді менеджерів, а також низькі витрати. Сучасні покупці зі швидко зростаючими потребами здійснюють покупки онлайн завдяки персоналізації через соціальні мережі та чекають миттєвої обробки замовлення з подальшою доставкою товару. У результаті дослідження та аналізу робіт провідних вчених й економістів [1–3] визначено ключові блоки цифровізації бізнесу, що дозволяють своєчасно реагувати на ринкові запити онлайн-покупців (рис. 1).

Відповідно до рисунка 1, за текстом наведено інтерпретацію ключових блоків цифровізації бізнесу. Так загальне адміністрування даних, їх когерентність та якість, а також дієві бізнес-моделі дозволяють акумулювати й обробляти великі за обсягом масиви даних (структуровані, неструктуровані). А передові статистичні методи й алгоритми у комплексі зі штучним інтелектом (враховуючи когнітивних агентів)

© А.О. Наторіна, 2019

сприяють розробці альтернативних рішень, що базуються на аналітиці. Модернізоване середовище даних, що містить архітектуру даних та базові системи, стає гнучким завдяки віртуалізації і використанню хмарних технологій. Релевантна інфраструктура забезпечує стабільну та злагоджену взаємодію онлайн-покупців та менеджерів одночасно на різних пристроях. У свою чергу, онлайн-інструменти та додатки надають онлайн-покупцям та менеджерам можливість контролювати, моніторити й аналізувати сукупність своїх послідовних дій онлайн. Партнерство з суб'єктами онлайн-простору розширює можливості цифрового бізнесу та прискорює експансію необхідної ринкової частки. Персонал володіє цифровими знаннями, вміннями, навичками і достатнім досвідом для роботи у сфері цифрового бізнесу, що безпосередньо пов'язана з аналітикою. А гнучка організаційна культура заохочує плідну співпрацю.



Довідка: розроблено автором на базі [1–3]

Рис. 1. Ключові блоки цифровізації бізнесу

Цифровізація забезпечила масове створення онлайн-платформ, де суб'єкти підприємницької діяльності можуть здійснювати продаж товарів, надавати онлайн-послуги, а також сприяла популяризації і розвитку цифрового бізнесу. У свою чергу, цифровий бізнес форматує імперативи менеджменту цифрових ризиків та інформаційної безпеки завдяки імплементації інноваційних технологічних бізнес-підходів з метою генерування безлічі альтернативних рішень керівництва і запобігання ринкових загроз. Під час формування вибірки прийнятних альтернативних адміністративних рішень автором запропоновано п'ять контурів адаптації та/або секвестування поточного комплексу маркетингових програм і заходів:

1. Розробка обґрунтованої візії менеджменту цифрових ризиків та інформаційної безпеки, що враховує специфіку підвищення рівня онлайн-довіри та облігатні атрибути стійкості цифрового бізнесу. Розробка обґрунтованої візії менеджменту цифрових ризиків та інформаційної безпеки є імпульсом для довгострокового сталого розвитку цифрового бізнесу та базується, головним чином, на онлайн-довірі.
2. Адаптація стратегічних цілей програм та заходів менеджменту цифрових ризиків й асекурації інформаційної безпеки у межах слідування новим реаліям цифрового бізнесу. Відправною точкою програми менеджменту цифрових ризиків та інформаційної безпеки є розробка візії, релевантної усім напрямам цифрового бізнесу, яка є вектором стратегічного планування. Типова мета такої програми полягає у застосуванні ітеративного методичного підходу до планування, генерування та реалізації рішень щодо підвищення рівня інформаційної безпеки, що не суперечить поточному порядку ведення бізнесу в онлайн-просторі.
3. Реновація бекграунду онлайн-довіри та сприяння стійкій проліферації цифрового бізнесу.
4. Проектування акомодаційної контекстно-залежної архітектури інформаційної безпеки. Важливо зауважити, що результати досліджень функціонування українських підприємств в умовах цифровізації [4–7] дають можливість стверджувати, що превалююча більшість з них розробила лише базову візію програми забезпечення інформаційної безпеки, ґрунтуючись на існуючих міжнародних стандартах у сфері IT, таких як ISO/IEC 27001:2013 [8]. Проте вкрай важливо, щоб візія була адаптована шляхом ідентифікації та обліку позитивного і негативного впливу на цифровий бізнес чинників, технологій і цифрових ризиків, що є унікальними з огляду на певні особливості бізнесу.
5. Впровадження комплексу програм менеджменту цифрових ризиків та заходів щодо забезпечення інформаційної безпеки цифрового бізнесу, що базується на інноваційних бізнес-процесах і сприяє перманентній дилатації сегментів ринку.

Впровадження на практиці диференційованих цифрових бізнес-підходів змінює традиційне середовище адміністрування та контролю цифрового бізнесу. При використанні нових цифрових технологій, цифровий бізнес розширює межі власної автономії на ринку та стимулює перехід офлайн-покупців в онлайн, що вимагає забезпечення інформаційної безпеки на високому рівні. А стрімке підвищення рівня омніканальності цифрового бізнесу (наприклад, за рахунок інформаційних систем, пристроїв, додатків та розгалужених IT-взаємозв'язків) ідентифікує проблеми, пов'язані з його масштабованістю, а також з багатьма традиційними рішеннями щодо менеджменту інформаційної безпеки.

Реальність вносить корективи в існуючу практику менеджменту цифрових ризиків та інформаційної безпеки, тому що більшість традиційних бізнес-технологій та методів не дозволяє масштабувати цифровий бізнес. Таким чином значення для цифрового бізнесу принципу мінімальних привілеїв [9] істотно знижується у зв'язку з активною імплементацією agile-методів [10]. З огляду на це цифровий бізнес має раціонально оцінювати власні цифрові ризики та переформатовувати комплекс маркетингових програм і заходів у такий спосіб, щоб вони не перешкоджали, у тому числі реалізації інноваційної політики. Конкурентоспроможність цифрового бізнесу багато у чому залежить від здатності менеджерів раціонально імплементувати інноваційні технологічні підходи на практиці для коректної адаптації стратегічних цілей маркетингової програми, зокрема, для збільшення охоплення потенційних онлайн-покупців.

Цифрове бізнес-середовище пов'язане з безпрецедентними цифровими ризиками, що виходять за межі бізнес-операцій, які охоплюють екосистему цифрового бізнесу, а не окремі його напрями. Отже, візія менеджменту цифрових ризиків та інформаційної безпеки має сприяти проектуванню цифрової ендогенної екосистеми та бути спрямованою на довгостроковий успішний розвиток бізнесу в онлайн-просторі. При аргументації та обґрунтуванні візії цифрового бізнесу рекомендовано врахувати такі референції:

1. Персистентність бізнес-процесів та систематичність імплементації різних технологій. Повномасштабний цифровий бізнес трансформує стандартні бізнес-процеси, модифікує типові бізнес-функції. Це доводить принципову важливість персистентності бізнес-процесів і технологій цифрового бізнесу, що підкреслює необхідність перманентного акцентування уваги менеджерів не тільки на стратегічних цифрових ризиках, але й на операційних. Тому на стадії реалізації бізнес-функцій доцільно слідувати agile-принципам. Персистентность бізнес-процесів та технологій потребує значних інвестицій.
2. Підвищення рівня обізнаності стейкхолдерів з метою формування онлайн-довіри. Проведення інформаційних кампаній є запорукою продуктивного ведення цифрового бізнесу.
3. Підтримка бімодальної IT-стратегії. Одним із завдань фахівців щодо нівелювання цифрових ризиків та забезпечення інформаційної безпеки, у процесі активної співпраці зі стейкхолдерами, має бути розробка сукупності альтернативних перспективних IT-проектів з безпосередньою орієнтацією на бімодальність.
4. Безпрецедентність бізнес-плану та унікальність курсу дій. Нестабільні умови цифрової трансформації унеможливлюють чітку предикативність цифрових ризиків, тому для досягнення поставлених стратегічних цілей менеджерам цифрового бізнесу важливо розглянути найбільш ймовірні цифрові ризики та розробити для них нестандартні ефективні рішення. Адекватна швидка реакція у безпрецедентній поточній ринковій ситуації каталізує прогресивний розвиток цифрового бізнесу.
5. Захист деперсоніфікованих IT-активів, які не перебувають у власності цифрового підприємця і не контролюються ним (хмарні сервіси, мобільні додатки та ін.). Закупівля й експлуатація IT-технологій за межами видимості або контролю IT-департаментів (IT-відділів) – доцільний практичний підхід під час ведення цифрового бізнесу. Децентралізовані витрати на IT побічно детермінують цифрові ризики, які сприяють мінімізації негативних наслідків для цифрового бізнесу, а також призводять до найменших витрат, що пов'язані з ліквідацією негативних наслідків.

Цифровізація змінює вектори організаційної безпеки та оцінки цифрових ризиків, а традиційна бізнес-модель ґрунтується на ключових принципах конфіденційності, цілісності та доступності. Цифровий бізнес створює платформу для протекції даних, IT-інфраструктури, інтегруючи функції, орієнтовані на передачу й обмін даних у навколишньому середовищі, з маркетинговими інструментами, які допомагають безпосередньо впливати на онлайн-покупців. Гарантування інформаційного захисту є партисипативним пріоритетним завданням під час розвитку цифрового бізнесу, адже конфіденційність, цілісність та доступність цієї інформації – завдання більш всеосяжного характеру. Цифровий бізнес має забезпечити інформаційну безпеку як онлайн-покупців, так й онлайн-платформи, завдяки якій відбувається взаємозв'язок з онлайн-покупцями, внаслідок чого утворюється позитивний мікроклімат.

Оскільки цифровий бізнес компліментарно розглядає застосування гетерогенних способів імплементації інноваційних технологій, що обумовлюють різноспрямованість IT-потоків, автором сформульовано директиви менеджменту цифрових ризиків та інформаційної безпеки, які є уніфікованими для реалізації у нестабільних умовах цифрової трансформації.

Директиви менеджменту цифрових ризиків та інформаційної безпеки:

Директива 1. Припинення фокусування на дотриманні певних метрик та перехід до прийняття обґрунтованих стратегічних й оперативних рішень з урахуванням потенційних цифрових ризиків.

Облік потенційних цифрових ризиків полягає у розумінні основних ІТ-загроз, з якими зіштовхується бізнес, та передбачає детермінування пріоритетів контролю й інвестицій з метою нівелювання найбільш ймовірних цифрових ризиків і забезпечення інформаційної безпеки для досягнення оптимальних бізнес-результатів. Цифровізація бізнес-процесів та збільшення кількості суб'єктів підприємницької діяльності в онлайн-середовищі каталізують появу можливих загроз для цифрового бізнесу у нестабільних умовах маркетингового середовища. Симультанна реалізація рівноцінних за фінансовими витратами заходів щодо конфронтування цифрових ризиків й уникнення потенційних погроз не є евентуальною. Реляційне бізнес-мислення, що базується на усвідомленні цифрових ризиків, дозволяє спрямовувати інвестиції у забезпечення інформаційної безпеки, що призводить до ліквідації найбільш ймовірного цифрового ризику, який негативно впливає на цифровий бізнес.

Директива 2. Орієнтація на позитивні бізнес-результати. Синхронність ідентифікації причинно-наслідкових зв'язків між погрозами цифрових ризиків та результатами ведення цифрового бізнесу.

ІТ-інфраструктура цифрового бізнесу має бути максимально розгалуженою та захищеною. Однак цифровим підприємцям не рекомендовано зациклюватися тільки на виконанні типових завдань, та для досягнення бажаних результатів діяльності в онлайн-просторі, що визначаються ключовими метриками (беручи до відома причинно-наслідкові зв'язки між погрозами цифрових ризиків і результатами ведення цифрового бізнесу), необхідно прикладати гранично допустимі зусилля з метою прийняття ефективних стратегічних рішень у сфері менеджменту цифрових ризиків, що сприяють підвищенню прибутковості бізнесу.

Директива 3. Пролонгація дії поточних ІТ, впровадження інноваційних підходів до адміністрування цифрового бізнесу.

Цифровий бізнес має прагнути пролонгувати дію поточних ІТ, традиційних бізнес-операцій із забезпечення інформаційної безпеки та онлайн-доступності. Проте швидкі темпи дисемінації інновацій спонукають підприємців в онлайн-просторі застосовувати відмінні від традиційних інноваційні підходи до впровадження нового інструментарію адміністрування цифрового бізнесу, який є більш гнучким і дозволяє швидко адаптуватися до перманентних змін маркетингового середовища, а також до складання програм щодо нівелювання цифрових ризиків та забезпечення інформаційної безпеки.

Директива 4. Інтерпретація впливу інформаційних потоків на цифровий бізнес.

Цифровий бізнес вимагає розуміння та коректної роботи з диференційованими інтернальними бізнес-процесами та екстернальними колосальними обсягами різнорідних інформаційних потоків. Раціональне ведення цифрового бізнесу має базуватися на інтерпретації менеджерами впливу інформаційних потоків на цифровий бізнес, замість їх контролю. Це дозволить підвищити організаційну стійкість цифрового бізнесу та досягти за короткі терміни бажаних метрик.

Директива 5. Холістичний підхід до менеджменту цифрових ризиків та інформаційної безпеки.

Обґрунтовані виважені рішення щодо менеджменту цифрових ризиків та інформаційної безпеки мають прийматися таким чином, щоб правильно мотивовані онлайн-покупці змогли стати найсильнішою рушійною силою для цифрового бізнесу. Виходячи з цього, важливо знаходити важелі впливу на поведінку онлайн-покупців, мотивувати їх та стимулювати онлайн-покупки. Холістичний підхід до менеджменту цифрових ризиків та інформаційної безпеки підкреслює першорядне значення онлайн-довіри між онлайн-покупцем і керівництвом, а також персональну відповідальність менеджерів цифрового бізнесу у процесі здійснення онлайн-покупок, та виключає обмежувальний, превентивний контроль над інформаційною безпекою.

Директива 6. Інвестиції у розвиток інноваційного та ресурсного потенціалів. Впровадження дієвої методики щодо кіберінцидентів.

Цифровий бізнес має бути зосереджений на запобіганні кібератак та реалізації релевантних запобіжних заходів. Ключовим пріоритетом при успішному веденні цифрового бізнесу є оперативна ідентифікація ризиків та миттєве реагування на них. В умовах цифрової трансформації темпи змін є досить швидкими для того, щоб їх можна було спрогнозувати, наслідком чого є відсутність можливості захисту бізнесу від усіх типів кібератак. Тому для активного розвитку цифрового бізнесу доцільно інвестувати в інноваційний і ресурсний потенціали, щоб зуміти ідентифікувати та нівелювати появу відповідних загроз. Потенціал цифрового бізнесу має сприяти швидкому реагуванню на негативний вплив чинників зовнішнього та внутрішнього середовищ за рахунок впровадження дієвої методики щодо виявлення та аналізу найбільш ймовірних причин, а також наслідків від кіберінцидентів.

Реалізація на практиці зазначених вище директив передбачає готовність цифрового бізнесу адаптуватися до зміни маркетингового середовища та сприяє не лише інтернальній трансформації цифрового бізнесу, але й залученню нових інвестицій для здійснення ефективного менеджменту цифрових ризиків та інформаційної безпеки. Готовність цифрового бізнесу активно імплементувати нові технології та інноваційні підходи є гарантією подальшої успішної ринкової експансії цифрового бізнесу.

Висновки та перспективи подальших досліджень. За результатами проведених ґрунтовних досліджень визначено роль цифровізації бізнесу у сучасних умовах та інтерпретовано ключові блоки цифровізації бізнесу, що дозволяють швидко та своєчасно реагувати на ринкові запити онлайн-покупців і є складовою успішної діяльності в онлайн-просторі. Детерміновано значущість імплементації інноваційних технологічних бізнес-підходів для розвитку цифрового бізнесу та запропоновано п'ять контурів адаптації та/або секвестування комплексу маркетингових програм і заходів. Надано рекомендації щодо врахування відповідних референцій при аргументації та обґрунтуванні візії цифрового бізнесу, що сприятиме ефективному веденню бізнесу у довгостроковій перспективі. Сформульовано директиви менеджменту цифрових ризиків та інформаційної безпеки, які є уніфікованими для реалізації у нестабільних умовах цифрової трансформації. Перспективами подальших досліджень є розробка алгоритмів ідентифікації та оцінки цифрових ризиків, а також комплексу релевантних маркетингових заходів і тактичних дій, спрямованих на їх нівелювання та/або ліквідацію.

Список використаної літератури:

1. *Istvanic M.* Digital Marketing in the Business Environment / *M.Istvanic, D.Milic, Z.Krpic* // International journal of electrical and computer engineering systems. – 2017. – Vol. 8. – No. 2. – P. 67–75.
2. PWC / Retail & Consumer, Report. – 2018 [Electronic resource]. – Access mode : https://www.pwc.ie/publications/2018/retail-consumer-report-2018.pdf.
3. Seeing beyond the loyalty illusion: it's time you invest more wisely / *R.Wollan, Ph.Davis, F.Angelis, K.Quiring* // Accenture. – 2017 [Electronic resource]. – Access mode : https://www.accenture.com/_acnmedia/PDF-43/Accenture-Strategy-GCPR-Customer-Loyalty.pdf.
4. Асоціація рітейлерів України [Електронний ресурс]. – Режим доступу : https://rau.ua/.
5. Disruptions in Retail through Digital Transformation Reimagining the Store of the Future / Deloitte. – 2017 [Electronic resource]. – Access mode : https://www2.deloitte.com/content/dam/Deloitte/in/Documents/CIP/in-cip-disruptions-in-retail-noexp.pdf.
6. *Бурачек І.В.* Pricing intelligence як інструмент підвищення конкурентоспроможності українських інтернет-магазинів / *І.В. Бурачек* // Вісник Житомирського державного технологічного університету / Серія : Економічні науки. – 2016. – № 4. – С. 136–142.
7. *Natorina A.* Online retailers' management system of marketing commodity policy» / *A.Natorina* // Economic Annals-XXI. – 2018. – № 174 (11–12). – С. 69–72.
8. Інформаційні технології. Методи захисту системи управління інформаційною безпекою : ДСТУ ISO/IEC 27001:2015 [Електронний ресурс]. – Режим доступу : https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf.
9. *Yin R.* Case Study Research Design and Methods / *R.Yin* ; 5th ed. – Thousand Oaks, CA : Sage, 2014. – 282 p.
10. *Iivari J.* The relationship between organizational culture and the deployment of agile methods / *J.Iivari, N.Iivari* // Information and Software Technology. – 2011. – № 53 (5). – P. 509–520.

References:

1. Istvanic, M., Milic, D. and Krpic, Z. (2017), «Digital Marketing in the Business Environment», *International journal of electrical and computer engineering systems*, Vol. 8. No. 2, pp. 67–75.
2. PWC (2018), «Retail & Consumer», *Report*, [Online], available at: https://www.pwc.ie/publications/2018/retail-consumer-report-2018.pdf
3. Wollan, R., Davis, Ph., Angelis, F. and Quiring, K. (2017), «Seeing beyond the loyalty illusion: it's time you invest more wisely», *Accenture*, [Online], available at: https://www.accenture.com/_acnmedia/PDF-43/Accenture-Strategy-GCPR-Customer-Loyalty.pdf
4. The Ukrainian Retail Association (2019), [Online], available at: https://rau.ua/
5. Deloitte (2017), «Disruptions in Retail through Digital Transformation Reimagining the Store of the Future», [Online], available at: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/CIP/in-cip-disruptions-in-retail-noexp.pdf
6. Burachek, I.V. (2016), «Pricing intelligence yak instrument pidvy'shhennya konkurentospromozhnosti u ukrai'ns'kyh internet-magazy'niv», *Visnyk Zhytomyrs'kogo derzhavnogo texnologichnogo universytetu*, Seriya *Ekonomichni nauky*, No. 4, pp. 136–142.
7. Natorina, A. (2018), «Online retailers' management system of marketing commodity policy», *Economic Annals-XXI*, No. 174 (11–12), pp. 69–72.
8. DP «UkrNDNC» (2015), *DSTU ISO/IEC 27001:2015 Informacijni tehnologii'. Metody zahystu systemy upravlinnja informacijnoju bezpekoju*, Ukrai'na, Kyi'v, [Online], available at: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf
9. Yin, R. (2014), *Case Study Research Design and Methods*, 5th ed., Thousand Oaks, CA, Sage, 282 p.
10. Iivari, J. and Iivari, N. (2011), «The relationship between organizational culture and the deployment of agile methods», *Information and Software Technology*, No. 53 (5), pp. 509–520.

Наторіна Альона Олександрівна – кандидат економічних наук, начальник відділу статистики і аналітики вищої освіти ДНУ «Інститут освітньої аналітики».

Наукові інтереси:

- економіка, цифровий бізнес, маркетинг, інновації.

ORCID: https://orcid.org/0000-0001-6367-879X

Стаття надійшла до редакції 28.06.2019.