УДК 338.48-022.316:004.056
JEL L83, M15, O33
DOI: 10.26906/EiR.2026.2(101).4643

СПЕЦИФІКА ТА ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ ТУРИСТИЧНОГО ПІДПРИЄМСТВА

Кожухівська Раїса Борисівна*, кандидат економічних наук, доцент
Массель Юрій Сергійович, здобувач вищої освіти освітньо-наукового ступеня «доктор філософії»**
Уманський національний університет

**ORCID 0000-0003-4066-4170*
***ORCID 0009-0000-5355-8305*

Дата надходження статті: 16.03.2026
Дата прийняття статті: 06.04.2026
Дата публікації статті: 29.05.2026

Вступ. Цифрова трансформація сучасної туристичної індустрії докорінно змінила традиційні підходи до ведення бізнесу, перенісши основні операційні процеси у віртуальний простір. Сьогоднішній ринок подорожей неможливо уявити без розгалужених систем онлайн-бронювання, інтегрованих хмарних систем управління, які автоматизують роботу готелів та туристичних підприємств, а також активного використання технологій аналізу великих цифрових даних для персоналізації клієнтських пропозицій. Проте такий стрімкий технологічний прогрес несе в собі не лише стратегічні переваги та підвищення ефективності, але й провокує ескалацію цифрових ризиків всієї галузі перед складними кіберзагрозами.

Актуальність дослідження особливостей цифрової безпеки туристичного підприємства зумовлена низкою критичних факторів, першим з яких є надзвичайно висока концентрація персональних даних. Туристичні підприємства щоденно оперують значними обсягами конфіденційної інформації, що включає не лише повні паспортні дані та детальні банківські реквізити, а й приватні маршрути пересування, деталі сімейного стану та специфічні споживчі переваги. Такий масив даних перетворює туристичне підприємство на пріоритетну ціль для зловмисників, які використовують витончені методи фішингу, атаки на ланцюжки постачання та розповсюдження вимагацького програмного забезпечення з метою шантажу або перепродажу інформації на прихованих мережевих ресурсах.

Окрім того, особливу роль відіграє глобальна мережева взаємозалежність, що є унікальною рисою туристичного продукту. Безпека одного конкретного підприємства не є ізольованим питанням, оскільки вона нерозривно пов'язана із рівнем захищеності контрагентської мережі: від глобальних дистриб'юторських систем та авіакомпаній до дрібних готельних операторів і локальних агрегаторів. Недостатній рівень кіберзахисту окремого контрагента є тригером масштабної компрометації, що ставить під загрозу операційну безпеку усіх інтегрованих з ним партнерів. Паралельно з цим, економічні та репутаційні ризики в туризмі мають кумулятивний характер. Будь-який витік даних або збій у роботі сервісів призводить не просто до миттєвих фінансових втрат через штрафні санкції або зупинку продажів, а спричиняє катастрофічне падіння довіри клієнтів. У сегменті гостинності, де лояльність та відчуття безпеки є фундаментом бренду, відновлення репутації після кіберінциденту може тривати роками або виявитися неможливим в умовах жорсткої глобальної конкуренції. Саме тому необхідність розробки спеціалізованих стратегій цифрового захисту, адаптованих під динамічну та відкриту структуру туристичного бізнесу, стає питанням виживання суб'єктів ринку в умовах сьогодення.

Огляд останніх джерел досліджень і публікацій. Дослідженню питання цифрової безпеки в туризмі та адаптивності бізнесу до кіберзагроз присвячено праці багатьох вітчизняних та закордонних

вчених, чий науковий доробок дозволяє сформувати комплексне бачення існуючих викликів. Зокрема, зарубіжні дослідники M. Aguiar, J. Kiderman, H. Shekar, O. Schilke пропонують розглядати цифрову безпеку крізь призму управління доходами, акцентуючи особливу увагу на вразливості динамічних алгоритмів ціноутворення, які можуть стати об'єктом маніпуляцій з боку конкурентів або хакерів [1]. У свою чергу, M. Hamouda фокусується на технологічних аспектах, досліджуючи ризики використання мобільних додатків у туристичній сфері та пропонуючи вдосконалені протоколи шифрування для гарантування безпеки фінансових транзакцій у режимі реального часу [2]. Аналізуючи стан кіберзахисту вітчизняних підприємств, Д. Попова, С. Яременко вказує на критично низький рівень цифрової грамотності персоналу, визначаючи «людський фактор» як головну слабку ланку в системі безпеки [3]. Цю думку розвивають Watson P., Deller S. [4], І. Олійник [5] та Ю. Миронов [6], які вивчають вплив інформаційних технологій на конкурентоспроможність туристичних підприємств і наголошує на безальтернативності впровадження інтегрованих систем захисту для виявлення складних загроз.

Проблематику безпеки хмарних сервісів, що дедалі частіше використовуються туристичними агенціями для автоматизації офісних процесів, детально висвітлює M. Heinze, вказуючи на ризики втрати контролю над даними у сторонніх сховищах [7]. Правовий вектор дослідження представлений працями І. Похиленко Н. [8] та Н. Головацьким [9], який аналізує стандарти GDPR та їх критичне значення для компаній, що працюють із персональними даними іноземних туристів у межах міжнародного законодавства D. Buhalis, A., Amaranggana, K. Boes, A. Inversini розширюють горизонти проблеми діджиталбезпеки, аналізуючи ризики Інтернету речей у сфері туризму й індустрії розваг та їх безпосередній вплив на приватність гостей [10; 11]. Економічну складову питання підкреслюють автори Д. Сергеєва, І. Нагорна [12], Т. Сімкова, Ю. Копча [13] обґрунтовуючи роль кібербезпеки як базового елемента фінансової стабільності та загальної економічної безпеки підприємства в цифрову епоху.

Психологічні аспекти протидії соціальній інженерії та розробку методик навчання співробітників для захисту від маніпулятивних технік детально розглядають у своїх працях Pham H. C., Ulhaq I., Nguyen M., Nkhoma M. [14], A. Fernández-Morales, S. McCabe, J.D. Cisneros-Martínez [15], М. Давидова та А. Сердюк [16]. Автори-дослідники Л. Гуцал, В. Столяр, С. Павлюк [17], Р. Горчак [18] та О. Графська, В. Холявка, О. Радзімовська, Р. Боднар [19] зосереджують увагу на специфічних проблемах малих та середніх туристичних підприємств, які через обмеженість ресурсів та відсутність власних IT-департаментів залишаються найбільш незахищеними перед глобальними цифровими викликами.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на значну кількість наявних теоретичних напрацювань у галузі кібербезпеки, багато аспектів захисту цифрового контуру туристичних компаній все ще залишаються недостатньо висвітленими та потребують глибшого наукового опрацювання. Зокрема, гостро постає питання створення адаптивних моделей захисту для малих туристичних агентств, які змушені функціонувати в умовах обмеженого бюджету та не мають фінансової спроможності впроваджувати дорогі комплексні рішення корпоративного рівня. Окремої уваги потребує вивчення специфіки безпеки при взаємодії з відкритими програмними інтерфейсами численних систем бронювання, агрегаторів та платіжних шлюзів, оскільки саме ці точки технічного сполучення часто стають вразливими вузлами для несанкціонованого проникнення. Крім того, нагальною є потреба в розробці чітких галузевих стандартів швидкого реагування на інциденти, які б враховували операційні особливості суб'єктів туристичного ринку та дозволяли мінімізувати репутаційні втрати безпосередньо в момент виникнення загрози. У сукупності ці чинники створюють прогалину між загальними теоріями кіберзахисту та практичними потребами сучасного туристичного бізнесу, що вимагає розробки цільових прикладних методик.

Мета дослідження полягає в теоретичному обґрунтуванні та розробка практичних рекомендацій щодо формування комплексної системи цифрової безпеки туристичного підприємства з урахуванням його галузевої специфіки.

Для успішної реалізації поставленої мети дослідження було визначено такі завдання: ідентифікація та визначення основних видів кіберзагроз, що є найбільш характерними та деструктивними для сучасної туристичної індустрії в умовах глобальної цифровізації; розробка комплексного та практично орієнтованого алгоритму дій, спрямованого на ефективну мінімізацію наслідків цифрових атак, що забезпечить стабільність функціонування туристичного підприємства в кризових ситуаціях.

Основний матеріал і результати. Загальні тренди вказують на те, що інформаційні технології продовжують сильно впливати на розвиток туристичної сфери та індустрії гостинності. Покращення та

безперешкодний доступ до інформації, автоматизація процесів, підвищення ефективності обслуговування туристів є ключовими перевагами застосування інформаційних технологій та елементів цифровізації [20, с. 25].

Аналіз сутності та ролі безпеки в системі функціонування туристичної індустрії, дає змогу визначити її як фундаментальну детермінанту конкурентоспроможності туристичного підприємства та важливу складову якості туристичного продукту (послуги). Варто зазначити, що безпека в туризмі, як комплексна багатовекторна система управління ризиками, спрямована на нівелювання загроз життю, здоров'ю, майну та законним інтересам усім суб'єктам туристичної діяльності. У контексті сучасних ринкових трансформацій стратегічне значення безпеки експоненціально зростає, оскільки вона виступає базисом формування споживчої довіри та репутаційного капіталу підприємства, без яких неможлива стабільна операційна діяльність у довгостроковій перспективі.

Важливість формування безпечного цифрового середовища туристичного підприємства зумовлена інтенсивною діджиталізацією галузі та перетворенням суб'єктів господарювання на потужні інформаційні хаби. Специфіка туристичного бізнесу, що полягає в оперуванні великими масивами персональних даних (паспортні відомості, фінансова інформація, маршрути переміщення), детермінує підвищену вразливість підприємств перед кіберзагрозами. Цифрова безпека в даному контексті розглядається не лише як технічний інструмент захисту мережевої інфраструктури, а як критичний чинник комплаєнсу – відповідності міжнародним правовим стандартам та протоколам фінансової безпеки, що мінімізує юридичні та санкційні ризики.

Побудова безпечного цифрового середовища туристичного підприємства ґрунтується на визначенні та аналізі основних видів кіберзагроз, що є найбільш характерними та деструктивними для сучасної туристичної індустрії в умовах глобалізаційних процесів. Ідентифікація та визначення діджитал-небезпек базується на розумінні галузі як відкритої цифрової системи, де дані постійно мігрують між різними суб'єктами, що робить їх надзвичайно вразливими до деструктивних впливів. Найбільш характерною загрозою є цільовий фішинг та методи соціальної інженерії, які експлуатують довіру персоналу шляхом підроблення запитів на бронювання або рахунки від імені бізнес-партнерів, що дозволяє зловмисникам отримувати несанкціонований доступ до внутрішніх систем керування. Не менш руйнівними є атаки на ланцюги постачання, коли об'єктом зламу стає не саме підприємство, а його технологічні партнери – розробники модулів бронювання чи платіжні шлюзи, що призводить до прихованого масового витоку даних банківських карток через вразливості стороннього програмного забезпечення.

Особливе місце серед деструктивних факторів посідають віруси-шифрувальники, які в умовах жорсткої прив'язки туризму до часових рамок здатні повністю паралізувати діяльність компанії у пік сезону, блокуючи доступ до критично важливих баз даних та шантажуючи бізнес оприлюдненням конфіденційної інформації клієнтів. Також значну небезпеку становить захоплення облікових записів у програмах лояльності, що спричиняє не лише прямі фінансові збитки, а й миттєву втрату довіри туристів. Специфічною загрозою є активність автоматизованих інструментів несанкціонованого доступу, які здійснюють масовий збір даних про ціноутворення або фіктивне бронювання місць, що деформує ринкові показники та створює штучний дефіцит інвентарю.

Завершують спектр загроз атаки на канали зв'язку через публічні мережі, які дозволяють перехоплювати дані мобільних додатків у реальному часі. Усі ці виклики вимагають від туристичного підприємства відмови від фрагментарних заходів на користь комплексної моделі цифрової резистентності, здатної протистояти багаторівневим загрозам у глобалізованому інформаційному просторі.

Процес формування цифрової безпеки туристичного підприємства є послідовним та циклічним процесом, який охоплює технічні, організаційні та кадрові аспекти діяльності. Науково обґрунтований підхід формування цифрової безпеки туристичного підприємства передбачає:

– аудит та інвентаризацію цифрових активів;

– аналіз ризиків та моделювання можливих загроз;

– розробку нормативної бази; упровадження технічних засобів захисту; навчання та сертифікація персоналу;

– моніторинг, контроль та реагування на інциденти;

– адаптацію та регулярне оновлення системи (табл. 1).

Процес проєктування комплексного та практично орієнтованого алгоритму мінімізації наслідків кіберінцидентів (рис. 1) базується на методології забезпечення операційної стійкості цифрової еко-

системи підприємства, що передбачає здатність туристичного підприємства підтримувати операційну спроможність за умов деструктивного зовнішнього впливу. Розробка зазначеного алгоритму інтегрує технічні, управлінські та комунікативні субпротоколи, спрямовані на стабілізацію системи в кризових ситуаціях.

Таблиця 1

Процес формування системи цифрової безпеки туристичного підприємства

Етап	Зміст діяльності	Передбачуваний результат
Аудит та інвентаризація	Повний облік цифрових активів: баз даних клієнтів, CRM-систем, каналів зв'язку та ПЗ.	Створення актуального реєстру об'єктів захисту та виявлення «критичних точок» інфраструктури.
Аналіз ризиків	Моделювання загроз (фішинг, втручання в GDS, витоки даних) та оцінка потенційних збитків.	Карта пріоритетних загроз та визначення допустимих рівнів ризику для бізнесу.
Нормативне забезпечення	Розробка внутрішніх регламентів доступу, політик конфіденційності процесів GDPR та PCI DSS.	Юридичне закріплення відповідальності персоналу та легітимізація процесів обробки даних.
Технічна імплементація	Упровадження шифрування, фаєрволів, багатофакторної автентифікації та систем бекапу.	Створення багаторівневого технічного бар'єру проти несанкціонованого доступу та втрати даних.
Кадрова підготовка	Навчання співробітників основам кібергігієни та методам протидії соціальній інженерії.	Трансформація персоналу зі «слабкої ланки» на активний рівень захисту.
Моніторинг та реагування	Налаштування контролю трафіку в реальному часі та підготовка планів відновлення (DRP).	Мінімізація часу технологічних перерв та мінімізація негативного впливу у разі інциденту.
Циклічна адаптація	Регулярне тестування на проникнення до баз даних та оновлення систем захисту.	Підтримка актуального рівня безпеки відповідно до кіберзагроз.

Джерело: побудовано автором за даними [3; 7; 16]

Фундаментальним етапом розробки є ієрархізація бізнес-процесів за критерієм критичності. Алгоритм передбачає ідентифікацію стратегічно важливих інформаційних вузлів (системи дистрибуції, платіжні шлюзи, реєстри персональних даних) та розробку для них моделей автономного функціонування. Це дозволяє впровадити архітектуру «планової деградації» сервісів, за якої другорядні функції обмежуються задля збереження цілісності життєво важливих операційних циклів.

Центральною ланкою алгоритму виступає протокол динамічної локалізації загрози, що реалізує стратегію сегментації мережевого простору. Практична орієнтація даного етапу полягає у розробці механізмів миттєвого ізолювання ураженого сегмента інфраструктури, що дозволяє нівелювати ризик горизонтального розповсюдження шкідливого програмного забезпечення та запобігти масовій ексфільтрації даних. Паралельно передбачається активація резервних каналів передачі інформації, що забезпечує стабільність зв'язку з контрагентами.

Процес відновлення в межах алгоритму базується на технологіях швидкого розгортання систем із верифікованих резервних копій. Науковий підхід до цього етапу вимагає мінімізації показників цільового часу відновлення (максимально допустимий період часу, протягом якого система може залишатися непрацездатною після збою або атаки до моменту повного відновлення її функцій) та цільової точки

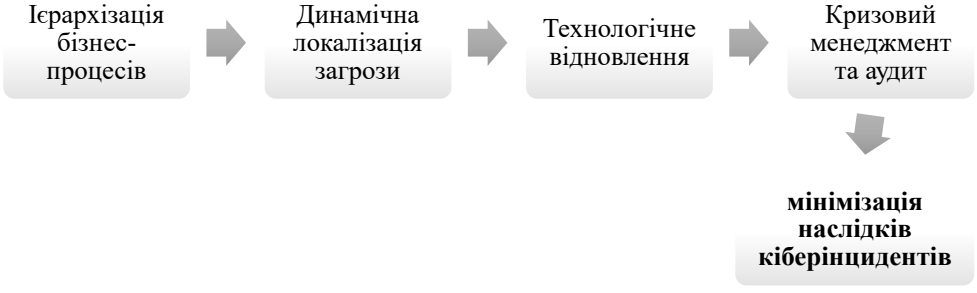

Рис. 1. Алгоритм мінімізації наслідків кіберінцидентів у туристичній індустрії

Джерело: побудовано автором на основі проведеного дослідження

відновлення (максимально допустимий обсяг даних (вимірюється в одиницях часу), який може бути втрачений внаслідок інциденту. Він визначає необхідну частоту резервного копіювання), що є критичним для туристичної індустрії з огляду на високу інтенсивність транзакцій. Це забезпечує безперервність надання послуг та запобігає каскадному накопиченню невиконаних зобов'язань перед клієнтами.

Завершальна фаза формування алгоритму включає кризовий комунікаційний менеджмент та постінцидентний аудит. Комунікаційна складова спрямована на правове та репутаційне регулювання наслідків атаки, що включає інформування стейкхолдерів згідно з вимогами комплаєнсу. Аналітичний етап забезпечує трансформацію отриманого досвіду в оновлені параметри системи безпеки, що гарантує еволюційну адаптацію підприємства до нових видів цілеспрямованих атак та зміцнює загальну стійкість інформаційної екосистеми суб'єкта туристичної діяльності.

Висновки. Отже, безпека в сучасній туристичній індустрії еволюціонувала з допоміжного сервісного елемента у фундаментальну передумову життєздатності бізнесу, де фізичний захист суб'єктів діяльності нерозривно пов'язаний із цілісністю цифрового середовища, у якому вони перебувають.

Варто зауважити, що в умовах тотальної діджиталізації усіх господарсько-економічних процесів та еволюції клієнтських баз даних у базовий інтелектуальний капітал, що визначає конкурентоспроможність туристичного підприємства, формування безпечного цифрового середовища стає ключовим інструментом збереження репутаційного капіталу та забезпечення правової легітимності в глобальному економічному просторі. Ця трансформація зумовлена тим, що сучасне туристичне підприємство фактично функціонує як складний інформаційний вузол, де найменша дестабілізація віртуальної інфраструктури здатна миттєво паралізувати реальні операційні цикли. У такому контексті кібербезпека перестає бути виключно технічним питанням захисту серверів і набуває статусу стратегічної функції управління ризиками. Вона виступає гарантом збереження нематеріальних активів, зокрема споживчої довіри та лояльності, які в сегменті гостинності є надзвичайно чутливими до будь-яких проявів некомпрометованості даних.

Формування цифрової безпеки туристичного підприємства є комплексним, циклічним процесом, що інтегрує технічні, організаційні та кадрові вектори захисту. Процес формування системи цифрової безпеки туристичного підприємства охоплює повний цикл життєдіяльності бізнес-системи: від початкового аудиту активів та ідентифікації критичних точок до безперервної адаптації під нові кіберзагрози. Ключовим елементом системи є перетворення персоналу зі «слабкої ланки» на активний рівень захисту та легітимізація процесів обробки даних згідно з міжнародними стандартами (GDPR, PCI DSS).

Чільне місце у забезпеченні операційної стійкості посідає практично орієнтований алгоритм реагування на інциденти, що базується на методиках керованого обмеження функцій задля збереження операційної цілісності та сегментації мережевого простору. Такий підхід дає змогу миттєво локалізувати загрозу, ізолюючи уражені сегменти без повної зупинки бізнес-процесів. Завдяки оптимізації цільових показників відновлення та використанню верифікованих резервних копій, підприємство здатне підтримувати функціональну спроможність навіть за умов деструктивного впливу. Підсумкова фаза алгоритму, що включає кризові комунікації та аналітичний аудит, забезпечує не лише мінімізацію репутаційних втрат, а й еволюційне зміцнення інформаційної екосистеми суб'єкта туристичної діяльності.

Отже, специфіка та особливості забезпечення цифрової безпеки туристичного підприємства полягають у необхідності захисту складних, територіально розподілених інформаційних систем, які оперують великими масивами конфіденційних даних клієнтів у режимі реального часу. В умовах високої залежності від безперервності онлайн-транзакцій та глобальних мереж бронювання, кіберзахист у туризмі трансформується з суто технічного завдання у стратегічну систему управління ризиками. Вона базується на поєднанні жорстких технологічних бар'єрів, суворого дотримання міжнародних стандартів комплаєнсу та високої адаптивності бізнес-процесів до деструктивних зовнішніх впливів, що в сукупності забезпечує не лише цілісність даних, а й непохитність споживчої довіри до туристичного бренду.

Перспективи подальших розвідок пов'язані з адаптацією безпекових моделей для малого туристичного бізнесу та імплементацією технологій штучного інтелекту для превентивного виявлення аномалій у системах дистрибуції.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Aguiar M., Kiderman J., Shekar H., Schilke O. Safeguarding trust in a digital ecosystem. *Journal of Business Strategy*. 2024. Vol. 45. No.5. pp. 356–362. DOI: https://doi.org/10.1108/JBS-08-2023-0157
2. Hamouda M. Mobile Applications in Tourism: Examining the Determinants of Intention to Use. *International Journal of Technology and Human Interaction.* 2022. Vol. 18. Issue 1. P. 1–13. DOI: https://doi.org/10.4018/IJTHI.293198
3. Попова Д.В., Яременко С.В. Кібербезпека в епоху індустрії 5.0: нові виклики та можливості. *Економічний вісник Донбасу*. 2024. № 3 (77). С. 203–216.
4. Watson P., Deller S. Tourism and economic resilience. *Tourism Economics*. 2022. Vol. 28. P. 1193–1215. DOI: https://doi.org/10.1177/1354816621990943
5. Олійник І.В. Стратегічний розвиток і конкурентоспроможність туристичного бізнесу в умовах військового стану: ризики, пріоритети та інноваційні підходи. *Агросвіт.* 2025. № 4. С. 98–107. DOI: https://doi.org/10.32702/2306-6792.2025.4.98
6. Миронов Ю.Б. Регулювання та прогнозування туристичного попиту в контексті сталого розвитку туризму. *Індустрія туризму і гостинності в Центральній та Східній Європі.* 2024. № 10. С. 17–23.
7. Heinze M. Data Sovereignty & Security in Hospitality. *Techtalk.Travel.* URL: https://www.techtalk.travel/post/data-sovereignty-security-hospitality
8. Похиленко І.С. Правове регулювання захисту персональних даних *Юридичний вісник «Повітряне і космічне право».* 2023. № 4. С. 94–99.
9. Головацький Н.Т. Правове регулювання захисту персональних даних: GDPR та законодавство США, Канади й України. *Науковий вісник Ужгородського Національного Університету.* 2024. Вип. 85. Ч.2. С. 288–292. DOI: https://doi.org/10.24144/2307-3322.2024.85.2.42
10. Buhalis D. Technology in tourism-from information communication technologies to e-Tourism and smart tourism towards ambient intelligence tourism: a perspective article. *Tourism Review*. 2020. Vol. 75. No.1. pp. 267–272. DOI: https://doi.org/10.1108/TR-06-2019-0258
11. Boes K., Buhalis D., Inversini A. Smart tourism destinations: ecosystems for tourism destination competitiveness, *International Journal of Tourism Cities*. 2016. Vol. 2 (2). pp.108–124. DOI: https://doi.org/10.1108/IJTC-12-2015-0032
12. Сергеєва Д.О., Нагорна І.І. Особливості забезпечення економічної безпеки підприємства в умовах цифрової трансформації. *Ефективна економіка*. 2025. № 11. DOI: http://doi.org/10.32702/2307-2105.2025.11.124
13. Сімкова Т., Копча Ю. Стратегічні імперативи забезпечення економічної безпеки підприємства в умовах інноваційного розвитку під впливом невизначеності і ризиків. *Економічний аналіз.* 2025. Т. 35. № 1. С. 167–177. DOI: https://doi.org/10.35774/econa2025.01.167
14. Pham H. C., Ulhaq I., Nguyen M., Nkhoma M. An Exploratory Study of the Effects of Knowledge Sharing Methods on Cyber Security Practice. *Australasian Journal of Information Systems*. 2021. No.25. P. 1–23. DOI: https://doi.org/10.3127/ajis.v25i0.2177
15. Fernández-Morales A., McCabe S., Cisneros-Martínez J.D. Is Social Tourism a Vector for Destination Resilience to External Shocks? Evidence From Spain. *Journal of Travel Research*. 2024. Vol. 63. Issue 7. P. 1606–1625. DOI: https://doi.org/10.1177/00472875231200493
16. Давидова М., Сердюк А. Соціальні аспекти туризму. *Вісник СНТ ННІ бізнесу і менеджменту ХНТУСГ.* 2020. Вип. 1. С. 92–95. URL: https://repo.btu.kharkiv.ua/server/api/core/bitstreams/61281918-3600-46a3-ba0b-18d8d68504c4/content
17. Гуцал Л.А., Столяр В.А., Павлюк С.І. Цифрові технології в організації туристичних подорожей. *Економіка та суспільство*. 2025. Вип. 80. DOI: https://doi.org/10.32782/2524-0072/2025-80-25
18. Горчак Р. Цифровізація внутрішнього туризму в україні: стан, ініціативи та аналітика. *Innovations and Technologies in the Service Sphere and Food Industry.* 2025. Вип. 2 (16). С. 139–145. DOI: https://doi.org/10.32782/2708-4949.2(16).2025.22
19. Графська О.І., Холявка В.З., Радзімовська О.В., Боднар Р.О. Ефективність цифрової трансформації бізнес-процесів підприємств індустрії гостинності. *Академічні візії.* 2026. Вип. 51. С. 1–9. DOI: https://doi.org/10.5281/zenodo.18226301
20. Кожухівська Р.Б. Цифрові технології у туризмі та готельно-ресторанному бізнесі. *Міжнародний науковий журнал «Інтернаука». Сер.: Економічні науки.* 2025. № 3 (95). Т.1. С. 19–26. DOI: https://doi.org/10.25313/2520 2294 2025 3 10694

REFERENCES:

1. Aguiar, M., Kiderman, J., Shekar, H., & Schilke, O. (2024). Safeguarding trust in a digital ecosystem. *Journal of Business Strategy*, vol. 45, no. 5, pp. 356–362. DOI: https://doi.org/10.1108/JBS-08-2023-0157
2. Hamouda, M. (2022). Mobile Applications in Tourism: Examining the Determinants of Intention to Use. *International Journal of Technology and Human Interaction*, no. 18, is.1, pp. 1–13. DOI: https://doi.org/10.4018/IJTHI.293198
3. Popova, D.V., & Yaremenko, S.V. (2024). Kiberbezpeka v epokhu industrii 5.0: novi vyklyky ta mozhlyvosti [Cybersecurity in the era of industry 5.0: new challenges and opportunities]. *Ekonomichnyi visnyk Donbasu – Economic Herald of the Donbas*, no. 3, is. 77, pp. 203–216.
4. Watson, P., & Deller, S. (2022). Tourism and economic resilience. *Tourism Economics*, no. 28, pp. 1193–1215. DOI: https://doi.org/10.1177/1354816621990943

5. Oliinyk, I.V. (2025). Stratehichnyi rozvytok i konkurentospromozhnist turystychnoho biznesu v umovakh viiskovoho stanu: ryzyky, priorytety ta innovatsiini pidkhody [Strategic development and competitiveness of the tourism business in the conditions of martial law: risks, priorities and innovative approaches]. *Ahrosvit – Agrosvit*, vol. 4, pp. 98–107. DOI: https://doi.org/10.32702/2306-6792.2025.4.98

6. Myronov, Y.B. (2024). Rehuliuvannia ta prohnozuvannia turystychnoho popytu v konteksti staloho rozvytku turyzmu [Regulation and forecasting of tourism demand in the context of sustainable tourism development]. *Industriia turyzmu i hostynnosti v Tsentralnii ta Skhidnii Yevropi – Tourism and Hospitality Industry in Central and Eastern Europe*, vol. 10, pp. 17–23.

7. Heinze, M. (2026). *Data Sovereignty & Security in Hospitality.* Techtalk.Travel. Available at: https://www.techtalk.travel/post/data-sovereignty-security-hospitality

8. Pokhylenko, I.S. (2023). Pravove rehuliuvannia zakhystu personalnykh danykh [Legal regulation of personal data protection]. *Yurydychnyi visnyk "Povitriane i kosmichne pravo" – Juridical Bulletin "Air and Space Law"*, vol. 4, pp. 94–99.

9. Golovatskyi, N.T. (2024). Pravove rehuliuvannia zakhystu personalnykh danykh: GDPR ta zakonodavstvo SShA, Kanady y Ukrainy [Legal regulation of personal data protection: GDPR and the legislation of the USA, Canada and Ukraine]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu – Scientific Herald of Uzhhorod National University*, no. 85, is. 2, pp. 288–292. DOI: https://doi.org/10.24144/2307-3322.2024.85.2.42

10. Buhalis, D. (2020). Technology in tourism-from information communication technologies to e-Tourism and smart tourism towards ambient intelligence tourism: a perspective article. *Tourism Review*, no. 75, is. 1, pp. 267–272. DOI: https://doi.org/10.1108/TR-06-2019-0258

11. Boes, K., Buhalis, D., & Inversini, A. (2016). Smart tourism destinations: ecosystems for tourism destination competitiveness. *International Journal of Tourism Cities*, no. 2, is. 2, pp. 108–124. DOI: https://doi.org/10.1108/IJTC-12-2015-0032

12. Serheieva, D. O., & Nahorna, I. I. (2025). Osoblyvosti zabezpechennia ekonomichnoi bezpeky pidpryiemstva v umovakh tsyfrovoi transformatsii [Features of ensuring the economic security of the enterprise in the conditions of digital transformation]. *Efektyvna ekonomika – Efficient Economy*, vol. 11. DOI: https://doi.org/10.32702/2307-2105.2025.11.124

13. Simkova, T., & Kopcha, Yu. (2025). Stratehichni imperatyvy zabezpechennia ekonomichnoi bezpeky pidpryiemstva v umovakh innovatsiinoho rozvytku pid vplyvom nevypravdanosti i ryzykiv [Strategic imperatives of ensuring the economic security of the enterprise in the conditions of innovative development under the influence of uncertainty and risks]. *Ekonomichnyi analiz – Economic Analysis*, no. 35, is. 1, pp. 167–177. DOI: https://doi.org/10.35774/econa2025.01.167

14. Pham, H. C., Ulhaq, I., Nguyen, M., & Nkhoma, M. (2021). An Exploratory Study of the Effects of Knowledge Sharing Methods on Cyber Security Practice. *Australasian Journal of Information Systems*, no. 25, pp. 1–23. DOI: https://doi.org/10.3127/ajis.v25i0.2177

15. Fernández-Morales, A., McCabe, S., & Cisneros-Martínez, J. D. (2024). Is Social Tourism a Vector for Destination Resilience to External Shocks? Evidence From Spain. *Journal of Travel Research*, no. 63 is. 7, pp. 1606–1625. DOI: https://doi.org/10.1177/00472875231200493

16. Davydova, M., & Serdiuk, A. (2020). Sotsialni aspekty turyzmu [Social aspects of tourism]. *Visnyk SNT NNI biznesu i menedzhmentu KhNTUSH – Bulletin of the SNT NNI of Business and Management of KhNTUSG*, no. 1, pp. 92–95. Available at: https://repo.btu.kharkiv.ua/server/api/core/bitstreams/61281918-3600-46a3-ba0b-18d8d68504c4/content

17. Gutsal, L. A., Stoliar, V. A., & Pavliuk, S. I. (2025). Tsyfrovi tekhnolohii v orhanizatsii turystychnykh podorozhei [Digital technologies in the organization of tourist trips]. *Ekonomika ta suspilstvo – Economy and Society*, no. 80. DOI: https://doi.org/10.32782/2524-0072/2025-80-25

18. Gorchak, R. (2025). Tsyfrovizatsiia vnutrishnyoho turyzmu v Ukraini: stan, initsiatyvy ta analityka [Digitalization of domestic tourism in Ukraine: state, initiatives and analytics]. *Innovations and Technologies in the Service Sphere and Food Industry*, vol. 2 (16), pp. 139–145. DOI: https://doi.org/10.32782/2708-4949.2(16).2025.22

19. Grafska, O. I., Kholyavka, V. Z., Radzimovska, O. V., & Bodnar, R. O. (2026). Efektyvnist tsyfrovoi transformatsii biznes-protsesiv pidpryiemstv industrii hostynnosti [Effectiveness of digital transformation of business processes of hospitality industry enterprises]. *Akademichni vizii – Academic Visions*, no. 51, pp. 1–9. DOI: https://doi.org/10.5281/zenodo.18226301

20. Kozhukhivska, R. B. (2025). Tsyfrovi tekhnolohii u turyzmi ta hotelno-restorannomu biznesi [Digital technologies in tourism and hotel-restaurant business]. *Mizhnarodnyi naukovyi zhurnal "Internauka". Ser.: Ekonomichni nauky – International Scientific Journal "Internauka". Series: Economic Sciences*, no.3, is. 95, pp. 19–26. DOI: https://doi.org/10.25313/2520-2294-2025-3-10694

УДК 338.48-022.316:004.056
JEL L83, M15, O33

Кожухівська Раїса Борисівна, кандидат економічних наук, доцент, Уманський національний університет. **Массель Юрій Сергійович,** здобувач вищої освіти освітньо-наукового ступеня «доктор філософії», Уманський національний університет. **Специфіка та особливості забезпечення цифрової безпеки туристичного підприємства.**

У статті досліджено специфіку та особливості забезпечення цифрової безпеки туристичного підприємства. Проаналізовано трансформацію цифрової безпеки з допоміжного технічного аспекту у фундаментальну детермінанту стратегічної стійкості та конкурентоспроможності туристичного підприємства в умовах тотальної діджиталізації галузі. Встановлено, що специфіка туристичного бізнесу, яка полягає в оперуванні значними масивами персональних і фінансових даних клієнтів та глибокій мережевій взаємозалежності суб'єктів ринку, зумовлює експоненціальне зростання вразливості внутрішньокорпоративної ІТ-інфраструктури перед складними кіберзагрозами. Обґрунтовано системний підхід до формування цифрового захисту туристичного підприємства. Розроблено алгоритм забезпечення операційної стійкості, який базується на методології керованого обмеження другорядних функцій задля збереження критичних бізнес-процесів та сегментації мережевого простору для локалізації інцидентів. Підсумкова фаза запропонованого алгоритму дає змогу не лише нівелювати репутаційні втрати, а й забезпечити еволюційну адаптацію інформаційної екосистеми до нових видів цілеспрямованих атак, гарантуючи непохитність споживчої довіри у довгостроковій перспективі.

Ключові слова: туризм, туристичне підприємство, цифрова безпека, кіберстійкість, кіберзагроза.

UDC 338.48-022.316:004.056
JEL L83, M15, O33

Raisa Kozhukhivska, Candidate of Economic Sciences, Associate Professor, Uman National University. **Yurii Massel,** Ph.D. Degree Applicant, Uman National University. **Specifics and features of ensuring digital security in a tourism enterprise.**

The article examines the specific nature and key features of ensuring digital security of a tourism enterprise under conditions of dynamic market transformations. An in-depth analysis is provided of the fundamental transformation in the role of digital security, which, in today's context, has evolved from a highly specialised technical support function into a key determinant of the strategic resilience and competitiveness of entities within the tourism industry. It has been substantiated that in the context of the widespread digitization of industry processes, digital security serves as the foundation for building reputational capital. It has been established that the specific nature of the tourism industry, which involves the handling of large volumes of customers' personal and financial data, as well as a high degree of network interdependence with numerous market players – from airlines to payment systems, – leads to an exponential increase in the vulnerability of internal corporate IT infrastructure against cyber threats. The article scientifically substantiates the need to adopt a systematic approach to the development of digital security, integrating technical, managerial and human resources aspects of countermeasures. Particular attention has been devoted to the development of an algorithm for ensuring operational stability, which is based on the methodology of controlled restriction of secondary functions. Such an approach ensures that critical business processes remain intact even during periods of peak disruptive impacts. The algorithm involves the implementation of protocols for dynamic network segmentation, which enables the immediate localization of cyber incidents and prevents large-scale data exfiltration. It has been proven that the integration of target time metrics and recovery points into an overall security strategy minimises the risk of a cascading accumulation of unfulfilled obligations towards stakeholders. The final phase of the proposed algorithm, which includes post-incident analysis and crisis communications, makes it possible not only to effectively mitigate reputational damage, but also to ensure the continuous, adaptive evolution of the organisation's information ecosystem in response to new types of targeted attacks. This creates a solid foundation for ensuring unwavering consumer confidence and safeguarding the legal legitimacy of the tourism industry in the long term, transforming the safety system into an active tool for sustainable development in the context of global digitalization.

Key words: tourism, tourism enterprise, digital security, cyber resilience, cyber threat.