УДК 338.48:004.056
DOI: https://doi.org/10.32782/2708-0366/2026.27.31

Грабар М.В.
кандидат економічних наук, доцент,
доцент кафедри туризму,
Державний вищий навчальний заклад
«Ужгородський національний університет»
ORCID: https://orcid.org/0000-0002-2753-4462

Hrabar Maryna
State University "Uzhhorod National University"

КІБЕРАТАКИ В ІНДУСТРІЇ ТУРИЗМУ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: ЗАГРОЗИ ТА ВИКЛИКИ КІБЕРСТІЙКОСТІ

CYBERATTACKS IN THE TOURISM INDUSTRY IN THE CONTEXT OF DIGITAL TRANSFORMATION: THREATS AND CHALLENGES TO CYBERRESILIENCE

У статті досліджено вплив кібератак на функціонування туристичної галузі в умовах поглиблення цифрової трансформації. Обґрунтовано, що активне використання онлайн-платформ, цифрових систем бронювання, платіжних сервісів та мобільних застосунків суттєво підвищує вразливість туристичних підприємств до кіберзагроз. Розкрито сутність поняття «кібератака» відповідно до законодавства України та узагальнено найбільш резонансні приклади кіберінцидентів на міжнародному туристичному ринку. Визначено основні типи кібератак та їх наслідки для суб'єктів туристичного бізнесу, зокрема фінансові втрати, репутаційні ризики та порушення безперервності надання послуг. Наголошено на зростанні значення кібербезпеки як складової стратегічного управління та фактора забезпечення кіберстійкості туристичної галузі.

Ключові слова: *кібербезпека, кібератаки, туризм, цифровізація, онлайн-платформи, персональні дані, цифрова стійкість, туристичні підприємства, штучний інтелект.*

The tourism industry is undergoing significant transformations under the influence of digitalization, which includes the introduction of online platforms, booking systems, mobile applications, cloud services and digital payment instruments. Digital technologies provide increased accessibility of tourism services, personalization of offers and optimization of business processes, but at the same time significantly increase the level of vulnerability of tourism enterprises to cyberattacks. The accumulation of significant volumes of personal and payment data of tourists, the integration of numerous information systems and the involvement of external providers of digital services form a complex and potentially dangerous digital ecosystem of tourism. The article examines the impact of cyberattacks on the functioning of the tourism industry in the context of digital transformation. The essence of the concept of "cyberattack" in accordance with the legislation of Ukraine is revealed and the most famous examples of cyber incidents in the international tourism market are summarized. The main types of cyber threats, including phishing, social engineering, data breaches, ransomware attacks and supply chain compromise, are analyzed, and their consequences for various tourism business entities are identified. It is substantiated that cyber incidents cause not only direct financial losses, but also long-term reputational risks, disruption of the continuity of tourism services, and a decrease in consumer trust. Particular attention is paid to the problem of insufficient cyber resilience of small and medium-sized tourism enterprises, which are often the most vulnerable link in the digital tourism environment. Cyberspace is becoming significantly more complex and less predictable, which is caused by the accelerated implementation of new technologies, especially artificial intelligence and the Internet of Things. It is concluded that cybersecurity in modern tourism is not only a technical, but also a strategic management task, the solution of which is a necessary

© Грабар М.В., 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

condition for the sustainable development and competitiveness of the tourism industry in the digital economy.

Keywords: *cybersecurity, cyberattacks, tourism, digitalization, online platforms, personal data, digital resilience, tourism businesses, artificial intelligence.*

Постановка проблеми. Туристична галузь зазнала глибоких змін за останні роки з появою цифрових технологій. Сьогодні туристи бронюють авіаквитки та готелі онлайн, порівнюють ціни на спеціалізованих платформах, діляться своїм досвідом у соціальних мережах та використовують мобільні додатки для навігації по містах, які вони відвідують. Ця зростаюча цифровізація пропонує багато переваг для зацікавлених сторін у сфері туризму, таких як підвищення видимості, оптимізація процесів та персоналізація обслуговування клієнтів.

Однак, зі зростанням залежності від цифрових технологій підвищується ризик кібератак. Кіберзлочинці націлені на туристичні компанії, оскільки вони збирають та зберігають велику кількість конфіденційних даних про своїх клієнтів, таких як платіжна інформація, паспорти та адреси електронної пошти. Ці дані можуть бути використані для зловмисних цілей, таких як крадіжка особистих даних, фінансове шахрайство або захоплення облікового запису. Індустрія туризму потерпає від значної кількості витоків даних. Тому питання кібератак в туризму набуває вагомості та потребує досліджень.

Аналіз останніх досліджень і публікацій. М. Руденко, І. Кочума, О. Кравченко, Н. Третяк досліджували інформаційну безпеку в smart-туризмі. Виявлено, що першочерговим завданням на шляху забезпечення інформаційної безпеки в Smart-туризмі є виявлення причин несанкціонованого доступу до інформації, оцінка загроз для інформаційної безпеки його суб'єктів та створення потужних систем її захисту [6, с. 351].

О. Дзяд, Д. Стародуб розглядали економічні втрати та механізми протидії кіберзлочинності у світовому господарстві. Авторами проаналізовано обсяги, динаміку, чинники зростання кіберзлочинності у світовому господарстві в період пандемії COVID-19, визначено та систематизовано економічні втрати від кіберзлочинності у розрізі країн (регіонів світу), причин виникнення, сфер діяльності постачальників інформаційних технологій та ресурсів [3].

О. Стрижак у дослідженнях цифрової трансформації індустрії туризму наголошує на зростанні залежності підприємств від інформаційних систем і необхідності захисту даних клієнтів [5, с. 41]. Подібну позицію поділяє Р. Горчак, який у працях про цифровізацію внутрішнього туризму в Україні прямо вказує на кібербезпеку як одну з ключових проблем упровадження цифрових платформ та онлайн-сервісів [1, с. 139]. У науковій публікації [2] підкреслюється ризик кібершахрайства та витоку інформації, охарактеризовано особливості технологічного простору кібербезпеки туризму.

Формулювання цілей статті. Метою статті є дослідження впливу кіберзагроз на функціонування туристичної галузі в умовах цифрової трансформації, визначення ключових векторів кібератак на міжнародному туристичному ринку, оцінка економічних, репутаційних та операційних наслідків кіберінцидентів для туристичних підприємств.

Виклад основного матеріалу. Сотні мільйонів приватних і ділових клієнтів зараз довіряють туристичним компаніям свою особисту ідентифікаційну інформацію, дані кредитної картки та інші конфіденційні дані. Туристичні веб-сайти є надзвичайно динамічними, оскільки ціни можуть відрізняються від користувача до користувача. Вони продиктовані поточним попитом, серед інших динамічних параметрів, які витягуються з багатьох джерел, що робить цифрову безпеку веб-сайту ще більш складною. Крім того, існує постійний зв'язок між авіакомпаніями, брендами готельних мереж і агрегаторами, щоб усе відбувалося без проблем. Наслідки для кібербезпеки стають прямопропорційними – більше цілей для туризму спричинює збільшення кібератак хакерів і зловмисних організацій.

Згідно закону України «Про основні засади забезпечення кібербезпеки України» кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [4].

Виходячи з вищенаведеного визначення розглянемо найбільш відомі приклади кібератак, що відбулися на міжнародному туристичному ринку табл. 1.

Таблиця 1

Кібератаки, що відбулися на міжнародному ринку туризму

Інцидентний напад	**Сектор, країна**	**Опис кібератаки**
1	2	3
Шкідливе програмне забезпечення	готель, США	Готелі та курорти Starwood зазнали атаки шкідливого програмного забезпечення, яке викрало дані кредитних та дебетових карток користувачів.
Витік даних	готель, США	Готельна група InterContinental повідомила про витік даних з кредитних карток приблизно в 5000 готелях по всьому світу.
Витік даних	система бронювання подорожей, США	Корпорацію Sabre зламали внаслідок витоку даних, в результаті чого було зібрано дані платіжних карток споживачів та особисту інформацію, що ідентифікує особу.
Витік даних	готель, США	Готелі та курорти Hyatt постраждали від витоку даних платіжних карток гостей у 41 готелі, що управляються корпорацією, в 11 країнах.
Хакінг	бездротовий інтернет, США	Orbitz, дочірня компанія онлайн-турагентства Expedia, повідомила, що хакери отримали доступ до особистої інформації приблизно 880 000 платіжних карток.
Витік даних	авіакомпанія, Велика Британія	Витік даних торкнувся 500 000 клієнтів British Airways. Внаслідок витоку даних було порушено дані для входу, платіжної картки та бронювання подорожей, а дані кредитної картки було викрадено під час їх введення.
Витік даних	авіакомпанія, США	Авіакомпанія Delta підтвердила витік платіжних даних клієнтів внаслідок кібератаки. Хакери мали несанкціонований доступ до інформації про кредитні картки менше ніж 100 000 її клієнтів.
Витік даних	туроператор, Велика Британія	Компанія Thomas Cook заявила про компрометацію даних понад 100 000 клієнтів. Хакери отримали доступ до електронної пошти та деталей паспорта користувачів.
Хакінг	бездротовий інтернет, США	Американська компанія з управління подорожами CWT повідомила, що вона заплатила 4,5 млн дол. США хакерам, які викрали купи конфіденційних корпоративних файлів, і заявила, що вивела з ладу 30000 комп'ютерів.

Продовження таблиці 1

1	2	3
POS-термінал	Ресторан США	Чотири мережі ресторанів у США розкрили випадки крадіжки платіжних карток за допомогою шкідливого програмного забезпечення PoS.
Фішинг	бездротовий інтернет, Нідерланди	Booking.com зазнав кількох кібератак на професійні інтерфейси готельєрів та їхніх клієнтів.
Хакінг	авіакомпанія, Франція	Air France KLM закрила функцію бронювання на своєму порталі туристичних агентів AgentConnect через хакерські атаки. Авіакомпанія повідомила, що кілька онлайн-агентств на французькому ринку постраждали від кібератак.
Хакінг	готель, США	Готельна група Marriot зазнала атаки з витоком даних після того, як хакерська група обдурила співробітника та згодом отримала доступ до комп'ютера.

Джерело: сформовано авторами за даними [12]

Ці приклади показують, що підприємства, яка задіяні у циклі надання туристичних послуг не зважаючи на масштаби своєї діяльності можуть бути вразливі до кіберзломів і повинні захистити свої системи та дані від цих загроз. Незалежно від того, транснаціональна корпорація чи невеликий стартап, жодна туристична компанія не застрахована від загрози кіберзлочинців і шахраїв.

Згідно із Phocuswright, туризм та рекреація є однією з галузей, які найбільше постраждали в усьому світі: кількість спроб цифрового шахрайства за останній рік зросла на 155,9%. Кібератаки в туристичному секторі в основному спрямовані на кредитні картки, особисту інформацію, програми винагород. Майбутні вразливості включають штучний інтелект і метавсесвіт. Індустрія туризму функціонує в середовищі, де численні потенційні точки збою значно ускладнюють запобігання та виявлення порушень кібербезпеки порівняно з іншими галузями [9].

Кібератаки на всі підприємства, але особливо на малий і середній бізнес, стають все більш частими, цілеспрямованими та складними. Згідно з дослідженням Accenture Cost of Cybercrime Study, 43% кібератак спрямовані на малий бізнес, але лише 14% готові захистити себе. Кібератака не тільки порушує нормальну роботу, але й може завдати шкоди важливим IT-активам та інфраструктурі, які неможливо відновити без бюджету чи ресурсів для цього.

Найпоширеніші типи атак на малий бізнес включають [10]:

– фішинг/соціальна інженерія – 57%;
– зламані/викрадені пристрої – 33%;
– крадіжка облікових даних – 30%.

Витрати, пов’язані з витоком даних, можуть тривати від місяців до років і включати значні видатки, про які компанії не знають або не передбачають у своєму плануванні. Наслідки інциденту кібербезпеки можуть проявитися у наступних аспектах: фінансові втрати, втрата продуктивності, шкода репутації, юридична відповідальність, проблеми безперервності бізнесу [11].

Кібератаки можуть мати серйозні наслідки для туризму, які залежать від інформаційних технологій та онлайн-систем для свого функціонування. Розглянемо чим небезпечні кібератаки для туризму.

Крадіжка персональних даних туристів: кіберзлочинці можуть спробувати зламати сайти туроператорів, готелів, авіакомпаній та онлайн-бронювання з метою викрасити особисті дані туристів, такі як ім'я, адреса, номери кредитних карт і паспортні дані. Ця інформація може бути використана для шахрайства, крадіжок та інших злочинів.

Розповсюдження дезінформації: кібератаки можуть бути спрямовані на поширення фальшивої інформації про певні туристичні місця, що може призвести до зниження числа туристів, які їх відвідують. Це може суттєво вплинути на доходи туристичних підприємств та місцевої економіки.

Вимагання виплати викупу: кібератаки типу "ransomvare" можуть зашифрувати важливі дані та системи туристичних компаній, вимагаючи виплати викупу для їх розблокування. Це може призвести до серйозних фінансових втрат і зупинки бізнесу.

Зупинка роботи туристичних послуг: кібератаки можуть призвести до паралічу роботи систем бронювання, авіаліній, готелів або туристичних агентств. Це може викликати негативний вплив на планування подорожей та спричинить розчарування серед туристів.

Пошкодження репутації туристичних підприємств: уразливість туристичних підприємств перед кібератаками може спричинити витоки даних або злому сайтів, що призведе до пошкодження репутації компаній. Негативна публічність може погіршити довіру споживачів.

Зниження інвестицій: постійні кіберзагрози можуть погіршити інтерес інвесторів до туристичних підприємств та місцевої інфраструктури. Відсутність інвестицій може обмежити розвиток туризму та вплинути на економічне зростання регіонів, що залежать від туризму.

Загрози кібербезпеки для туристів: кібератаки також можуть направлятися на туристів, наприклад, через підроблені точки доступу Wi-Fi. Це може призвести до крадіжки персональних даних та грошей туристів або зламу їх пристроїв.

Загалом, кібератаки провокують значні збитки для туризму, а також підривають довіру і безпеку туристів, що може вплинути на здатність галузі досягти свого повного потенціалу. Проактивні заходи з кібербезпеки є сегментами туристичних підприємств та організацій, щоб захистити свої системи та клієнтів від цих загроз.

Кібербезпека сьогодні є не виключно технічною проблемою IT, а й бізнес-ризиком. Тому завдання полягає в тому, щоб впоратися з «внутрішнім корпоративним дисонансом», який виникає з маркетинговими та операційними командами, які хочуть спростити доступ до інформації, яку юридичні та фінансові команди вважають за краще ніколи не фіксувати.

Дослідження під назвою «Кібербезпека в подорожах виходить за межі технологій», вказує на численні характеристики глобальної туристичної індустрії, які роблять її вразливою для хакерів, зокрема: складні системні архітектури, застарілі основні технології, кілька точок контакту з персоналом і клієнтами, дефіцит кадрів і висока плинність кадрів, великі програми винагород, великі профілі клієнтів, низька технічна складність, розпорошені локалізовані операції, обслуговування 24/7/365, великі знижки та схеми винагород, цифрові та локальні точки продажу, кілька способів оплати [9].

Кібербезпека – це складова діяльності, якою має зайнятися практично кожна компанія, щоб забезпечити та підвищити успіх цифрової трансформації своєї операційності (наприклад, автоматизованих процесів, хмарних інструментів або підтримки програмного забезпечення). Глобальний ринок кібербезпеки спонукає зростаюче усвідомлення ризиків і загроз для даних.

Звіт Global Cybersecurity Outlook підкреслює, що кіберпростір стає значно складнішим і менш передбачуваним, що спричинено:

1) прискореним впровадженням нових технологій (особливо штучного інтелекту, IoT тощо);
2) глобальною взаємозалежністю цифрових ланцюгів постачання та IT-систем;
3) загостренням геополітичних напружень.

Опитування, проведені в рамках Outlook 2025, показують, що приблизно 72% організацій зафіксували зростання кіберризиків у 2025 р. Серед найпоширеніших трендів:

– посилення активності ransomeware-груп та хакерів, які використовують автоматизовані інструменти;

– поглиблення ризиків компрометації ланцюгів постачання (supply chain vulnerabilities);

– поява та розширення складних атак з використанням штучного інтелекту [8].

Ці тенденції створюють середовище, де кіберінциденти стають частішими, масштабнішими та складнішими для запобігання.

Ускладнення кіберпростору зумовлено технологічною багатошаровістю та взаємопов'язаністю цифрових систем. Для туризму це означає формування єдиної вразливої екосистеми «туроператор – готель – транспорт – платіжний сервіс – онлайн-платформа». Кіберінцидент в одному елементі ланцюга здатний масштабуватися на всю систему обслуговування туристів, порушуючи безперервність сервісів та довіру клієнтів.

Основною метою кібератак у 2024–2025 рр. залишаються дані. Для туристичної галузі це насамперед персональні та платіжні дані туристів, маршрути подорожей, копії документів, історія бронювань. Масове накопичення таких даних робить туристичні компанії привабливою метою для ransomware-угруповань та фішингових кампаній. Витоки даних у туризмі мають не лише фінансові, а й довгострокові репутаційні наслідки, що безпосередньо впливають на попит.

У туристичному секторі ШІ активно використовують для персоналізації пропозицій, динамічного ціноутворення та клієнтської підтримки. Водночас хакери застосовують ШІ для створення персоналізованих фішингових повідомлень, підроблених сторінок бронювання та deepfake-контенту, що імітує туристичні бренди. Це значно підвищує ефективність соціальної інженерії та складність виявлення атак.

Однією з ключових тенденцій є зростання розриву в кіберстійкості між великими та малими організаціями. Для туризму ця проблема є критичною, оскільки значна частина ринку представлена малими та середніми підприємствами (турагентства, малі готелі, локальні перевізники), які мають обмежені фінансові та кадрові ресурси для інвестування в кіберзахист. Це формує асиметрію ризиків: слабко захищені учасники стають «точками входу» для атак на більші туристичні мережі.

Airbnb стверджує, що шахрайство з кредитними картками, фішинг та шахрайство на туристичних сайтах є найпоширенішими видами шахрайства у Великій Британії. Згідно з їх дослідженням, постраждалі втрачають через шахраїв в середньому 1937 фунтів стерлінгів. Понад дві третини (68%) дорослих британців стверджували, що можуть розпізнати підроблений веб-сайт про подорожі чи бронювання проживання. Однак, коли їх попросили вирішити, чи чотири зображення бронювання житла, створені штучним інтелектом, є справжніми чи підробленими, понад третина (34%) дорослих британців вважали, що зображення, були справжніми, а понад чверть (27%) не були впевнені. Ця складність, з якою стикаються деякі споживачі у виявленні зображень, створених штучним інтелектом, підкреслює важливість бронювання, оплати та спілкування на надійних платформах [7].

Get Safe Online та Airbnb сформували порадами, які допоможуть туристам уникнути шахрайства під час відпустки:

– ніколи не натискайте на неочікувані посилання – шахрайські посилання та вкладення в електронних листах і текстових повідомленнях мають на меті перенаправити на сайти, розроблені так, щоб виглядати як справжній вебсайт компанії, але можуть обманом змусити людей розкрити особисту інформацію, таку як паролі та номери кредитних карток;

– завжди повідомляйте про підозри у шахрайстві;

– остерігайтеся надзвичайно дешевих пропозицій. Не оплачуйте відпустки чи проживання прямим банківським переказом;

– використовуйте перевірені платформи для бронювання, оплати та спілкування – бронювання та оплату проживання слід завжди здійснювати лише на перевірених платформах;

– використовуйте різні паролі для кожного онлайн-облікового запису та додайте двофакторну або багатофакторну автентифікацію [7].

Висновки. Туристична галузь функціонує в умовах зростаючої кібертурбулентності, де кібератаки набувають системного характеру. Висока цифрова інтегрованість, домінування операцій із даними, залежність від ланцюгів постачання та структурна кібернерівність формують підвищену вразливість туристичних підприємств. Мільйони туристів і ділових мандрівників залишають свою особисту ідентифікаційну інформацію та дані кредитної картки на різних веб-сайтах, тому ризики та проблеми кібербезпеки також зростають безпрецедентними темпами. Туристичні оператори можуть бути вразливі до кіберзломів, особливо якщо вони зберігають та обробляють конфіденційні дані своїх клієнтів, такі як імена, адреси, інформацію про кредитні картки тощо.

Встановлено, що кібератаки в туристичній галузі мають системний характер і охоплюють широкий спектр загроз – від фішингових кампаній та соціальної інженерії до витоків даних, ransomware-атак та компрометації ланцюгів постачання. Особливо вразливою до кіберзагроз залишається категорія малих та середніх туристичних підприємств, які мають обмежені фінансові та кадрові ресурси для впровадження комплексних систем кіберзахисту. Це формує асиметрію кіберризиків у галузі та створює додаткові точки входу для атак на більші туристичні мережі.

Обґрунтовано, що в сучасних умовах кібербезпека повинна розглядатися не як суто технічна функція, а як ключовий елемент стратегічного управління та цифрової стійкості туристичних підприємств.

Список використаних джерел:

1. Горчак Р. Цифровізація внутрішнього туризму в Україні: стан, ініціатива та аналітика. *Інновації та технології в сфері послуг і харчування.* 2025. № 2 (16). С. 139–145. DOI: https://doi.org/10.32782/2708-4949.2(16).2025.22

2. Грабар М.В., Машіка Г.В., Кашка М.Ю., Пригара О.В. Концептуальні основи кібербезпеки сфери туризму та рекреації. *Агросвіт.* 2023. № 3–4. С. 43–48. DOI: https://doi.org/10.32702/2306-6792.2023.3-4.43

3. Дзяд О. В., Стародуб Д. С. Економічні втрати та механізми протидії кіберзлочинності у світовому господарстві. *Ефективна економіка.* 2022. № 1. DOI: https://doi.org/10.32702/2307-2105-2022.1.91

4. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 17.01.2026).

5. Стрижак О.О. Трансформації індустрії туризму в умовах цифрової економіки. *Економіка та управління АПК.* 2021. № 2. С. 41–49.

6. Руденко М. В., Кочума І. Ю., Кравченко О. О., Третяк Н. М. Інформаційна безпека у SMART-туризмі: управління ризиками, маркетингові стратегії, перспективи. *Вісник Хмельницького національного університету. Серія: Економічні науки.* 2024. № 2 (328). С. 351–359. DOI: https://doi.org/10.31891/2307-5740-2024-328-42

7. Airbnb and Get Safe Online raise awareness of holiday scams this Easter. URL: https://news.airbnb.com/en-uk/airbnb-and-get-safe-online-raise-awareness-of-holiday-scams-this-easter/ (дата звернення 27.01.2026).

8. Global Cybersecurity Outlook 2025. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (дата звернення 30.01.2026).

9. The new ways cybercriminals are attacking travel companies. URL: https://phocuswire.com/cybercriminals-find-new-ways-to-attack-travel-companies (дата звернення 17.01.2026).

10. Travel's persistent cybersecurity problem, and why it could get worse. URL: https://www.phocuswire.com/cybersecurity-travel-data-online-threats

11. Tourism & Cybersecurity. URL: https://blog.httpcs.com/en/tourism-cybersecurity/ (дата звернення 29.01.2026).

12. Florido-Benítez L. Cybersecurity applied by on-line travel agencies and hotels to protect users' private data in smart cities. *Smart Cities.* 2024. vol. 7 (1). pp. 475–495. DOI: https://doi.org/10.3390/smartcities7010019

References:

1. Horchak R. (2025) Tsyfrovizatsiia vnutrishnoho turyzmu v Ukraini: stan, initsiatyva ta analityka [Digitalization of domestic tourism in Ukraine: status, initiative and analytics] *Innovatsii ta tekhnolohii v sferi posluh i kharchuvannia.* vol. №2 (16), pp. 139–145. DOI: https://doi.org/10.32782/2708-4949.2(16).2025.22 (in Ukrainian)

2. Hrabar M. V., Mashika H. V., Kashka M. Yu. & Pryhara O. V. (2023) Kontseptualni osnovy kiberbezpeky sfery turyzmu ta rekreatsii [Conceptual foundations cyber security of tourism and recreation]. *Ahrosvit.* vol. 3–4, pp. 43–49. DOI: https://doi.org/10.32702/2306-6792.2023.3-4.43 (in Ukrainian)

3. Dzyad O. and Starodub D. (2022) Ekonomichni vtraty ta mekhanizmy protydii kiberzlochyn-nosti u svitovomu hospodarstvi. [Economic losses and international methods against cybercrimes and ways to oppose cybercrimes worldwide] *Efektyvna ekonomika*. vol. 1. DOI: https://doi.org/10.32702/2307-2105-2022.1.91 (in Ukrainian)

4. Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" [Law of Ukraine "On the basic principles of ensuring cybersecurity of Ukraine"]. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (accessed January 17, 2026).

5. Stryzhak O.O. (2021) Transformatsii industrii turyzmu v umovakh tsyfrovoi ekonomiky [Transformations of the tourism industry in the digital economy]. *Ekonomika ta upravlinnia APK*. vol. 2. pp. 41–49. (in Ukrainian)

6. Rudenko M. V., Kochuma I. Yu., Kravchenko O. O., Tretiak N. M. (2024) Informatsiina bezpeka u SMART-turyzmi: upravlinnia ryzykamy, marketynhovi stratehii, perspektyvy [Information security in SMART tourism: risk management, marketing strategies, prospects]. *Visnyk Khmelnytskoho natsionalnoho universytetu. Seriia: Ekonomichni nauky.* vol. 2 (328). pp. 351–359. DOI: https://doi.org/10.31891/2307-5740-2024-328-42 (in Ukrainian)

7. Airbnb and Get Safe Online raise awareness of holiday scams this Easter. Available at: https://news.airbnb.com/en-uk/airbnb-and-get-safe-online-raise-awareness-of-holiday-scams-this-easter/ (accessed January 27, 2026).

8. Global Cybersecurity Outlook 2025. Available at: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (accessed January 30, 2026).

9. The new ways cybercriminals are attacking travel companies. Available at: https://.phocuswire.com/cybercriminals-find-new-ways-to-attack-travel-companies (accessed January 19, 2026).

10. Travel's persistent cybersecurity problem, and why it could get worse. Available at: https://www.phocuswire.com/cybersecurity-travel-data-online-threats

11. Tourism & Cybersecurity. Available at: https://blog.httpcs.com/en/tourism-cybersecurity/ (accessed January 29, 2026).

12. Florido-Benítez L. (2024) Cybersecurity applied by on-line travel agencies and hotels to protect users' private data in smart cities. *Smart Cities.* vol. 7 (1). pp. 475–495. DOI: https://doi.org/10.3390/smartcities7010019

Дата надходження статті: 30.01.2026
Дата прийняття статті: 24.02.2026
Дата публікації статті: 02.03.2026