ІНЖЕНЕРНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ГОТЕЛЬНО-РЕСТОРАННОГО ГОСПОДАРСТВА

УДК 338.48:004.056
DOI https://doi.org/10.37734/2518-7171-2025-3-13

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВ ГОТЕЛЬНО-РЕСТОРАННОГО БІЗНЕСУ

В. М. ПОДОЛЯК, кандидат технічних наук, доцент
(Луцький національний технічний університет)

Анотація. *У статті досліджується проблематика інформаційної безпеки підприємств готельно-ресторанного бізнесу (HoReCa) в умовах цифрової трансформації галузі. Сучасна індустрія гостинності переживає етап переходу від традиційного сервісу до високотехнологічних екосистем, що супроводжується активним впровадженням автоматизованих систем управління, CRM-систем та хмарних сервісів. Це, своєю чергою, створює нові вектори загроз, роблячи заклади гостинності привабливими мішенями для кіберзлочинців через накопичення значних масивів персональних та платіжних даних клієнтів. Метою статті є комплексне дослідження сучасного стану інформаційної безпеки в готельно-ресторанній сфері, виявлення спеціальних загроз та розробка практичних рекомендацій щодо побудови ефективної системи захисту інформаційних ресурсів підприємства в умовах цифровізації галузі. У дослідженні використано методи системного аналізу для класифікації загроз, а також порівняльний аналіз для оцінки ефективності сучасних програмних рішень безпеки. Автором детально проаналізовано специфіку інформаційних потоків у готельно-ресторанному бізнесі. Акцентовано увагу, що особливе місце в загрозах інформаційної безпеки сфери готельно-ресторанного бізнесу посідають технічні вразливості застарілого програмного забезпечення та людський фактор, оскільки велика кількість сезонного персоналу підвищує ризики внутрішніх загроз. Встановлено, що в умовах війни українські готелі та ресторани стикаються з гібридними загрозами, де кібератаки можуть поєднуватися зі збором даних.*

На основі проведеного аналізу авторами запропоновано концептуальну модель системи безпеки «Система мережевої безпеки для індустрії гостинності». Ключовою особливістю розробленої архітектури є її хмарна орієнтація, що є критично важливим для забезпечення безперервності бізнес-процесів в умовах енергетичної нестабільності та фізичних загроз серверному обладнанню в Україні.

Впровадження запропонованої моделі дозволяє мінімізувати капітальні витрати на IT-інфраструктуру, вирішити проблему «людського фактора» через автоматизацію політик безпеки та забезпечити захист як корпоративних даних, так і приватності гостей.

Ключові слова: *інформаційна безпека, індустрія гостинності, кіберзагрози, хмарні технології, захист персональних даних, інформаційна система.*

Постановка проблеми. Сучасний етап розвитку індустрії гостинності характеризується масштабною цифровою трансформацією, де використання автоматизованої системи управління, хмарних сервісів бронювання та програми лояльності стає стандартним виживанням на ринку. Проте стрімка комп'ютеризація підприємств готельно-ресторанного бізнесу сприяє критичному зростанню ризиків у сфері інформаційної безпеки [1].

Автоматизовані системи управління, програмне забезпечення для керування взаємовідносинами з клієнтами та хмарні сервіси дозволяють забезпечити клієнтам персоналізований сервіс, однак створюють нові вектори загроз для інформаційної безпеки, що призводить до зростання кількості викликів кібербезпеки, а також підвищення складності самих загроз.

Аналіз останніх досліджень і публікацій. Вагомий науковий внесок в опрацювання питань управління безпекою підприємств індустрії гостинності зробили такі вітчизняні та зарубіжні дослідники: Л.Г. Агафонова, С.І. Байлик, Е.А. Балашова, Н.М. Гоблик-Маркович, М.І. Миронова, Т. Незвещук-Когут, В. Язіна [5] та ін. Вороняк Є.В. [2] досліджував основні ризики та загрози економічної безпеки підприємств галузі тимчасового розміщення. Проаналізовано їх вплив на рівень економічної безпеки підприємств готельної галузі. Худавердієва В.А. [12] розглянула методологічні засади дослідження інформаційних аспектів безпеки туризму. Особливу увагу приділено актуальному на сучасному етапі розвитку інформаційних технологій безпеки та захисту даних у комп'ютерних мережах. Сусіденко В., Сусіденко О. [10] досліджували комплексне забезпечення

інформаційної безпеки як передумова інноваційного розвитку готельно-ресторанного бізнесу. Стегней М.І., Нодь О.Л., Бергхауер О.О., Кампов Н.С. [7] розглядали трансформацію готельно-ресторанного обслуговування в умовах цифровізації.

Проте, впровадження інформаційної безпеки підприємств готельно-ресторанного бізнесу як чинник підвищення ефективності діяльності підприємств готельно-ресторанної сфери не знайшла достатнього висвітлення в наукових працях і потребує подальшого поглибленого дослідження.

Формування цілей статті. Метою статті є комплексне дослідження сучасного стану інформаційної безпеки в готельно-ресторанній сфері, виявлення спеціальних загроз та розробка практичних рекомендацій щодо побудови ефективної системи захисту інформаційних ресурсів підприємства в умовах цифровізації галузі.

Для досягнення поставленої мети необхідно таке завдання:

– проаналізувати специфіку інформаційних потоків у готельно-ресторанному бізнесі;

– класифікувати основні загрози інформаційній безпеці;

– оцінити стан захисту даних у сфері гостинності;

– запропонувати модель захисту, що включає технічні, організаційні та програмні інструменти для підприємств HoReCa.

Виклад основного матеріалу досліджень. Специфіка інформаційних потоків у готельно-ресторанному бізнесі визначається високою швидкістю обслуговування, цілодобовим циклом роботи та необхідністю синхронізації багатьох складових. Інформаційні потоки в індустрії гостинності мають нелінійний характер – на відміну від виробництва, де потік іде від сировини до продукту, у готелі чи ресторані інформація циркулює між гостем, фронт-офісом та бек-офісом одночасно [2].

Основні вектори руху інформації:

– зовнішні вхідні – бронювання через онлайн-платформи, запити в соцмережах, відгуки на туристичних сайтах;

– внутрішні горизонтальні – комунікація між рецепцією та службою клінінгу або між офіціантом та кухнею;

– внутрішні вертикальні – звітність перед менеджментом, розпорядження щодо стандартів обслуговування;

– вихідні – маркетингові розсилки, підтвердження бронювань, відповіді на скарги [5].

Специфічні особливості інформаційних потоків:

– висока чутливість до часу – затримка передачі інформації про готовність номера або замовлення страви безпосередньо впливає на лояльність клієнта;

– мультимодальність – використання різних каналів одночасно (від усних наказів до складних систем);

– персоналізація – потік даних обов'язково включає специфічні переваги гостя (алергії, улюблений номер, час сніданку) [10].

Систематизація інформаційних потоків за їх призначенням та інструментами реалізації подана в табл. 1.

Особливе місце в загрозах інформаційної безпеки сфери готельно-ресторанного бізнесу посідають технічні вразливості застарілого програмного забезпечення та людський фактор, оскільки велика кількість сезонного персоналу підвищує ризики внутрішніх загроз (табл. 2).

Аналіз наведених загроз свідчить про те, що інформаційна безпека в готельно-ресторанному бізнесі виходить за межі суто технічного захисту серверів. Вона охоплює цілісну екосистему, де безпека гостьового Wi-Fi так само важлива, як і захист централізованої бази даних.

Забезпечення кібербезпеки в індустрії гостинності вимагає переходу від фрагментарних рішень до побудови комплексної екосистеми захисту інформації всього закладу чи мережі. Аналіз сучасної літератури дозволяє виділити спектр технологій, які забезпечують конфіденційність, цілісність та доступність даних:

– системи управління ідентифікацією та доступом;

– інтелектуальний аналіз подій безпеки;

– багатолінійний захист мережі [11].

У сучасному готелі чи ресторані, де персонал має різний рівень доступу до даних (від покоївки,

Таблиця 1

Типологія та характеристика інформаційних потоків на підприємствах готельно-ресторанного бізнесу

Тип потоку	Джерело / Отримувач	Зміст інформації	Ключовий інструмент (IT)
Операційний	Гість ↔ Рецепція / Офіціант	Замовлення послуг, бронювання, процедура реєстрації/виписки	PMS, POS-системи
Виробничо-логістичний	Зал ↔ Кухня; Склад ↔ Постачальник	Технологічні карти, замовлення продуктів, інвентаризація	Модулі складського обліку
Аналітичний	Відділи ↔ Менеджмент	Звіти про завантаженість, показники собівартості продуктів	Програмні інструменти для збору, обробки, аналізу та візуалізації великих обсягів бізнес-даних
Комунікативно-маркетинговий	Ринок ↔ Відділ маркетингу	Відгуки, моніторинг цін конкурентів, використання соціальних мереж	Channel Manager, CRM-системи

Джерело: складено автором на основі [4-9]

Таблиця 2

Класифікація ключових загроз інформаційної безпеки підприємств готельно-ресторанного бізнесу

Категорія загрози	Конкретні типи загроз	Об'єкт впливу	Потенційні наслідки
Кіберзлочинність та зовнішні атаки	Фішинг, віруси-вимагачі, DDoS-атаки	Сервери бронювання, фінансові звіти, бази даних	Фінансові втрати, зупинка операційної діяльності.
Компрометація платіжних даних	Скімінг, злам POS-терміналів, атаки на протоколи оплати	Карткові рахунки клієнтів, транзакційні шлюзи	Штрафні санкції, втрата довіри клієнтів
Внутрішні загрози (людський фактор)	Крадіжка бази лояльності персоналом, несанкціонований доступ	Конфіденційна інформація про VIP-гостей, комерційна таємниця	Репутаційні збитки, перехід клієнтів до конкурентів
Вразливості інфраструктури	Незахищений громадський Wi-Fi, злам систем «Smart Room»	Персональні пристрої гостей, готелю	Витік приватних даних гостей, втручання в особисте життя
Техногенні та системні ризики	Збої в енергопостачанні, помилки в оновленні ПЗ	Хмарні сховища, цифрові архіви	Втрата даних, неможливість поселення або розрахунку гостей.

Джерело: складено автором на основі [1, 2, 6, 12]

офіціанта до фінансового директора), критично важливим є впровадження систем ідентифікації та керування доступом. Це одна з найбільш передових технологій, яка не просто надає доступ до даних, але й дозволяє чітко регламентувати ролі та повноваження кожного з користувачів, визначаючи правила, за якими вони надаються або скасовуються.

Функціональна архітектура систем системи управління ідентифікацією та доступом включає:

– технологію єдиного входу, що дозволяє користувачеві авторизуватися в мережі один раз і отримувати доступ до всіх необхідних додатків без повторного введення облікових даних протягом всього часу перебування в мережі. Це зменшує ризик використання слабких паролів;

– багатофакторна аутентифікація – вимагає використання двох або більше доказів ідентичності особи при вході в систему (пароль + смс/біометрія);

– управління життєвим циклом користувача – автоматизують управління обліковим записом від моменту реєстрації працівника до його звільнення. Це критично важливо для блокування доступу звільнених співробітників, які часто стають джерелом інсайдерських загроз;

– поведінковий аналіз – надають фахівцям з безпеки розширену видимість підозрілої поведінки на кінцевих пристроях, навіть тих, до яких вони не мають фізичного доступу [2].

Для обробки величезних масивів даних, які генерує ІТ-інфраструктура закладу готельно-ресторанного бізнесу, використовуються системи інтелектуального аналізу подій безпеки, що поєднують збір даних про події безпеки з їх аналізом у реальному часі для автоматичного виявлення загроз. Ключовою їх перевагою є використання штучного інтелекту та аналізу поведінки користувачів, що дозволяє системі автоматично виявляти інциденти відповідно до цілей управління ризиками організації.

Багатолінійний захист мережі виступає бар'єром між внутрішньою мережею готелю чи ресторану та зовнішнім світом. Він дозволяє фільтрувати вхідний та вихідний трафік, аналізуючи властивості вхідних та вихідних пакетів інформації по тип протоколу, IP-адресу джерела/призначення та портах. Він повинен за замовчуванням відкидати всі пакети, які не дозволені правилами.

Окрему нішу займають спеціалізовані екрани захисту, які аналізують, фільтрують та блокують HTTP/HTTPS-трафік між веб-додатком і користувачами і які захищають веб-додатки (сайти бронювання, портали лояльності). На відміну від звичайних, вони аналізують вміст HTTP-трафіку, запобігаючи специфічним атакам, таким як SQL-ін'єкції та переповнення буфера. Це критично важливо, оскільки у випадку атаки на базу даних кредитних карток саме вони здатні ідентифікувати загрозу та заблокувати запит до бази [8].

На основі проведеного аналізу загроз та порівняння існуючого інструментарію пропонується концептуальна модель «Система мережевої безпеки для індустрії гостинності». Ця система розроблена з урахуванням специфіки готельно-ресторанного бізнесу, де критичним є баланс між зручністю для гостя та жорсткістю політик безпеки.

Концепція хмарно-орієнтованої архітектури враховує досвід функціонування бізнесу в умовах нестабільності енергопостачання та фізичних загроз серверному обладнанню, для українських готелів чи ресторанів найбільш доцільною є повністю хмарна архітектура. На відміну від традиційних локальних рішень, вона не потребує складного апаратного забезпечення на місці, що знижує капітальні витрати та спрощує масштабування. Система базується на рольовій моделі доступу, виділяючи дві групи користувачів це – персонал та клієнти [7].

Запропонована архітектура інтегрує функції, які були виокремлені як критичні та включає чотири основних модулі:

1. Модуль сканування та оцінки вразливостей – ІТ-персонал отримує інструмент для безперервного сканування мережевого периметра. Система автоматично генерує звіти про «дірки» в безпеці (наприклад, не оновлене ПЗ на рецепції), що дозволяє діяти на випередження.

2. Модуль управління політикою – впроваджує стандартизовані протоколи дій в критичних ситуаціях. Наприклад, система блокує доступ до внутрішніх баз даних для пристроїв, які не відповідають корпоративним стандартам безпеки, що вирішує проблему «людського фактора» в роботі системи.

3. Клієнтський модуль самодіагностики – перед підключенням до високошвидкісної мережі готелю чи ресторану, гостя можуть попросити пройти швидке сканування пристрою. Це захищає мережу від інфікування через гаджети відвідувачів, які часто є носіями вірусів.

4. Інтелектуальний моніторинг активів – система веде реєстр усіх підключених ІТ-активів (камери, смарт-ТВ, POS-термінали), що дозволяє адміністратору бачити «сліпі зони» мережі, які часто використовуються хакерами для непомітного проникнення.

Ключовим елементом системи мережевої безпеки для індустрії гостинності є процедура контролю доступу до мережі, згідно з якою процес доступу відбувається наступним чином:

– верифікація – для отримання доступу до мережі користувач (гість або працівник) повинен підтвердити свою особу. Лише після цього персонал (або автоматизована система) надає дозвіл;

– реагування в реальному часі – система забезпечує захист через фаєрвол, який постійно оновлюється. У разі виявлення підозрілої активності (наприклад, спроба вивантаження бази даних), система надсилає миттєве сповіщення адміністратору та автоматично блокує процес порушення;

– керування виправленнями – система дозволяє централізовано завантажувати оновлення для усунення вразливостей на всіх пристроях готелю чи ресторану одночасно.

Отже, стратегія захисту повинна базуватися на комплексному підході: регулярному аудиті вразливостей, навчанні персоналу гігієні кібербезпеки та впровадженні багаторівневої аутентифікації в системах управління.

Висновки. У ході дослідження було встановлено, що інформаційна безпека підприємств готельно-ресторанного бізнесу в умовах глобальної цифровізації є не просто технічним аспектом підтримки ІТ-інфраструктури, а стратегічним компонентом забезпечення економічної стійкості та конкурентоспроможності. Специфіка галузі, що базується на обробці масивів персональних даних та проведенні великої кількості безготівкових транзакцій, робить її критично вразливою до широкого спектра кіберзагроз.

Визначено, що найбільш критичними для готелів та ресторанів є загрози витоку конфіденційних даних клієнтів (через фішинг або вразливості POS-систем) та атаки вірусів-вимагачів, що можуть повністю паралізувати операційну діяльність.

Доведено, що низький рівень цифрової грамотності персоналу залишається «найслабшою ланкою» в системі захисту. Висока плинність кадрів у секторі HoReCa вимагає впровадження автоматизованих протоколів контролю доступу та регулярних тренінгів.

Обґрунтовано, що ефективна система інформаційної безпеки повинна поєднувати технічні засоби (шифрування, моніторинг трафіку, захист пристроїв) із організаційними заходами та жорстким дотриманням міжнародних стандартів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баля Д.М., Рогова Н.В. Сучасні інформаційні технології в діяльності готельно-ресторанного підприємства. *Наука і молодь у XXI сторіччі: збірник матеріалів X Міжнародної молодіжної науково-практичної Інтернет-конференції (м. Полтава, 28 листопада 2024 року).* Полтава: ПУЕТ, 2025. 1127 с. С. 19–21.

2. Воронюк Є.В. Ключові загрози економічній безпеці підприємств готельно-ресторанної галузі. *Бізнес Інформ*. 2021. №6. С. 145–150. DOI: https://doi.org/10.32983/2222-4459-2021-6-145-150

3. Дітковський І.М., Мізюк Б.М. Вплив інформаційних технологій на удосконалення індустрії гостинності. *Матеріали II Міжнар. наук.-практ. конф. «Інновації, тренди та виклики в індустрії гостинності» (м. Львів, 4-5 травня 2023 р.).* Львів: ЛТЕУ, 2023. 190 с. С.162–165.

4. Лисюк Т.В. Інноваційні рішення в готельно-ресторанному бізнесі: технології автоматизації та персоналізації послуг. *Економіка та суспільство,* (67). 2024. DOI: https://doi.org/10.32782/2524-0072/2024-67-13

5. Незвещук-Когут Т., Язіна В. Управління безпекою підприємств індустрії гостинності в сучасних умовах. *Вісник Чернівецького торговельно-економічного інституту.* Вип. I (89), 2023. С. 105–113. DOI: http://doi.org/10.34025/2310-8185-2023-1.89.08

6. Нікітенко С. В. Управлінські виклики цифровізації в готельно-ресторанному бізнесі. *Економічний простір: зб. наук. праць*. 2025. № 202. С. 196–201. DOI: https://doi.org/10.30838/EP.202.196-201

7. Стегней М.І., Нодь О.Л., Бергхауер О.О., Кампов Н.С. Трансформація готельно-ресторанного обслуговування в умовах цифровізації. *Український журнал прикладної економіки та техніки.* 2024. Том 9. № 3. С. 26–29. DOI: https://doi.org/10.36887/2415-8453-2024-3-4

8. Сусіденко В.Т., Гуштан Т.В., Каганець-Гаврилко Л.П., Вакула І. Сучасні інформаційні системи в готельно-ресторанному бізнесі. *Академічні візії.* Вип. 41/2025. DOI: https://doi.org/10.5281/zenodo.15306137

9. Сусіденко В.Т., Підлипний Ю.В., Гуштан Т.В., Каганець-Гаврилко Л.П. Роль інформаційних технологій в готельно-ресторанному бізнесі. *Академічні візії.* Вип. 42/2025. DOI: https://doi.org/10.5281/zenodo.15306391

10. Сусіденко В., Сусіденко О. Комплексне забезпечення інформаційної безпеки як передумова інноваційного розвитку готельно-ресторанного бізнесу. *Економіка та суспільство*, (74). 2025. DOI: https://doi.org/10.32782/2524-0072/2025-74-96

11. Фостолович В., Боцян Т. Місце цифрових трендів в сфері готельноресторанного бізнесу. Економіка. *Управління. Інновації.* 2022. Вип. 2 (31). DOI 10.35433/ISSN2410-3748-2022-2(31)-9

12. Худавердієва В.А. Інформаційна безпека туризму: технології та алгоритми інформаційної безпеки. *Наука і техніка сьогодні. Серія: техніка.* №8(8). 2022. С. 161–174.

REFERENCES

1. Balia, D. M., & Rohova, N. V. (2025). Modern information technologies in the activities of a hotel and restaurant enterprise. In *Science and youth in the XXI century*: *Proceedings of the X International Youth Scientific and Practical Internet Conference* (pp. 19–21). PUET.

2. Voroniuk, Ye. V. (2021). Key threats to the economic security of enterprises in the hotel and restaurant industry. *Business Inform*, (6), 145–150. https://doi.org/10.32983/2222-4459-2021-6-145-150.

3. Ditkovskyi, I. M., & Miziuk, B. M. (2023). The influence of information technologies on the improvement of the hospitality industry. In *Innovations, trends and challenges in the hospitality industry*: *Materials of the II International Scientific and Practical Conference* (pp. 162–165). LTEU.

4. Lysiuk, T. V. (2024). Innovative solutions in the hotel and restaurant business: Technologies of automation and personalization of services. *Economy and Society*, (67). https://doi.org/10.32782/2524-0072/2024-67-13.

5. Nezvashchuk-Kohut, T., & Yazina, V. (2023). Safety management of hospitality industry enterprises in modern conditions. *Herald of Chernivtsi Trade and Economic Institute*, (I (89)), 105–113. http://doi.org/10.34025/2310-8185-2023-1.89.08.

6. Nikitenko, S. V. (2025). Managerial challenges of digitalization in the hotel and restaurant business. *Economic Space*, (202), 196–201. https://doi.org/10.30838/EP.202.196-201.

7. Stehnei, M. I., Nod, O. L., Berkhauer, O. O., & Kampov, N. S. (2024). Transformation of hotel and restaurant service in the conditions of digitalization. *Ukrainian Journal of Applied Economics and Technology*, 9(3), 26–29. https://doi.org/10.36887/2415-8453-2024-3-4.

8. Susidenko, V. T., Hushtan, T. V., Kahanets-Havrylko, L. P., & Vakula, I. (2025). Modern information systems in the hotel and restaurant business. *Academic Visions*, (41). https://doi.org/10.5281/zenodo.15306137.

9. Susidenko, V. T., Pidlypnyi, Yu. V., Hushtan, T. V., & Kahanets-Havrylko, L. P. (2025). The role of information technologies in the hotel and restaurant business. *Academic Visions*, (42). https://doi.org/10.5281/zenodo.15306391.

10. Susidenko, V., & Susidenko, O. (2025). Comprehensive provision of information security as a prerequisite for the innovative development of the hotel and restaurant business. *Economy and Society*, (74). https://doi.org/10.32782/2524-0072/2025-74-96.

11. Fostolovych, V., & Botsian, T. (2022). The place of digital trends in the field of hotel and restaurant business. *Economics. Management. Innovations*, 2(31). https://doi.org/10.35433/ISSN2410-3748-2022-2(31)-9.

12. Khudaverdiieva, V. A. (2022). Information security of tourism: Technologies and algorithms of information security. *Science and Technology Today. Series: Technology*, (8(8)), 161–174.

V. Podoliak, *PhD, Associate Professor (Lutsk National Technical University).* ***Information security for hotel and restaurant businesses***

Abstract. *The article examines the issues of information security of hospitality and restaurant enterprises (HoReCa) in the context of the digital transformation of the industry. The modern hospitality industry is undergoing a transition from traditional services to high-tech ecosystems, which is accompanied by the active implementation of automated management systems, CRM systems and cloud services. This, in turn, creates new threat vectors, making hospitality establishments attractive targets for cybercriminals due to the accumulation of significant amounts of personal and payment data of customers. The purpose of the article is a comprehensive study of the current state of information security in the hospitality and restaurant sector, the identification of special threats and the development of practical recommendations for building an effective system for protecting the enterprise's information resources in the context of the digitalization of the industry. The study uses systems analysis methods to classify threats, as well as comparative analysis to assess the effectiveness of modern software security solutions. The author has analyzed in detail the specifics of information flows in the hospitality and restaurant business. It is emphasized that a special place in the threats to information security in the hotel and restaurant business is occupied by technical vulnerabilities of outdated software and the human factor, since a large number of seasonal personnel increases the risks of internal threats. It has been established that in wartime conditions, Ukrainian hotels and restaurants face hybrid threats, where cyberattacks can be combined with data collection.*

Based on the analysis, the authors proposed a conceptual model of the security system "Network Security System for the Hospitality Industry". The key feature of the developed architecture is its cloud orientation, which is critically important for ensuring the continuity of business processes in conditions of energy instability and physical threats to server equipment in Ukraine.

The implementation of the proposed model allows minimizing capital expenditures on IT infrastructure, solving the problem of the "human factor" through the automation of security policies, and ensuring the protection of both corporate data and guest privacy.

Key words: *information security, hospitality industry, cyber threats, cloud technologies, personal data protection, information system.*

Дата першого надходження статті до видання: 11.11.2025
Дата прийняття статті до друку після рецензування: 09.12.2025
Дата публікації (оприлюднення) статті: 29.12.2025