DOI: https://doi.org/10.32782/2524-0072/2025-74-96

УДК 004.056:640.4(477)

КОМПЛЕКСНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ПЕРЕДУМОВА ІННОВАЦІЙНОГО РОЗВИТКУ ГОТЕЛЬНО-РЕСТОРАННОГО БІЗНЕСУ

COMPREHENSIVE INFORMATION SECURITY AS A PREREQUISITE FOR INNOVATIVE DEVELOPMENT OF THE HOSPITALITY INDUSTRY

Сусіденко Валентин Трохимович
доктор економічних наук,
професор кафедри менеджменту, підприємництва та торгівлі,
Ужгородський торговельно-економічний інститут
Державного торговельно-економічного університету
ORCID: https://orcid.org/0000-0002-4839-3267

Сусіденко Олексій Валентинович
кандидат економічних наук,
доцент кафедри соціальних та економічних дисциплін,
Харківський національний університет внутрішніх справ
ORCID: https://orcid.org/0000-0003-0841-768X

Susidenko Valentin
Uzhgorod Trade and Economic Institute
of the State Trade and Economic University

Susidenko Oleksii
Kharkiv National University of Internal Affairs

Стаття присвячена сфері готельно-ресторанного бізнесу (ГРБ), як складова індустрії гостинності, зазнала суттєвих трансформацій внаслідок цифровізації та змін у споживчій поведінці клієнтів. У зв'язку з активним впровадженням інформаційно-комунікаційних технологій (ІКТ) у процеси бронювання, оплати, обліку, персоналізованого сервісу, взаємодії з клієнтами та аналітики даних, значно зросла кількість персональних і фінансових даних, які обробляються та зберігаються в електронному вигляді. Тим часом, згідно з аналітичним звітом IBM Cost of a Data Breach Report 2023, середня вартість витоку даних у сфері гостинності зросла до 3,36 мільйона доларів США, а час виявлення та усунення витоку в середньому становив 277 днів. В умовах воєнного стану в Україні, підприємства готельно-ресторанного бізнесу вимушені шукати нові шляхи стабілізації, підвищення ефективності й адаптації до нестабільного середовища.

Ключові слова: інформаційна безпека, готельно-ресторанний бізнес, кіберзагрози, інноваційний розвиток, конкурентоспроможність, цифрова трансформація, управління ризиками.

The article examines current challenges and trends in the field of information security of the hotel and restaurant business (HRB) in the context of digital transformation. It is emphasized that the growing number of cyber threats, the introduction of online services, cloud technologies, electronic payment systems and CRM platforms into the activities of hospitality enterprises require an integrated approach to the protection of information resources. The author emphasizes that information security is no longer an exclusively technical function – it is turning into a strategic factor that affects competitiveness, innovation and customer confidence. The author reveals three key areas of research: analysis of current cyber threats to the hotel and restaurant industry, the role of information security in ensuring service quality and competitive advantages, and organizational mechanisms for integrating security into the management system. The article is based on modern statistical and analytical sources, including reports by IBM, UpGuard, Oracle Hospitality, and regulatory and strategic documents of Ukraine, in particular, the National Cybersecurity Strategy. It is substantiated that most Ukrainian enterprises of the GRB, especially small and medium-sized businesses, do not have a clearly defined information security policy, which makes them vulnerable to data leaks, hacker attacks and social engineering. The article proves that comprehensive information security,

which covers technological, personnel, organizational and legal aspects, is a prerequisite for sustainable and innovative development in the digital age. Particular attention is paid to the importance of forming an internal digital security culture at the staff level, integrating the principles of risk-based thinking into management, using cloud solutions, and complying with data protection standards. The article concludes with conclusions regarding the role of information security as a component of strategic management in a dynamic market and hybrid challenges. The author substantiates the need for further research, in particular, in the area of economic justification of investments in information security, analysis of employee behavior in the context of compliance with security policies, and formation of a national system to support the digital resilience of service sector enterprises.

Keywords: information security, hospitality industry, cyber threats, innovative development, competitiveness, digital transformation, risk management.

Постановка проблеми полягає в тому що, військова агресія Російської Федерації проти України створила надзвичайно складні умови для функціонування бізнесу та організацій усіх рівнів. В умовах воєнного стану організації змушені швидко адаптуватися до нових реалій, що включає реорганізацію бізнес-процесів, перебудову ланцюгів постачання, зміну ринків збуту та забезпечення безпеки персоналу. В цих умовах управління змінами набуває критичного значення, оскільки від швидкості і ефективності адаптації залежить виживання організацій.

Аналіз останніх досліджень і публікацій. У світовій та вітчизняній літературі дедалі більше уваги приділяється питанням кризового менеджменту та управління змінами в умовах невизначеності. Зокрема, вагомий внесок зробили такі вітчизняні автори, як Балабанова, Л. В. Василенко, В. О. Зінченко, П. І. Ковальчук, С. П. Зокрема, науковці досліджували питання ефективності контролю в умовах ринкової економіки. Дослідження, проведені в період COVID-19, показали, що адаптація до різких змін середовища може бути вирішальною для збереження конкурентоспроможності організацій. Проте, дослідження управління змінами в умовах воєнного стану є менш поширеними, що обумовлює необхідність поглибленого аналізу існуючих підходів та розробки нових інструментів.

Виділення невирішених раніше частин загальної проблеми. У процесі дослідження управління змінами в організаціях України під час воєнного стану було виявлено кілька невирішених раніше аспектів, які потребують глибшого аналізу та розробки відповідних підходів. Однією з таких проблем є недостатня розробленість механізмів підтримки морального стану та психічного здоров'я працівників у довготривалій кризовій ситуації. Більшість існуючих підходів орієнтовані на короткострокові стратегії, тоді як війна вимагає тривалої підтримки та адаптації.

Ще однією невирішеною проблемою є ефективне управління знаннями та їх передача в умовах високої плинності кадрів і часткової втрати інфраструктури. Питання збереження та накопичення організаційного досвіду стає особливо гострим у воєнний час, коли доступ до традиційних ресурсів обмежений.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження ролі комплексного забезпечення інформаційної безпеки як ключового фактора інноваційного розвитку готельно-ресторанного бізнесу. Для досягнення цієї мети необхідно: проаналізувати сучасні загрози інформаційній безпеці в ГРБ, оцінити вплив інформаційної безпеки на конкурентоспроможність підприємств, розробити рекомендації щодо інтеграції заходів інформаційної безпеки в стратегію інноваційного розвитку ГРБ.

Виклад основного матеріалу дослідження. У межах дослідження комплексного забезпечення інформаційної безпеки в готельно-ресторанному бізнесі доцільно зосередити увагу на трьох ключових напрямах: аналізі сучасних кіберзагроз для ГРБ, оцінці ролі інформаційної безпеки у формуванні конкурентоспроможності та інноваційного розвитку підприємств сфери гостинності, а також визначенні організаційно-технологічних механізмів інтеграції інформаційної безпеки в стратегічне управління.

Перший напрям дослідження зосереджено на глибокому аналізі актуальних загроз інформаційній безпеці в готельно-ресторанній галузі як одній із найдинамічніших і водночас найвразливіших сфер сучасної економіки. У світлі стрімкої діджиталізації бізнес-процесів у сегменті HoReCa, питання захисту інформаційної інфраструктури набуває пріоритетного значення. Готелі та ресторани дедалі частіше інтегрують у свою діяльність високотехнологічні цифрові інструменти – від онлайн-сервісів бронювання та мобільних застосунків

для замовлення послуг до багаторівневих систем управління взаємовідносинами з клієнтами (CRM), електронної комерції та хмарних платформ для зберігання даних [3, с. 16]. Водночас вони зберігають і обробляють значні обсяги чутливої інформації, що стосується персональних та платіжних даних споживачів, включно з паспортними реквізитами, банківськими картками, звичками споживання, історією бронювань і навіть інформацією про пересування.

Цей високий ступінь цифрової інтеграції у поєднанні з великою кількістю точок доступу до інформаційних систем створює передумови для зростання кіберзагроз, які мають як економічні, так і репутаційні наслідки для бізнесу. Відповідно до звітів IBM Security (2023) та Asimily (2024), готельно-ресторанний бізнес систематично входить до переліку найбільш вразливих до кіберзлочинності секторів. Основні причини цього явища – не лише технологічна відкритість, а й відсутність достатньої культури інформаційної безпеки серед працівників, які часто не мають спеціалізованої підготовки у сфері кіберзахисту.

До найпоширеніших форм атак, що становлять серйозну загрозу для підприємств гостинності, належать фішингові кампанії, що імітують легітимні повідомлення та з великою ймовірністю змушують користувачів розкривати конфіденційні дані; методи соціальної інженерії, які передбачають психологічний вплив на працівників з метою доступу до систем управління; атаки на облікові записи адміністраторів, що відкривають кіберзлочинцям шлях до критичних елементів цифрової інфраструктури; віруси-шифрувальники, які блокують доступ до інформаційних систем і вимагають викуп; а також витоки даних, зумовлені використанням незахищених Wi-Fi мереж у публічних зонах готелів. Показовим є те, що у 2023 році, за даними компанії UpGuard, понад 68% усіх інцидентів у сфері гостинності починались із компрометації електронної пошти. Така статистика свідчить не лише про недосконалість технічних заходів безпеки, але й про низький рівень обізнаності персоналу в основах кібергігієни – елементарних правилах безпечної поведінки у цифровому середовищі.

Особливої актуальності проблема набуває в контексті безпекових реалій сучасної України, що перебуває в умовах воєнного стану. У таких обставинах інформаційна безпека підприємств HoReCa набуває не лише комерційного, а й стратегічного значення. Зростає ймовірність реалізації гібридних загроз, які можуть бути спрямовані не лише на знищення або дестабілізацію систем, а й на досягнення політичних чи військових цілей через деструктивний вплив на IT-інфраструктуру об’єктів, що обслуговують іноземних дипломатів, волонтерів, представників міжнародних місій. У таких випадках зловмисники можуть використовувати технології шпигунства, впроваджуючи складне шкідливе програмне забезпечення, що дає змогу вести приховане спостереження, викрадати інформацію або здійснювати саботаж.

У другій під тематичній частині дослідження розглядається роль інформаційної безпеки як чинника конкурентоспроможності та інноваційного розвитку готельно-ресторанних закладів. У сучасних умовах забезпечення конфіденційності даних і цифрової довіри до бренду виступає одним із ключових критеріїв вибору споживачем готельних і ресторанних послуг. Клієнти очікують не лише високого рівня сервісу, а й впевненості в тому, що їхні персональні дані не будуть зкомпрометовані. Це особливо актуально для міжнародних туристів і ділових клієнтів, що бронюють номери онлайн і здійснюють передоплату [1, с. 209]. Як показують дослідження компанії Oracle Hospitality (2023), понад 79% гостей вважають політику конфіденційності готелю важливим фактором при прийнятті рішення про бронювання. Інформаційна безпека таким чином стає не просто вимогою регуляторів, а невід'ємною складовою сервісної якості, репутаційної стійкості і клієнтської лояльності. Успішна реалізація інновацій – зокрема впровадження мобільних додатків, безконтактних систем заселення, смарт-ключів, електронних меню тощо – можлива лише за умови побудови безпечного інформаційного середовища, де кожна точка взаємодії з гостем є контрольованою і захищеною [2, с. 117].

Третій напрям дослідження фокусується на організаційних і технологічних механізмах інтеграції інформаційної безпеки в стратегічне управління готельно-ресторанним підприємством. Комплексне забезпечення інформаційної безпеки передбачає не лише технічне обладнання – сервери, фаєрволи, резервні копії – а й формування внутрішньої політики безпеки, призначення відповідальних осіб, регулярне навчання персоналу та аудит вразливостей. Одним із найважливіших елементів є впровадження принципів

risk-based thinking – тобто побудови системи безпеки не за принципом «що є в наявності», а з урахуванням аналізу реальних ризиків і сценаріїв порушень, притаманних саме цій організації. На практиці це означає, що невеликий готель у провінційному місті повинен захищати інші елементи, ніж готель міжнародної мережі в столиці [5, с. 13]. В українському контексті особливої ваги набуває питання кадрового забезпечення – переважна більшість підприємств не мають фахівців з IT-безпеки, а функції захисту інформації делегуються або зовнішнім провайдерам, або адміністраторам сайтів. Це створює ризики несанкціонованого доступу, зниження оперативності реагування на загрози та формального підходу до безпеки. Одним із рішень може стати впровадження хмарних рішень з вбудованим захистом, які автоматизують оновлення, контроль доступу та ведення логів подій, що суттєво знижує вразливість навіть для малих підприємств [4, с. 88].

Усі ці аспекти свідчать, що інформаційна безпека у готельно-ресторанному бізнесі не повинна розглядатися як суто технічне завдання IT-відділу. Вона має бути інтегрована у всі рівні управління підприємством – від стратегічного до операційного – й сприйматися як фактор стабільності, розвитку та довгострокової конкурентної переваги в умовах постійних зовнішніх загроз і високої турбулентності середовища.

Висновки. Проведене дослідження дозволяє стверджувати, що інформаційна безпека в готельно-ресторанному бізнесі набуває статусу одного з ключових елементів інноваційного розвитку та конкурентоспроможності в цифрову епоху. Зростаюча кількість цифрових каналів обслуговування, онлайн-трансакцій, віддаленого адміністрування й обробки персональних даних клієнтів формує нову реальність, у якій захист інформації є не лише технічною функцією, а повноцінним бізнес-пріоритетом.

У процесі аналізу виявлено, що сучасна практика управління інформаційною безпекою в українських готельно-ресторанних закладах здебільшого не відповідає викликам, що постають унаслідок глобальної цифровізації та кіберзагроз. Значна частина малих і середніх підприємств не має навіть базової політики інформаційної безпеки, що унеможливлює своєчасне реагування на витоки даних, фішингові атаки чи внутрішні загрози. У поєднанні з низьким рівнем цифрової культури персоналу це формує додаткові репутаційні та фінансові ризики, які у довгостроковій перспективі можуть стати фатальними для бізнесу.

Окрему увагу варто приділити тому, що інформаційна безпека дедалі більше впливає на формування клієнтського досвіду та лояльності. Сучасні споживачі очікують не тільки комфортного і швидкого сервісу, а й гарантій захисту своїх даних. У разі компрометації таких даних навіть одиничний інцидент може стати причиною масового відтоку клієнтів і шкоди діловій репутації. Це свідчить, що інвестиції в інформаційну безпеку мають розглядатися не як витрати, а як довгостроковий актив, що створює додану вартість у вигляді довіри, стабільності та адаптивності до цифрових трансформацій.

Важливим результатом дослідження є визначення необхідності інтеграції інформаційної безпеки в загальну систему стратегічного управління готельно-ресторанними підприємствами. Це має проявлятися у створенні внутрішніх політик безпеки, регулярному навчанні персоналу, впровадженні принципів управління ризиками, використанні хмарних захищених платформ і дотриманні національних та міжнародних стандартів. У контексті цифрової трансформації та змін у поведінці споживачів саме такі комплексні дії дозволять підприємствам залишатися конкурентоспроможними, інноваційно гнучкими й захищеними в умовах підвищеної невизначеності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Балабанова Л. В. Управління розвитком підприємства в умовах нестабільного зовнішнього середовища. Київ : КНЕУ, 2020. 211 с.

2. Василенко В. О. Кризовий менеджмент: методологія, практика, перспективи розвитку. Київ : ВД "Професіонал", 2015. 322 с.

3. Гаврилюк О. В. Адаптивне управління в умовах економічних криз і воєнних конфліктів: теорія та практика. Львів : Видавництво ЛНУ імені Івана Франка, 2022. С. 16–24.

4. Зінченко П. І. Управління змінами в організаціях під час війни: стратегічні підходи та практичні інструменти. Харків : ХНЕУ, 2023. С. 85–89.

5. Ковальчук С. П. Кризове управління: український досвід та міжнародні підходи. Одеса : ОНУ імені І. І. Мечникова, 2021. С. 12–18.

REFERENCES:

1. Balabanova L. V. (2020) Upravlinnia rozvytkom pidpryiemstva v umovakh nestabilnoho zovnishnoho seredovyshcha [Enterprise development management in unstable external environment]. Kyiv: KNEU, 211 p.

2. Vasylenko V. O. (2015) Kryzovyi menedzhment: metodolohiia, praktyka, perspektyvy rozvytku [Crisis management: methodology, practice, development prospects]. Kyiv: VD "Profesional", 322 p.

3. Havryliuk O. V. (2022) Adaptyvne upravlinnia v umovakh ekonomichnykh kryz i voiennykh konfliktiv: teoriia ta praktyka [Adaptive management in conditions of economic crises and military conflicts: theory and practice]. Lviv: Vydavnytstvo LNU imeni Ivana Franka, pp. 16–24.

4. Zinchenko P. I. (2023) Upravlinnia zminamy v orhanizatsiiakh pid chas viiny: stratehichni pidkhody ta praktychni instrumenty [Change management in organizations during wartime: strategic approaches and practical tools]. Kharkiv: KhNEU, pp. 85–89.

5. Kovalchuk S. P. (2021) Kryzove upravlinnia: ukrainskyi dosvid ta mizhnarodni pidkhody [Crisis management: Ukrainian experience and international approaches]. Odesa: ONU imeni I. I. Mechnykova, pp. 12–18.