КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1103
УДК 004.056:640.4

Полотай Орест Іванович
кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0000-0003-4593-8601
orest.polotaj@gmail.com

Кухарська Наталія Павлівна
кандидат фізико-математичних наук, доцент, доцент кафедри безпеки інформаційних технологій
Національний університет Львівська Політехніка, Львів, Україна
ORCID: 0000-0002-0896-8361
kukharska.n@gmail.com

Полотай Богдана Ярославівна
старший викладач кафедри туризму та готельно-ресторанної справи
Львівський торговельно-економічний університет, Львів, Україна
ORCID: 0000-0003-1600-2724
bogdanaf@ukr.net

Вітик Юлія Ярославівна
здобувач вищої освіти 3 курсу групи КБ-31, кафедра управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0009-0004-6782-866X
pyrih.ulia2018@gmail.com

ІНФОРМАЦІЙНА БЕЗПЕКА КІБЕРФІЗИЧНИХ СИСТЕМ ЯК ЧИННИК ЯКОСТІ ПОСЛУГ У ГОТЕЛЬНО-РЕСТОРАННОМУ БІЗНЕСІ

Анотація. У статті досліджено роль інформаційної безпеки кіберфізичних систем у забезпеченні якості надання послуг об’єктами готельно-ресторанного бізнесу в умовах цифрової трансформації. Обґрунтовано, що сучасні підприємства індустрії гостинності активно використовують кіберфізичні системи, зокрема системи онлайн-бронювання, електронні замки, POS-системи, системи відеоспостереження та IoT-рішення для управління інженерною інфраструктурою і сервісами «розумних» номерів. Такі системи поєднують програмні, апаратні та мережеві компоненти, що зумовлює зростання кіберризиків і потребу в комплексному підході до інформаційної безпеки. У роботі проаналізовано теоретичні підходи до визначення кіберфізичних систем та багаторівневої моделі їхнього захисту. Побудовано детальну модель загроз для основних складових кіберфізичної інфраструктури готельно-ресторанного бізнесу, що включає технічні, організаційні та людські фактори. Встановлено, що порушення конфіденційності, цілісності або доступності інформації безпосередньо впливає на якість сервісу, рівень задоволеності клієнтів, безпеку гостей і персоналу, а також на фінансову стабільність і репутацію закладів. Особливу увагу приділено аналізу взаємозв’язку між станом інформаційної безпеки окремих компонентів кіберфізичних систем і показниками якості надання послуг. Показано, що недостатній рівень захисту систем бронювання та POS-інфраструктури призводить до збоїв у процесах обслуговування і втрати довіри клієнтів, тоді як уразливості електронних замків, відеоспостереження та IoT-систем створюють загрози фізичній безпеці та комфорту гостей. На основі проведеного аналізу сформовано модель-рекомендації щодо підвищення рівня інформаційної безпеки кіберфізичних систем, яка передбачає впровадження багаторівневих механізмів захисту, регулярний аудит безпеки та підвищення кіберобізнаності персоналу. Отримані результати можуть бути використані керівниками та ІТ-фахівцями підприємств готельно-ресторанного бізнесу для вдосконалення систем управління інформаційною безпекою, а також у подальших наукових дослідженнях, спрямованих на кількісну оцінку впливу кібербезпеки на якість сервісу.

Ключові слова: кіберфізичні системи, інформаційна безпека, кіберзагрози, багаторівневий захист, готельно-ресторанний бізнес, якість послуг, цифровізація, IoT.

ВСТУП

Сучасний готельно-ресторанний бізнес перебуває в умовах активної цифрової трансформації, що зумовлює широке впровадження інформаційних та кіберфізичних систем у всі ключові бізнес-процеси. Автоматизовані системи бронювання, електронні платіжні сервіси, системи контролю доступу, відеоспостереження, клімат-контроль, а також елементи Інтернету речей стали невід'ємною частиною функціонування закладів індустрії гостинності. Використання таких технологій спрямоване на підвищення ефективності управління, оптимізацію ресурсів та покращення якості надання послуг клієнтам.

Разом із тим зростання рівня цифровізації зумовлює появу нових загроз інформаційній безпеці, що безпосередньо впливають на стабільність роботи кіберфізичних систем. Порушення цілісності, конфіденційності або доступності інформаційних ресурсів у готельно-ресторанному бізнесі може призводити до збоїв у процесах обслуговування, фінансових втрат, витоку персональних даних клієнтів, зниження рівня довіри та погіршення репутації закладу. У результаті інформаційна безпека набуває не лише технічного, а й управлінського та сервісного значення.

Кіберфізичні системи, на відміну від традиційних інформаційних систем, поєднують програмні, апаратні та фізичні компоненти, що забезпечують взаємодію цифрового середовища з реальними об'єктами. У готельно-ресторанному бізнесі це проявляється у керуванні доступом до приміщень, автоматизації енергоспоживання, обліку замовлень, моніторингу безпеки та інших критично важливих функціях. Уразливість таких систем до кібератак або технічних збоїв створює ризики, які можуть безпосередньо позначатися на комфорті клієнтів і якості сервісу.

Якість надання послуг у сфері гостинності є комплексною характеристикою, що включає швидкість обслуговування, надійність сервісів, безпеку клієнтів, зручність використання технологій та загальне враження від перебування в закладі. В умовах цифрової економіки інформаційна безпека кіберфізичних систем стає одним із ключових чинників, що формують цю якість. Відсутність належного рівня захисту інформаційних ресурсів може нівелювати переваги сучасних технологій та негативно вплинути на конкурентоспроможність підприємств готельно-ресторанного бізнесу.

Незважаючи на значну кількість наукових досліджень, присвячених проблемам інформаційної безпеки та якості послуг окремо, питання впливу стану інформаційної безпеки кіберфізичних систем на якість обслуговування у готельно-ресторанному бізнесі залишається недостатньо висвітленим. Це зумовлює актуальність даного дослідження та необхідність комплексного аналізу взаємозв'язку між рівнем захищеності кіберфізичних систем і показниками якості послуг у сфері гостинності.

Постановка проблеми. Активне впровадження кіберфізичних систем у діяльність підприємств готельно-ресторанного бізнесу суттєво підвищує рівень автоматизації та цифрової взаємодії з клієнтами, проте водночас загострює проблему забезпечення інформаційної безпеки. Зростання кількості взаємопов'язаних цифрових і фізичних компонентів призводить до розширення поверхні атак, що ускладнює контроль за станом захищеності систем та підвищує ймовірність виникнення інцидентів інформаційної безпеки.

Порушення функціонування кіберфізичних систем унаслідок кібератак, програмних збоїв або несанкціонованого доступу безпосередньо впливає на ключові процеси надання послуг у готельно-ресторанному бізнесі. Відмова систем бронювання, платіжних сервісів, електронних замків або автоматизованих систем управління може

призводити до зниження оперативності обслуговування, виникнення конфліктних ситуацій із клієнтами та погіршення загального рівня сервісу. Таким чином, інформаційна безпека перестає бути виключно технічною проблемою і трансформується у фактор, що впливає на якість послуг і споживче сприйняття закладу.

Складність проблеми полягає також у тому, що на практиці питання інформаційної безпеки кіберфізичних систем часто розглядається ізольовано від оцінювання якості послуг. Управлінські рішення у сфері готельно-ресторанного бізнесу переважно орієнтовані на підвищення комфорту клієнтів і впровадження інноваційних сервісів, тоді як аспекти захисту інформаційних ресурсів розглядаються як другорядні або витратні. Це створює дисбаланс між рівнем технологічного розвитку закладів та рівнем їхньої готовності до протидії сучасним кіберзагрозам.

У зв’язку з цим виникає наукова та практична проблема визначення і обґрунтування впливу стану інформаційної безпеки кіберфізичних систем на якість надання послуг у готельно-ресторанному бізнесі. Відсутність чітких підходів до оцінювання цього впливу ускладнює формування ефективної стратегії управління безпекою та якістю сервісу, що зумовлює необхідність проведення комплексних досліджень у даному напрямі.

Аналіз останніх досліджень і публікацій. Сучасні наукові праці одностайно підкреслюють, що інформаційні системи в готельно-ресторанному бізнесі сьогодні вже не є лише інструментом автоматизації – вони визначають стратегічну адаптацію закладів до умов цифрової економіки і конкурентного середовища. Так, Валентин Сусіденко та співавтори зазначають, що інформаційні технології формують нову модель управління в індустрії гостинності, де кібербезпека є частиною стратегії цифрової присутності підприємства й підвищення його динамічності та прозорості сервісу [11].

В окремому дослідженні Сусіденка підкреслюється, що комплексне забезпечення інформаційної безпеки є передумовою інноваційного розвитку готельно-ресторанного бізнесу, а зростаючі обсяги обробки персональних і фінансових даних висувають нові вимоги до управління ризиками та захисту інформації [10].

Робота Панасенка та інших дослідників демонструє, що цифрова трансформація готельно-ресторанного бізнесу суттєво впливає на організацію сервісу та взаємодію з клієнтами, оскільки інтеграція цифрових технологій дозволяє не лише оптимізувати внутрішні процеси, а й підвищувати рівень безпеки споживачів шляхом впровадження систем відеоспостереження, електронних замків та інших smart-рішень. Таке – дослідження виділяє інформаційну безпеку як одну з головних технологічних і організаційних проблем цифровізації сфери гостинності [5].

Крім того, окремі академічні праці присвячені загальним питанням інформаційної безпеки підприємств і теоретичному осмисленню відповідних механізмів захисту. У статті Кицюка і Пупиніна розглядається сутність поняття «інформаційна безпека», класифікація загроз та принципи побудови захисних систем у підприємствах, що створює загальну платформу для подальших прикладних досліджень у конкретних сферах, таких як гуртовий обслуговуючий бізнес [2].

Попри наявність досліджень цифрових систем і загальних аспектів інформаційної безпеки, саме комплексний аналіз впливу стану інформаційної безпеки кіберфізичних систем на якість надання послуг у готельно-ресторанному бізнесі ще залишається недостатньо висвітленим у науковій літературі. Це підтверджує необхідність подальших досліджень у цьому напрямі, зокрема емпіричних і кількісних оцінок

безпеки конкретних компонентів кіберфізичних систем та їхнього впливу на показники якості сервісу.

Мета статті. Метою статті є дослідження впливу стану інформаційної безпеки кіберфізичних систем на якість надання послуг у готельно-ресторанному бізнесі, а також обґрунтування ролі інформаційної безпеки як ключового чинника забезпечення стабільності сервісних процесів, підвищення рівня довіри клієнтів і конкурентоспроможності підприємств індустрії гостинності.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Кіберфізичні системи (КФС) (англ. Cyber-Physical Systems, CPS) – це складні технічні системи, які інтегрують обчислювальні алгоритми, мережеві засоби й фізичні процеси таким чином, що цифрові (кібернетичні) компоненти тісно взаємодіють з фізичними об’єктами та середовищем. У таких системах датчики і виконавчі пристрої збирають інформацію з фізичного світу, передають її в обчислювальну частину, де здійснюється обробка, аналіз та прийняття рішень, а потім ці рішення впливають на фізичні процеси через механізми управління. Така інтеграція дозволяє створювати адаптивні, автономні й ефективні рішення для моніторингу, контролю та оптимізації поведінки складних систем у реальному часі. Важливою характеристикою КФС є зворотний зв’язок між кібернетичними і фізичними компонентами: дані з фізичного середовища впливають на цифрові обчислення, а цифрові рішення змінюють фізичний стан системи, що забезпечує їхню синхронізовану і складно взаємодіючу роботу. Такі системи широко застосовуються в промисловості, енергетиці, транспорті, медичних технологіях, «розумних» будівлях та інших галузях, де необхідне поєднання цифрових технологій зі складними фізичними процесами [3].

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У готельно-ресторанному бізнесі КФС являють собою інтегровані комплекси апаратних, програмних та мережевих рішень, які забезпечують автоматизацію, контроль і оптимізацію фізичних процесів у закладі. Вони поєднують цифрову обробку інформації з безпосереднім впливом на фізичні об’єкти та середовище, що дозволяє підвищити ефективність управління, покращити якість обслуговування клієнтів та зменшити людський фактор у виконанні рутинних завдань. У таких системах дані, отримані з датчиків, камер, сенсорів або інших пристроїв, обробляються програмним забезпеченням і впливають на фізичні компоненти – наприклад, автоматично регулюють клімат у номері, відкривають двері, керують освітленням або контролюють роботу кухонного обладнання.

КФС у готельно-ресторанному бізнесі можна умовно поділити на кілька типів залежно від їхньої функціональної спрямованості. Перший тип – системи управління доступом і безпекою, що включають електронні замки, турнікети, відеоспостереження та системи сигналізації, які забезпечують контроль за фізичною безпекою приміщень та відвідувачів. Другий тип – системи автоматизації сервісу та обслуговування клієнтів, наприклад, електронне бронювання, POS-термінали, CRM-системи, мобільні додатки для замовлень і доставки, які дозволяють оптимізувати процеси взаємодії з гостями. Третій тип – системи управління внутрішніми процесами закладу, що включають клімат-контроль, енергоменеджмент, автоматизацію кухонного обладнання, управління

запасами та логістику, які забезпечують економію ресурсів і підвищення ефективності роботи персоналу.

Усі ці види КФС взаємопов'язані та утворюють єдину цифрову екосистему закладу. Впровадження таких систем дозволяє не лише підвищити швидкість і точність обслуговування, а й зменшити ризики помилок, забезпечити безперервність сервісу та підвищити рівень задоволеності клієнтів. Водночас збільшення кількості КФС у готельно-ресторанному бізнесі створює додаткові виклики щодо забезпечення їхньої інформаційної безпеки, адже будь-яка уразливість може безпосередньо впливати на якість надання послуг.

Розглянемо детальніше, які з чого складаються КФС в готельно-ресторанному бізнесі.

Системи бронювання є ключовою складовою кіберфізичних систем у готельному та ресторанному бізнесі, оскільки вони забезпечують ефективну організацію взаємодії із клієнтами (рис. 1).

Рис. 1. Життєвий цикл роботи системи бронювання [9]

Такі системи дозволяють автоматизувати процеси резервування номерів або столиків, вести облік наявності вільних ресурсів, здійснювати онлайн-оплату та обробку даних про гостей. Вони інтегруються з CRM-системами та електронними каналами комунікації, що дозволяє персоналу своєчасно реагувати на замовлення, уникати подвійного бронювання та підвищувати якість обслуговування клієнтів. Завдяки аналітичним модулям такі системи можуть прогнозувати заповнюваність і оптимізувати розподіл ресурсів закладу.

Електронні замки забезпечують безпечний доступ до приміщень для гостей і персоналу. Вони можуть працювати через картки, мобільні додатки або безконтактні технології, що дозволяє контролювати хто і коли заходить у номер чи службові приміщення. Системи електронних замків інтегруються з іншими кіберфізичними системами закладу, такими як відеоспостереження або системи бронювання, що забезпечує централізований контроль та підвищує рівень безпеки. Крім безпеки, електронні замки впливають на комфорт гостей, спрощуючи процес заселення та виїзду.

POS-системи (Point of Sale) відповідають за автоматизацію фінансових та торгових процесів у ресторанах і кафе (рис. 2). Вони дозволяють здійснювати облік замовлень, обробку платежів, ведення складських запасів і аналітику продажів у режимі реального часу. Інтеграція POS-систем із CRM-системами та мобільними додатками забезпечує персоналізований сервіс, наприклад, швидке повторне замовлення або збереження історії клієнта. Надійність POS-систем критично важлива,

оскільки будь-який збій може призвести до затримки обслуговування або фінансових втрат.

Системи відеоспостереження забезпечують моніторинг безпеки як гостей, так і персоналу закладу. Вони можуть включати камери спостереження у номерах, коридорах, на кухні або в залах ресторану. Сучасні системи відеоспостереження інтегруються з аналітичними модулями, здатними розпізнавати рух, виявляти підозрілі дії або контролювати дотримання персоналом стандартів обслуговування. Ці системи не лише підвищують рівень безпеки, а й дозволяють удосконалювати управління закладом та оптимізувати процеси обслуговування [6].

Рис. 2. Типова схема роботи POS-системи [1]

IoT-системи у готельному та ресторанному бізнесі включають «розумні» елементи управління кліматом, освітленням та іншими функціями номерів або залів. Наприклад, датчики температури і вологості автоматично регулюють опалення або кондиціонування, освітлення адаптується до часу доби або присутності гостей, а «розумні» номери можуть автоматично запускати різні сервіси під час заселення. Такі системи підвищують комфорт перебування, оптимізують енергоспоживання та дозволяють персоналу закладу концентруватися на обслуговуванні гостей, а не на ручному контролі інженерних систем (рис. 3).

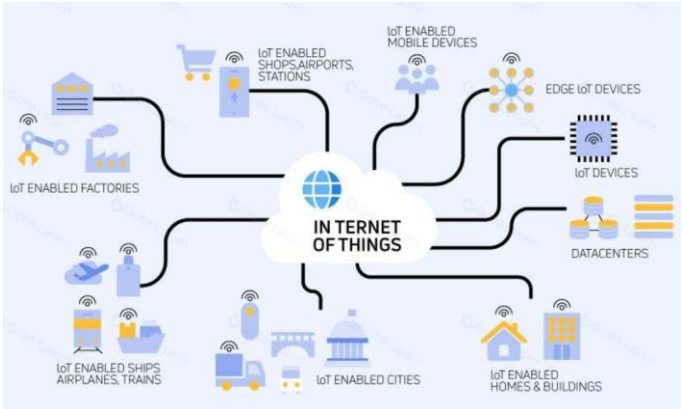

Рис. 3. Структура IoT-системи [12]

Для забезпечення безпеки цих систем необхідно розглядати модель загроз, що охоплює потенційні ризики на фізичному, програмному, мережевому та організаційному рівнях. Опишемо основні загрози інформаційної безпеки складових КФС у вигляді моделі загроз.

Таблиця 1

Модель загрозі інформаційної безпеки складових КФС готельно-ресторанного бізнесу

Складова CPS	Фізичні загрози	Програмні загрози	Мережеві загрози	Організаційні загрози
Системи бронювання	Пошкодження серверів, крадіжка обладнання	Віруси, модифікація або видалення даних про бронювання	Перехоплення даних, Man-in-the-Middle, DDoS, фішинг	Несанкціонований доступ персоналу, порушення політик обробки даних
Електронні замки	Механічне зламування, пошкодження модулів	Підробка цифрових ключів, злом програмного забезпечення	Атаки на канали управління, втручання у синхронізацію з центральною системою	Помилки персоналу при налаштуванні, неправильне видавання доступу
POS-системи	Крадіжка або пошкодження терміналів	Віруси, трояни, модифікація ПЗ для зловживань фінансовими даними	Перехоплення платіжних даних, атаки на сервери обробки платежів, підробка транзакцій	Недбалість персоналу, відсутність контролю доступу до адміністрування
Відеоспостереження	Пошкодження камер, кабелів, крадіжка обладнання	Шкідливе ПЗ для запису або модифікації відео, порушення роботи аналітичних модулів	Перехоплення або підміна відеопотоку, атаки на сервери зберігання відео, DDoS на віддалений доступ	Неналежне керування доступом до архівів, порушення політик конфіденційності
IoT-системи (клімат, освітлення, “розумні” номери)	Пошкодження датчиків, контролерів або виконавчих пристроїв [7]	Злом ПЗ управління кліматом або освітленням, несанкціонована модифікація налаштувань	Атаки через Wi-Fi, ZigBee, Bluetooth; підключення неавторизованих пристроїв; DoS	Неправильне налаштування систем, відсутність оновлень ПЗ, відсутність моніторингу та реагування на інциденти

Системи бронювання піддаються різним видам загроз. До фізичних належать пошкодження або крадіжка серверного обладнання, а також несанкціоноване втручання у сервери, які забезпечують роботу системи. Програмні ризики охоплюють шкідливе програмне забезпечення, віруси, а також спроби змінити чи видалити дані про бронювання. Серед мережевих загроз – перехоплення конфіденційних даних клієнтів, атаки типу «Man-in-the-Middle», DDoS-атаки на сервери та фішинг. Організаційні ризики пов’язані з недотриманням персоналом правил безпеки, несанкціонованим доступом до даних або порушенням політик щодо обробки персональної інформації.

Електронні замки також мають власні категорії загроз. Фізичні ризики включають спроби механічного зламу чи пошкодження електронних компонентів. Програмні загрози стосуються зламу програмного забезпечення або підробки цифрових ключів. Мережеві ризики пов’язані з атаками через бездротові канали, наприклад Wi-Fi, або втручанням у синхронізацію з центральною системою. Організаційні проблеми можуть

виникати через людський фактор – помилки персоналу при налаштуванні доступу чи відсутність знань про дії у разі інцидентів.

POS-системи (системи для обробки платежів) зазнають фізичних загроз у вигляді крадіжки або пошкодження терміналів. Програмні загрози включають віруси, трояни та зміну ПЗ для викрадення фінансових даних. Мережеві ризики пов'язані з перехопленням платіжної інформації або підробкою транзакцій. Організаційні фактори, такі як неуважність працівників чи відсутність контролю доступу до адміністративних функцій, також підвищують ризики безпеки.

Системи відеоспостереження вразливі до фізичного пошкодження камер чи кабелів, а також до крадіжки обладнання. Програмні загрози включають шкідливе ПЗ, яке може спотворювати або видаляти відеозаписи. Мережеві атаки, зокрема підміна відеопотоку, DDoS чи вторгнення в сервери зберігання, також є серйозними ризиками. Організаційні недоліки можуть проявлятися у неналежному контролі доступу до архівів відео або порушенні правил конфіденційності.

IoT-системи, що відповідають за клімат, освітлення чи «розумні» номери, стикаються з фізичними загрозами у вигляді пошкодження датчиків або контролерів. Програмні загрози включають злом систем управління та зміну налаштувань. До мережевих загроз належать атаки через бездротові протоколи (Wi-Fi, ZigBee, Bluetooth), підключення неавторизованих пристроїв і DoS-атаки. Організаційні проблеми можуть бути спричинені неправильним налаштуванням, відсутністю оновлень ПЗ або контролю за інцидентами.

Усі ці загрози взаємопов'язані: компрометація однієї системи може вплинути на інші, створюючи ефект ланцюгового збою. Саме тому модель загроз допомагає визначити критичні ризики та розробити комплексну систему безпеки, що охоплює фізичний, мережевий, програмний та організаційний рівні. Такий підхід забезпечує не лише захист інфраструктури, а й стабільність і якість надання послуг.

Розглянемо, як впливає стан інформаційної безпеки КФС готельно-ресторанного бізнесу на якість надання послуг.

Стан інформаційної безпеки систем бронювання безпосередньо визначає рівень надійності та безперервності обслуговування клієнтів. Захищені системи бронювання забезпечують коректність обліку замовлень, своєчасне підтвердження резервування та збереження персональних і платіжних даних гостей. У разі порушення інформаційної безпеки можливі збої в роботі системи, втрата або підміна даних про бронювання, що призводить до накладок, відмов у заселенні або обслуговуванні, а також до зниження довіри клієнтів. Таким чином, високий рівень інформаційної безпеки систем бронювання є передумовою стабільності сервісу, прогнозованості процесів і позитивного клієнтського досвіду.

Інформаційна безпека електронних замків має безпосередній вплив на фізичну безпеку гостей і їхнє відчуття комфорту. Захищені електронні замки гарантують контрольований доступ до номерів і службових приміщень, виключаючи можливість несанкціонованого проникнення. Уразливість таких систем або порушення їхньої безпеки може призвести до несанкціонованого доступу, втрати особистих речей гостей або виникнення конфліктних ситуацій. Це негативно впливає на сприйняття якості послуг і репутацію закладу. Водночас стабільна і безпечна робота електронних замків підвищує рівень довіри клієнтів і формує відчуття захищеності під час перебування в готелі чи ресторані.

Стан інформаційної безпеки POS-систем критично важливий для забезпечення якості фінансових і торговельних операцій. Захищені POS-системи забезпечують

швидке та безпомилкове обслуговування клієнтів, коректну обробку платежів і збереження фінансових даних. Порушення інформаційної безпеки може призводити до затримок у розрахунках, фінансових втрат, компрометації платіжної інформації та зниження рівня довіри клієнтів. У результаті якість сервісу знижується, оскільки клієнти стикаються з незручностями, чергами або ризиками втрати коштів. Отже, високий рівень захисту POS-систем є необхідною умовою надійного та безперебійного обслуговування.

Інформаційна безпека систем відеоспостереження впливає не лише на рівень фізичної безпеки, а й на організацію процесів обслуговування. Захищені системи відеоспостереження дозволяють оперативно реагувати на інциденти, контролювати дотримання стандартів обслуговування та забезпечувати безпеку гостей і персоналу. Уразливість таких систем може призвести до витоку відеоданих, втрати контролю за приміщеннями або порушення конфіденційності клієнтів. Це негативно впливає на репутацію закладу та сприйняття якості послуг, особливо в умовах підвищеної уваги до захисту персональних даних.

Стан інформаційної безпеки IoT-систем (клімат-контроль, освітлення, «розумні» номери) безпосередньо впливає на комфорт перебування клієнтів. Захищені IoT-рішення забезпечують стабільну роботу систем автоматизації, підтримку оптимального мікроклімату, адаптацію освітлення та персоналізацію сервісів. Порушення безпеки таких систем може призводити до некоректної роботи обладнання, збоїв у кліматичних або освітлювальних режимах, що знижує рівень комфорту і задоволеності гостей. Крім того, компрометація IoT-систем може створювати додаткові ризики для безпеки всієї інфраструктури закладу, що опосередковано впливає на якість надання послуг.

Узагальнюючи, стан інформаційної безпеки кожної складової КФС готельно-ресторанного бізнесу формує комплексний вплив на якість надання послуг. Захищені системи забезпечують стабільність, безпеку, комфорт і довіру клієнтів, тоді як їхня уразливість призводить до зниження рівня сервісу, фінансових втрат і репутаційних ризиків. Таким чином, інформаційна безпека виступає не лише технічним, а й ключовим сервісним чинником у сучасній індустрії гостинності.

Розглянемо основні рекомендації, щодо захисту складових КФС готельно-ресторанного бізнесу, з точки хору багаторівневої системи безпеки.

Багаторівнева система безпеки КФС (рис. 4) передбачає комплексний підхід до захисту як цифрових, так і фізичних компонентів, забезпечуючи цілісність, конфіденційність та доступність даних, а також безпечну роботу всіх елементів системи. Така система безпеки формується як сукупність взаємопов’язаних рівнів, на кожному з яких реалізуються специфічні механізми захисту, що доповнюють один одного. На фізичному рівні забезпечується захист обладнання, сенсорів і виконавчих пристроїв від несанкціонованого доступу, пошкоджень або саботажу. На мережевому рівні реалізуються засоби безпечної передачі даних, шифрування, контроль доступу та захист від зовнішніх атак, таких як злом або DoS-атаки. На програмному та кібернетичному рівні застосовуються механізми аутентифікації, авторизації, моніторингу цілісності програмного забезпечення та протидії шкідливим програмам. Крім того, важливим є організаційний рівень, який передбачає політики безпеки, процедури реагування на інциденти та регулярний аудит стану безпеки системи.

Використання багаторівневої моделі забезпечує системний захист, оскільки помилка або уразливість на одному рівні компенсується заходами безпеки на інших рівнях. Для кіберфізичних систем, де цифрові процеси безпосередньо впливають на фізичні об’єкти, багаторівневий підхід є критично важливим, адже навіть незначна

вразливість може призвести до технічних збоїв, фінансових втрат або погіршення якості надання послуг. У контексті готельно-ресторанного бізнесу це означає, що безпека повинна охоплювати і систему бронювання, і платіжні сервіси, і «розумні» замки, і моніторинг безпеки приміщень, щоб гарантувати безперебійне та надійне обслуговування клієнтів.

Багаторівнева система безпеки також передбачає постійний моніторинг і адаптацію заходів, оскільки кіберзагрози постійно змінюються, а системи модернізуються і розширюються. Такий підхід дозволяє виявляти потенційні уразливості на ранніх етапах, оперативно реагувати на інциденти і підтримувати високий рівень захищеності протягом життєвого циклу кіберфізичної системи.

Багаторівнева система безпеки усіх описаних елементів в готельно-ресторанному бізнесі передбачає комплексну організацію захисту цифрових і фізичних компонентів закладу, що взаємопов’язані через кіберфізичні системи. Вона спрямована на забезпечення безпеки клієнтів, персоналу та конфіденційної інформації, а також на підтримку стабільності роботи всіх сервісів. На фізичному рівні заходи безпеки включають контроль доступу до приміщень, охоронні системи, відеоспостереження, а також захист від фізичного пошкодження обладнання, серверів чи терміналів оплати.

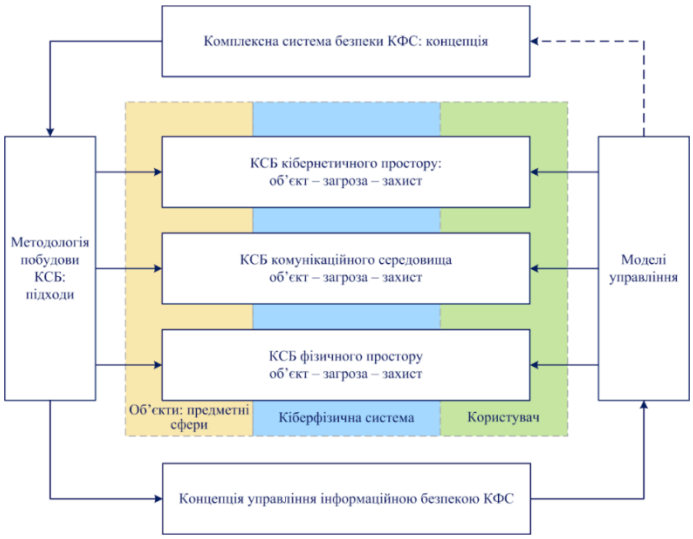

Рис. 4. Багаторівнева система безпеки КФС

На мережевому рівні реалізується безпечна передача даних між серверами, точками продажу та мобільними пристроями, застосовуються шифрування, системи аутентифікації та моніторинг трафіку для виявлення аномалій або спроб несанкціонованого доступу. Програмний рівень охоплює захист програмного забезпечення бронювання, POS-систем, CRM-систем і мобільних додатків закладу від шкідливого ПЗ, збоїв та несанкціонованих змін.

Організаційний рівень передбачає розробку політик інформаційної безпеки, навчання персоналу, контроль виконання процедур та реагування на інциденти. Важливим елементом є регулярний аудит безпеки, оцінка ризиків і впровадження превентивних заходів, що дозволяють зменшити ймовірність негативного впливу кібератак на обслуговування клієнтів.

У сукупності багаторівнева система безпеки забезпечує безперебійність та надійність роботи всіх сервісів закладу, включаючи електронні замки, системи бронювання, оплату послуг і автоматизацію внутрішніх процесів. Вона дозволяє не

лише захищати дані та обладнання, а й безпосередньо впливати на якість обслуговування клієнтів, підвищуючи рівень довіри та задоволення від наданих послуг.

В таблиці 2 показано деякі пропозиції, щодо покращення стану інформаційної безпеки складових КФС готельно-ресторанного бізнесу.

Таблиця 2

Рекомендації, щодо покращення стану інформаційної безпеки складових КФС готельно-ресторанного бізнесу

Складова КФС	Основні ризики інформаційної безпеки	Рекомендовані заходи з підвищення безпеки	Очікуваний вплив на якість послуг
Системи бронювання	Витік персональних даних, збої в роботі системи, DDoS-атаки	Використання захищених серверів і резервного копіювання; шифрування даних клієнтів; багатофакторна автентифікація; регулярне оновлення ПЗ	Стабільність процесів бронювання, зменшення помилок, підвищення довіри клієнтів
Електронні замки	Несанкціонований доступ, підробка цифрових ключів, збої синхронізації	Централізоване управління доступом; регулярна зміна ключів; використання захищених протоколів зв'язку; аудит доступів персоналу	Підвищення рівня фізичної безпеки, відчуття захищеності та комфорту гостей
POS-системи	Компрометація платіжних даних, фінансові втрати, простої в роботі	Сертифіковані платіжні рішення; сегментація мережі; контроль доступу до адміністративних функцій; навчання персоналу	Швидке та надійне обслуговування, зменшення черг і фінансових ризиків
Системи відеоспостереження	Несанкціонований доступ до відео, витік даних, порушення конфіденційності	Обмеження доступу до архівів; шифрування відеопотоків; журналювання доступів; регулярний аудит політик конфіденційності	Підвищення рівня безпеки та довіри клієнтів, зниження інцидентів
IoT-системи (клімат, освітлення, "розумні" номери)	Злом пристроїв, несанкціоноване керування, нестабільність роботи	Ізоляція IoT-мережі; регулярні оновлення прошивок; моніторинг аномальної активності; контроль підключених пристроїв	Стабільний комфорт перебування, персоналізований сервіс, оптимізація ресурсів

Запропонована модель рекомендацій щодо підвищення рівня інформаційної безпеки складових кіберфізичних систем готельно-ресторанного бізнесу ґрунтується на поєднанні технічних, організаційних та управлінських заходів і орієнтована на безпосереднє покращення якості надання послуг. Для систем бронювання ключовими напрямами підвищення безпеки визначено використання захищених серверних рішень, резервне копіювання даних, шифрування персональної інформації клієнтів і впровадження багатофакторної автентифікації. Реалізація таких заходів дозволяє мінімізувати ризики збоїв, втрати даних і несанкціонованого доступу, що забезпечує стабільність процесів бронювання та підвищує рівень довіри клієнтів до закладу.

Для електронних замків першочерговими є рекомендації щодо централізованого управління доступом, регулярної зміни цифрових ключів і використання захищених протоколів зв'язку. Додатково наголошується на необхідності періодичного аудиту прав доступу персоналу. Виконання цих рекомендацій сприяє зниженню ризику несанкціонованого проникнення, підвищує рівень фізичної безпеки та формує у гостей відчуття захищеності і комфорту під час перебування у готелі чи ресторані.

Підвищення інформаційної безпеки POS-систем передбачає застосування сертифікованих платіжних рішень, сегментацію мережевої інфраструктури, суворий

контроль доступу до адміністративних функцій та навчання персоналу основам кібербезпеки. Такі заходи спрямовані на захист платіжної інформації клієнтів і запобігання фінансовим втратам, що, у свою чергу, забезпечує швидке, надійне та безперебійне обслуговування і позитивно впливає на сприйняття якості сервісу.

У контексті систем відеоспостереження основна увага приділяється обмеженню доступу до відеоархівів, шифруванню відеопотоків, журналюванню дій користувачів і регулярному перегляду політик конфіденційності. Реалізація цих рекомендацій дозволяє забезпечити баланс між безпекою та дотриманням прав клієнтів на приватність, знижує ймовірність витоку даних і підвищує загальний рівень довіри до закладу.

Для IoT-систем, що забезпечують клімат-контроль, освітлення та функціонування «розумних» номерів, рекомендовано ізоляцію IoT-мережі від інших сегментів інфраструктури, регулярне оновлення прошивок, моніторинг аномальної активності та контроль підключених пристроїв. Застосування цих заходів забезпечує стабільну роботу систем автоматизації, підтримку комфортних умов перебування гостей і зменшення ризиків негативного впливу кіберінцидентів на якість надання послуг.

Загалом запропонована модель рекомендацій демонструє, що підвищення рівня інформаційної безпеки кожної складової кіберфізичної системи має прямий і опосередкований вплив на якість послуг у готельно-ресторанному бізнесі. Комплексна реалізація запропонованих заходів сприяє забезпеченню стабільності сервісних процесів, зростанню довіри клієнтів і підвищенню конкурентоспроможності підприємств індустрії гостинності.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження встановлено, що кіберфізичні системи є невід’ємною складовою сучасних об’єктів готельно-ресторанного бізнесу та відіграють ключову роль у забезпеченні безперервності операційних процесів і високого рівня сервісу. Їх активне впровадження дозволяє автоматизувати бронювання, контроль доступу, фінансові операції, управління інженерними системами та взаємодію з клієнтами. Водночас зростання рівня цифровізації зумовлює підвищення вразливості таких систем до кіберзагроз, що робить питання інформаційної безпеки критично важливим для стабільної діяльності підприємств галузі.

Аналіз складових кіберфізичних систем готельно-ресторанного бізнесу показав, що кожен елемент – від систем бронювання та POS-рішень до електронних замків, відеоспостереження й IoT-інфраструктури – має власний спектр загроз і потенційних ризиків. Порушення інформаційної безпеки цих компонентів безпосередньо впливає на якість надання послуг, проявляючись у вигляді збоїв у роботі сервісів, втрати довіри клієнтів, фінансових збитків, витоку персональних даних і погіршення репутації закладів.

Побудована модель загроз та розроблені рекомендації щодо підвищення рівня інформаційної безпеки засвідчили доцільність застосування багаторівневого підходу до захисту кіберфізичних систем. Такий підхід передбачає поєднання технічних, організаційних і програмних заходів безпеки, регулярний моніторинг стану систем, навчання персоналу та впровадження сучасних засобів кіберзахисту. Реалізація запропонованих рекомендацій сприяє зменшенню ризиків кіберінцидентів і підвищенню стійкості бізнес-процесів.

Отже, інформаційна безпека кіберфізичних систем виступає одним із визначальних чинників якості послуг у готельно-ресторанному бізнесі. Забезпечення належного рівня захисту цифрової інфраструктури дозволяє не лише запобігати загрозам, а й формувати позитивний клієнтський досвід, підвищувати конкурентоспроможність закладів та забезпечувати їх сталий розвиток в умовах цифрової трансформації.

Перспективи подальших досліджень полягають у розробленні та апробації кількісних методів оцінювання рівня інформаційної безпеки кіберфізичних систем об’єктів готельно-ресторанного бізнесу, а також у дослідженні впливу конкретних кіберінцидентів на показники якості обслуговування та задоволеності клієнтів. Окрему увагу доцільно приділити використанню штучного інтелекту та машинного навчання для прогнозування загроз і автоматизованого реагування на інциденти, а також аналізу відповідності систем безпеки вимогам міжнародних стандартів і нормативних актів у сфері захисту інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. POS-система від А до Я: що вміє та чим корисна? (n.d.). *CHM-S*. Retrieved January 25, 2026, from https://chm-s.com/pos-sistema-ot-do-ya-chto-umeet-i-chem-polezna
2. Кицюк, В. М., & Пупинін, О. С. (2024). Інформаційна безпека підприємства: теоретичний аспект. *Сучасний захист інформації*, (2), 103–108.
3. Cyber-physical systems. (n.d.). *University of California, Berkeley*. Retrieved January 25, 2026, from https://ptolemy.berkeley.edu/projects/cps/Cyber-Physical_Systems.html
4. Мельник, А. О. (2014). Кіберфізичні системи: проблеми створення та напрями розвитку. *Вісник Національного університету «Львівська політехніка». Комп’ютерні системи та мережі*, (806), 154–161.
5. Панасенко, Н. Л., Калашник, О. В., & Тищенко, О. В. (n.d.). Цифрова трансформація готельно-ресторанного бізнесу: роль інформаційних систем у формуванні сучасного сервісу. *Modern Engineering and Innovative Technologies*, 187–201.
6. Полотай, О. І. (2024). Особливості захисту приміщення з використанням обладнання TP-LINK TAPO. In *Сучасні комп’ютерні та інформаційні системи і технології: матеріали IV Всеукраїнської науково-практичної інтернет-конференції* (pp. 139–142). ТДАТУ.
7. Полотай, О. І., Пиріг, Ю., & Вітик, Д. (2025). Технічний захист приміщення за допомогою пристроїв розумного будинку. In *Proceedings of the 3rd International Scientific and Practical Conference “Global Trends in the Development of Information Technology and Science”* (pp. 117–121).
8. Полотай, О. І., & Полотай, Б. Я. (2017). Актуальність захисту інформації підприємств туристичної галузі. In *Автоматизація та комп’ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку* (pp. 56–58). ЧНУ ім. Богдана Хмельницького.
9. Система бронювання готелів – сучасний вид заробітку. (n.d.). *Canis Club*. Retrieved January 25, 2026, from https://canis-club.kharkov.ua/sistema-bronyuvannya-goteliv-suchasnij-vid-zarobitku/amp/
10. Сусіденко, В., & Сусіденко, О. (n.d.). Комплексне забезпечення інформаційної безпеки як передумова інноваційного розвитку готельно-ресторанного бізнесу. *Економіка та суспільство*, (74). Retrieved January 25, 2026, from https://economyandsociety.in.ua/index.php/journal/issue/view/74
11. Сучасні інформаційні системи в готельно-ресторанному бізнесі. (n.d.). *Zenodo*. Retrieved January 25, 2026, from https://zenodo.org/records/15306137
12. Що таке Інтернет речей? (n.d.). *GATE*. Retrieved January 25, 2026, from https://www.gate.com/uk/learn/articles/what-is-the-internet-of-things/179

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Orest Polotai
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID: 0000-0003-4593-8601
orest.polotaj@gmail.com

Natalia Kukharska
Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-0896-8361
kukharska.n@gmail.com

Bohdana Polotai
Senior Lecturer, Department of Tourism and Hotel and Restaurant Management
Lviv University of Trade and Economics, Lviv, Ukraine
ORCID: 0000-0003-1600-2724
bogdanaf@ukr.net

Yulia Vityk
3th year higher education student, group KB-31, Department of Information Security Management
University of Life Safety, Lviv, Ukraine
ORCID: 0009-0004-6782-866X
pyrih.ulia2018@gmail.com

INFORMATION SECURITY OF CYBER-PHYSICAL SYSTEMS AS A FACTOR OF SERVICE QUALITY IN THE HOTEL AND RESTAURANT BUSINESS

Abstract. The article examines the role of information security of cyber-physical systems in ensuring the quality of service provision by hotel and restaurant business facilities in the context of digital transformation. It is substantiated that modern hospitality industry enterprises actively use cyber-physical systems, in particular online booking systems, electronic locks, POS systems, video surveillance systems and IoT solutions to manage engineering infrastructure and services of "smart" rooms. Such systems combine software, hardware and network components, which leads to an increase in cyber risks and the need for a comprehensive approach to information security. The paper analyzes theoretical approaches to defining cyber-physical systems and a multi-level model of their protection. A detailed threat model for the main components of the cyber-physical infrastructure of the hotel and restaurant business is built, which includes technical, organizational and human factors. It was found that violations of confidentiality, integrity or availability of information directly affect the quality of service, the level of customer satisfaction, the safety of guests and staff, as well as the financial stability and reputation of establishments. Particular attention was paid to the analysis of the relationship between the state of information security of individual components of cyber-physical systems and indicators of the quality of service provision. It was shown that an insufficient level of protection of reservation systems and POS infrastructure leads to failures in service processes and loss of customer trust, while vulnerabilities of electronic locks, video surveillance and IoT systems create threats to the physical safety and comfort of guests. Based on the analysis, a model-recommendations were formed to increase the level of information security of cyber-physical systems, which involves the implementation of multi-level protection mechanisms, regular security audits and increasing cyber awareness of staff. The results obtained can be used by managers and IT specialists of hotel and restaurant businesses to improve information security management systems, as well as in further scientific research aimed at quantitatively assessing the impact of cybersecurity on service quality.

Keywords: cyber-physical systems, information security, cyber threats, multi-layered protection, hotel and restaurant business, service quality, digitalization, IoT.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. POS system from A to Z: What it can do and why it is useful. (n.d.). *CHM-S*. Retrieved January 25, 2026, from https://chm-s.com/pos-sistema-ot-do-ya-chto-umeet-i-chem-polezna
2. Kitsiuk, V. M., & Pupynin, O. S. (2024). Information security of an enterprise: Theoretical aspect. *Modern Information Security*, (2), 103–108.
3. Cyber-physical systems. (n.d.). *University of California, Berkeley*. Retrieved January 25, 2026, from https://ptolemy.berkeley.edu/projects/cps/Cyber-Physical_Systems.html
4. Melnyk, A. O. (2014). Cyber-physical systems: Challenges of creation and directions of development. *Bulletin of Lviv Polytechnic National University: Computer Systems and Networks*, (806), 154–161.
5. Panasenko, N. L., Kalashnyk, O. V., & Tyshchenko, O. V. (n.d.). Digital transformation of the hotel and restaurant business: The role of information systems in shaping modern service. *Modern Engineering and Innovative Technologies*, 187–201.
6. Polotai, O. I. (2024). Features of room protection using TP-LINK TAPO equipment. In *Modern computer and information systems and technologies: Proceedings of the 4th All-Ukrainian scientific and practical Internet conference* (pp. 139–142). TDATU.
7. Polotai, O. I., Pyrih, Y., & Vityk, D. (2025). Technical protection of premises using smart home devices. In *Proceedings of the 3rd International Scientific and Practical Conference "Global Trends in the Development of Information Technology and Science"* (pp. 117–121).
8. Polotai, O. I., & Polotai, B. Y. (2017). The relevance of information protection for enterprises in the tourism industry. In *Automation and computer-integrated technologies in production and education: State, achievements, and prospects of development* (pp. 56–58). Bohdan Khmelnytsky National University of Cherkasy.
9. Hotel booking systems: A modern source of income. (n.d.). *Canis Club*. Retrieved January 25, 2026, from https://canis-club.kharkov.ua/sistema-bronyuvannya-goteliv-suchasnij-vid-zarobitku/amp/
10. Susidenko, V., & Susidenko, O. (n.d.). Comprehensive information security as a prerequisite for innovative development of the hotel and restaurant business. *Economy and Society*, (74). Retrieved January 25, 2026, from https://economyandsociety.in.ua/index.php/journal/issue/view/74
11. Modern information systems in the hotel and restaurant business. (n.d.). *Zenodo*. Retrieved January 25, 2026, from https://zenodo.org/records/15306137
12. What is the internet of things? (n.d.). *GATE*. Retrieved January 25, 2026, from https://www.gate.com/uk/learn/articles/what-is-the-internet-of-things/179

Отримано редакцією журналу / Received: 15.01.26
Прорецензовано / Revised: 30.01.26
Схвалено до друку / Accepted: 26.03.26