

ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Кафедра готельно-ресторанного бізнесу

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Інформаційно-комунікаційні технології суб'єкта готельного бізнесу

Студента 3 курсу, 10с групи
спеціальності

241 «Готельно-ресторанна справа»
освітньої програми
«Готельно-ресторанна справа»

Науковий керівник
к.е.н., доц.

Гарант освітньої програми
к.е.н., доц.

Диреволкова
Марія
Вікторівна

Федоряк
Руслан
Михайлович

Расулова
Алла
Миколаївна

Київ 2023

ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ**Факультет** ресторанно-готельного та туристичного бізнесу**Кафедра** готельно-ресторанного бізнесу**Спеціальність** 241 «Готельно-ресторанна справа»**Спеціалізація** «Готельно-ресторанна справа»**ЗАТВЕРДЖУЮ**

Зав. кафедри
готельно-ресторанного бізнесу
проф. _____ М.Г. Бойко
« ____ » _____ 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу студентіві

Диреволкова Марія Вікторівна

(прізвище, ім'я, по батькові)

1. Тема випускної кваліфікаційної роботи: «Інформаційно-комунікаційні технології суб'єкта готельного бізнесу»

Затверджена наказом ректора від «30» вересня 2022 р. № 2417.

2. Строк здачі студентом закінченої роботи: 27 січня 2023 р.

3. Цільова установка та вихідні дані до роботи

Мета роботи розроблення та обґрунтування методичних та практичних засад впровадження інформаційно-комунікаційних технологій у закладі готельного бізнесу.

Об'єкт дослідження – інформаційно-комунікаційні технології та процеси підприємства готелю.

Предмет дослідження – методичні та практичні підходи до удосконалення інформаційно-комунікаційних технологій у ресторані ПРАТ «ПРЕЗИДЕНТ-ГОТЕЛЬ» міста Києва.



ЗМІСТ

ВСТУП.....	5
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ТА ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ.....	8
1.1. Сутність поняття, класифікація та історія розвитку підходів до використання інформаційно-комунікаційних технологій.....	8
1.2. Специфіка організації системи інформаційно-комунікаційних технологій на підприємстві готельного господарства.....	15
1.3. Закордонний досвід та тренди у сфері інформаційно-комунікаційних технологій.....	21
РОЗДІЛ 2. АНАЛІЗ СИСТЕМИ ТА РЕКОМЕНДАЦІЇ ЩОДО МОДЕРНІЗАЦІЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОГО КОМПЛЕКСУ ГОТЕЛЬНОГО ПІДПРИЄМСТВА «ПРЕЗИДЕНТ ГОТЕЛЬ».....	24
2.1. Загальна характеристика готельного підприємства «Президент Готель» та аналіз його господарської діяльності.....	24
2.2. Структурно-функціональна схема інформаційно-комунікаційних технологій «Президент Готель».....	26
2.3. Рекомендації по удосконаленню інформаційно-комунікаційного комплексу технологій підприємства «Президент Готель».....	33
ВИСНОВКИ.....	34
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	43
ДОДАТКИ.....	47

ВСТУП

Актуальність дослідження. У зв'язку зі зростанням інтересу до інформаційно-комунікаційних технологій (ІКТ) не лише представників комп'ютерної спільноти, а й широкої громадськості, стрімко зростає і кількість робіт, присвячених проблемам їх функціонування та подальшого розвитку.

Водночас глобальна економіка вільного та відкритого ринку переживає період незворотних трансформацій внаслідок формування абсолютно нового типу економічних і соціальних відносин. Усе це характеризується виробництвом знань, інтеграцією технологій та розвитком інформаційних децентралізованих мереж з розгалуженими та комплексними система контролю доступу. Використовуючи Інтернет як основу для створення ІКТ, організації можуть легко керувати великим обсягами даних всередині своєї структури без необхідності звертатися до спеціалістів.

Якісно налаштовані ІКТ забезпечують високий рівень організації, конфіденційність та безпеку, при цьому вони гарантують низьку вартість обслуговування, відсутність територіальних обмежень та можливість роботи у режимі реального часу. В результаті ці системи отримують все більшого поширення, зокрема серед готельних підприємств.

Однак, проблеми розвитку ІКТ, пов'язані з надмірною централізацією, зумовлюють необхідність трансформації наявних моделей та практик. В цьому контексті, актуальним стає дослідження ІКТ, їх класифікацій, проблем функціонування та потенціалу до розвитку як методу забезпечення функціонування організацій, зокрема готельних підприємств.

Мета дослідження – здійснити фундаментальний аналіз сучасного стану та особливостей розвитку ІКТ у контексті підприємства готельного господарства. Висвітлити основні форми та механізми роботи подібних

систем та визначити перспективні орієнтири вдосконалення та розвитку у майбутньому.

Для досягнення поставленої мети необхідно вирішити наступні **завдання:**

- встановити сутність поняття «інформаційно-комунікаційні технології» і визначити етапи становлення та класифікацію;
- висвітлити специфіку організації системи контролю управління доступом у готельній сфері;
- проаналізувати основні тренди у сфері використання ІКТ;
- надати характеристику господарської діяльності «Президент Готель»;
- дослідити систему ІКТ готельного підприємства «Президент Готель»;
- виокремити шляхи модернізації чинної ІКТ «Президент Готель».

Об'єктом дослідження є розвиток інформаційно-комунікаційних технологій суб'єктами готельного бізнесу.

Предметом дослідження є особливості, масштаби та механізми функціонування ІКТ «Президент Готелю».

Методи дослідження. Для досягнення поставлених цілей дослідження використовувалися різноманітні загальнонаукові та спеціалізовані методи, що забезпечують концептуальну єдність дослідження. До цих методів відносяться: наукова абстракція, яка підкреслює найбільш істотні особливості розвитку ІКТ; аналіз, який висвітлює переваги та недоліки різних підходів до використання ІКТ; історико-логічний метод, який описує виникнення, становлення та розвиток підходів до організації ІКТ та метод формалізації, який окреслює шляхи модернізації існуючих підходів та систем ІКТ).

Інформаційну та фактологічну основу дослідження було отримано з різноманітних джерел, у тому числі спеціальної літератури: монографій та навчальних посібників. Крім того, були використані публікації у

вітчизняних та зарубіжних журналах, що містять елементи економічних, інформаційних та соціологічних спостережень, а також комп'ютерні опитування спеціалізованих компаній, готелів та національних туристичних комісій.

Питання розробки систем контролю доступу широко досліджувалися зарубіжними фахівцями, такими як та ін. Їхні роботи стали цінним ресурсом для поточного дослідження і допомогли поглибити розуміння предмета.

Наукова новизна отриманих результатів полягає в комплексному дослідженні функціонування ІКТ готелю «Президент Готель» та супутніх процесів. У цьому дослідженні не тільки оцінюються загальні особливості ІКТ, такі як використання хмарних технологій для збереження даних, а й спеціалізовані технічні функції та характеристики різних елементів ІКТ, які складають систему.

Практичне значення одержаних результатів дослідження. Дослідження забезпечує теоретичну основу для розуміння тонкощів розробки ІКТ суб'єктів готельного підприємства. Результати цього дослідження можуть слугувати основою для формулювання стратегій розвитку, які враховують найкращі міжнародні практики, особливо зосереджуючись на інтеграції механізмів контролю та перевірки осіб у існуючі моделі управління доступом готельних підприємств.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ТА ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

1.1. Сутність поняття, класифікація та історія розвитку підходів до використання інформаційно-комунікаційних технологій

Сьогодні всі організації покладаються на системи баз даних як ключову технологію керування даними для широкого спектра завдань, починаючи від повсякденних операцій і закінчуючи прийняттям критичних рішень. Швидке поширення вебдодатків та інформаційних систем, а також останні тенденції, такі як хмарні обчислення та зовнішнє керування даними, ще більше збільшили доступність систем баз даних, тому питання їх використання та значення для бізнесу стало надзвичайно важливим.

Д'яченко у своїх дослідженнях зазначив, що інформаційно-комунікаційні технології використовуються у різноманітних сферах життєдіяльності людини, починаючи від урядових і військових, і закінчуючи громадськими та комерційними організаціями [2].

Інформаційно-комунікаційні технології (ІКТ) стали невід'ємною частиною сучасного суспільства, впливаючи на різні аспекти людського життя, включаючи освіту, бізнес і політику. Концепція ІКТ охоплює широкий спектр технологій, включаючи комп'ютери, Інтернет і мобільні пристрої.

Суть концепції ІКТ можна визначити як використання технологій для обробки, зберігання та передачі інформації (Turban et al., 2018). Це включає використання комп'ютерів, Інтернету та мобільних пристроїв для спілкування, доступу до інформації та виконання різноманітних завдань. Інше визначення ІКТ – це використання цифрових технологій для передачі, створення та поширення інформації (Warschauer & Matuchniak, 2010).

Директива 2002/21/ЄС Європейського Парламенту та Ради від 7 березня 2002 року про загальну нормативну базу для електронних

комунікаційних мереж і послуг (Рамкова Директива) визначила ІКТ як будь-яке обладнання, систему або підсистему обладнання, яке використовується для генерування, надсилання, отримання або зберігання знаків, сигналів, записів, зображень, звуків, даних або розвідувальних даних будь-якого характеру [16].

ООН у рамках A/RES/70/1.ООН теж надала визначення ІКТ, яке можна описати як набір технічних засобів та інструментів, які використовуються для обробки, зберігання, передачі та захисту інформації [20].

Крім того, ІКТ можна визначити як набір технологічних інструментів і ресурсів, які використовуються для спілкування, створення, розповсюдження, зберігання та управління інформацією. Саме цим визначенням користується Міжнародний союз електрозв'язку з 2017 року [13].

Важливо відзначити, що ІКТ стали необхідним інструментом для ефективного функціонування окремих осіб, організацій та урядів у сучасному цифровому світі.

ІКТ можна класифікувати за кількома категоріями, як показано в таблиці 1.1.

Таблиця 1.1

Класифікація ІКТ

Категорія	Пояснення
Апаратне забезпечення	Фізичні компоненти ІКТ, такі як комп'ютери та мобільні пристрої
Програмне забезпечення	Програми та програми, які працюють на апаратних пристроях
Послуги	Різноманітні способи використання ІКТ, наприклад онлайн-банкінг або телемедицина

Джерело: складено автором за даними [3].

Історію розвитку підходів до використання ІКТ можна простежити до винаходу телеграфу в 1830-х роках Семюелем Морзе та подальшої розробки телефону Олександром Гремом Беллом у 1876 році та радіо Гульєльмо Марконі в 1895 році. Таблиця 1.2 ілюструє деякі ключові віхи в історії ІКТ.

Таблиця 1.2

Основні події в історії розвитку ІКТ

Рік	Подія
1830	Семюел Морзе винайшов телеграф
1876	Винахід телефону Олександр Грем Белл
1895	Гульєльмо Марконі винайшов радіо
1945	Винахід електронного комп'ютера Джоном Атанасовим і Кліффордом Беррі
1969	Створення мережі ARPANET

Джерело: складено автором за [3].

Винахід комп'ютера в середині 20 століття ознаменував значну зміну способів обробки та зберігання інформації. Розвиток Інтернету наприкінці 20-го століття зробив революцію в комунікації та доступі до інформації, дозволивши окремим особам і організаціям підключатися та обмінюватися інформацією по всьому світу.

В останні роки відбувся зсув у бік мобільних пристроїв як основного засобу доступу до ІКТ. Широке поширення смартфонів і планшетів призвело до збільшення використання мобільних додатків або «додатків» для виконання різноманітних завдань, таких як онлайн-магазини, соціальні мережі та банківська справа. Цю тенденцію називають «мобільною революцією» і вона значно вплинула на те, як люди взаємодіють з ІКТ [4]. Такі дослідники, як Ніколас Карр (2008), стверджують, що цей перехід до мобільних пристроїв призвів до збільшення використання ІКТ для розваг і соціальних цілей, а не для продуктивних завдань [9].

Дослідники також виділили три ключові вимоги, яким повинен відповідати інформаційно-технологічний комплекс будь-якої сучасної організації [9]:

- секретність або конфіденційність – захист даних від несанкціонованого розкриття;
- цілісність – запобігання неналежним модифікаціям даних;
- доступність – можливість доступу та відновлення даних після апаратних і програмних помилок, а також після зловмисних дій, які призводять до того, що система стає недоступною.

Ці три вимоги виникають практично в усіх сферах. Наприклад, розглянемо базу даних, що зберігає інформацію про гостей готелю. Важливо, щоб записи клієнтів не передавалися неавторизованим суб'єктам, щоб записи змінювали лише ті суб'єкти, які належним чином уповноважені, і була гарантована їх точність, а також щоб записи клієнтів були легкодоступними для відповідальних робітників готелю, особливо в екстрених ситуаціях.

Для цього система (або механізм) контролю доступу перевіряє, чи має суб'єкт авторизацію для виконання певного виду дій з даними. Авторизації надаються суб'єктам відповідно до політики контролю доступу організації. Конфіденційність може бути додатково посилена за допомогою методів шифрування, застосованих до даних, коли вони зберігаються у вторинному сховищі або передаються через мережу, або керуються третіми сторонами, як у випадку зовнішнього керування базами даних [12].

Цілісність спільно забезпечується механізмом контролю доступу та семантичними обмеженнями. Щоразу, коли суб'єкт намагається змінити деякі дані, механізм контролю доступу перевіряє, чи суб'єкт має право змінювати дані, а підсистема семантичної цілісності перевіряє, чи оновлені дані є правильними щодо набору семантичних умов, які називаються

обмеженнями цілісності. Крім того, щоб захистити дані від підробки під час передачі в мережі, дані можна підписати цифровим підписом. Водночас підсистема збереження та відновлення разом з механізмом керування паралелізмом гарантують, що дані є доступними та актуальними, попри апаратні та програмні збої та доступ до бази з різних пристроїв в один і той же час. Доступність даних, особливо для баз даних, які знаходяться в мережі Інтернет, може бути додатково посилена за допомогою використання методів захисту від атак типу «відмова в обслуговуванні» [10].

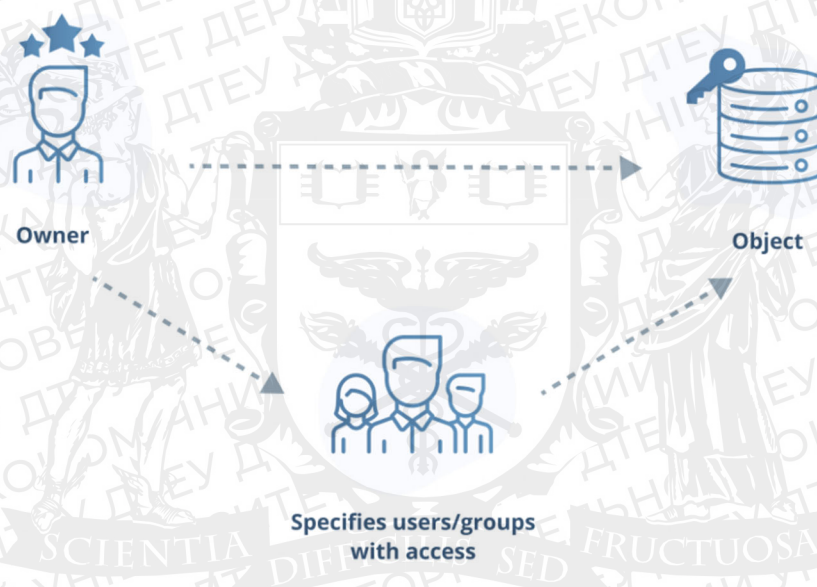


Рис. 1.1. Схема роботи політики дискреційного контролю доступу ІКТ

Джерело: [10].

Ранні дослідницькі пропозиції в області інформаційно-комунікаційних технологій були зосереджені на розробці двох різних класів моделей, заснованих на політиці дискреційного контролю доступу (DAC) і на політиці обов'язкового контролю доступу (MAC), відповідно. Політика дискреційного контролю доступу дозволяла суб'єктам-адміністраторам надавати авторизацію на дані іншим суб'єктам (рис. 1.1). На відміну від обов'язкової політики контролю доступу, яка регулює доступ суб'єктів до даних на основі попередньо визначених класифікацій суб'єктів і даних (рис. 1.2).

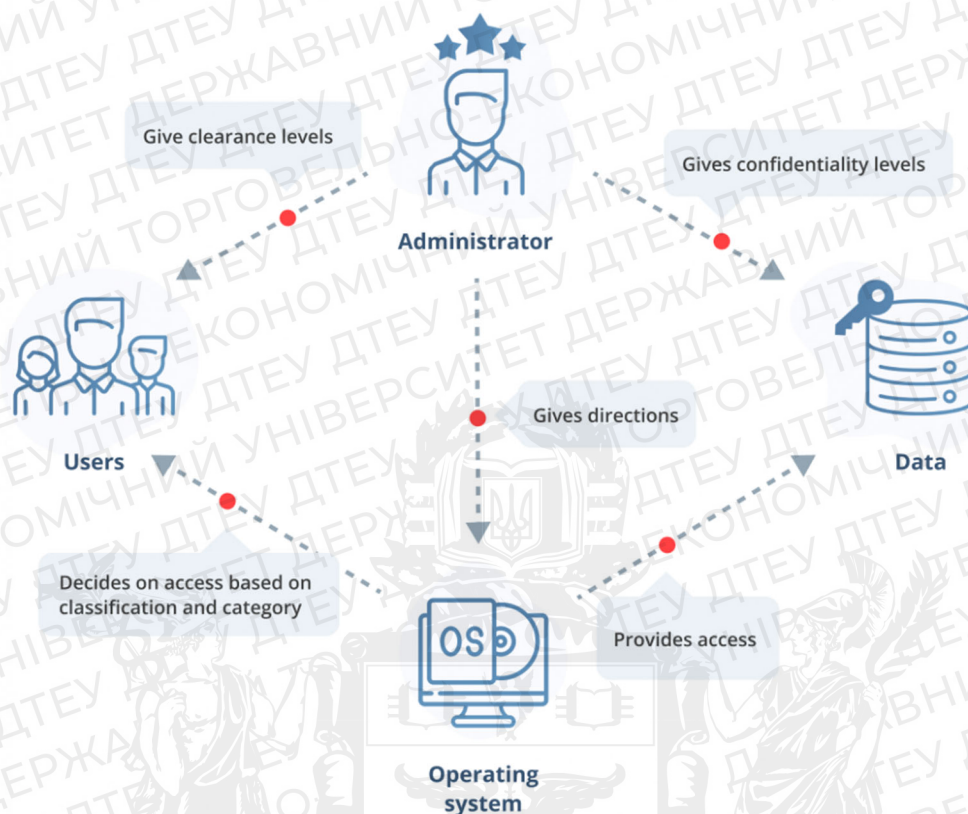


Рис. 1.2. Схема роботи політики обов'язкового контролю доступу ІКТ

Джерело: [10].

Відповідно до такої політики, навіть творець об'єкта даних не може на власний розсуд надавати авторизації доступу іншим суб'єктам.

Ці підходи до організації ІКТ були розширені внаслідок розробки передових систем керування даними та додатками, такими як цифрові бібліотеки та мультимедійні дані, складські системи та системи документообігу. Важливою вимогою для подальших ІКТ став захист не тільки даних, але і схеми бази даних, що містить конфіденційну інформацію. У цьому відношенні ІКТ почали потребувати власного захисту, оскільки вони можуть розкривати конфіденційну інформацію щодо підприємства.

Таким чином, сформувалась необхідність визначати політики контролю доступу для об'єктів, які не є даними користувача, а скоріше являють собою інші політики контролю доступу. Іншою важливою характеристикою сучасних інформаційно-комунікаційних технологій є те, що вони часто мають справу з мультимедійними даними, для яких

автоматична інтерпретація вмісту є набагато складнішою, і до них, у більшості випадків, доступ мають різноманітні користувачі, які знаходяться поза межами системи, наприклад через мережу Інтернет.

Однак важливо також зазначити, що використання ІКТ принесло численні переваги, такі як підвищення продуктивності та доступу до інформації, а також покращення спілкування та співпраці. Наприклад, використання ІКТ в освіті призвело до розвитку онлайн та дистанційного навчання, що зробило освіту більш доступною для людей у віддалених регіонах. Крім того, використання ІКТ у сфері охорони здоров'я призвело до розвитку телемедицини, яка дозволяє проводити дистанційну діагностику та лікування, покращуючи доступ до медичної допомоги для людей у сільській місцевості та районах із недостатнім обслуговуванням.

Крім того, використання ІКТ у бізнесі призвело до розвитку електронної комерції та створення глобальної економіки, що сприяло збільшенню торгівлі та транскордонної торгівлі. Водночас використання ІКТ у політиці призвело до розвитку електронного урядування, яке дозволяє підвищити прозорість і участь у політичному процесі.

Підсумовуючи, концепція ІКТ охоплює використання технологій для обробки, зберігання, захисту та передачі інформації. Їх можна класифікувати за категоріями обладнання, програмного забезпечення та послуг, а історію їх розвитку можна простежити до винаходу телеграфу та подальшого розвитку телефону, радіо, комп'ютера та Інтернету. Нещодавня тенденція до мобільних пристроїв значно вплинула на те, як люди взаємодіють з ІКТ, і такі дослідники, як Ніколас Карр, стверджують, що ця зміна призвела до збільшення використання ІКТ для розваг і соціальних цілей. Однак важливо також зазначити, що використання ІКТ принесло численні переваги, такі як підвищення продуктивності та доступу до інформації, а також покращення спілкування та співпраці. Усунення

цифрового розриву має вирішальне значення для того, щоб усі люди мали рівний доступ до можливостей і переваг, які надають ІКТ.

1.2. Специфіка організації системи інформаційно-комунікаційних технологій на підприємстві готельного господарства

Готелі стикаються зі специфічними проблемами, властивими тільки індустрії гостинності. Безпека гостей, персоналу та будь-кого, хто приходить до готелю, є життєво важливою для готельної індустрії, що робить системи контролю доступу в готелі цінним інструментом. Таким чином, готелі вимушені зробити все можливе, щоб не порушити приватність і комфорт гостей. При цьому готелі мають захищати як клієнтів, так і працівників.

У своєму дослідженні Родрігез стверджує, що однією з головних причин, чому туристи повертаються до певного готелю, є відчуття безпеки, яким вони там насолоджувалися. Крім того, на міжнародному рівні готелі можуть отримати додаткову сертифікацію внаслідок добре розвиненої та захищеної ІКТ, що тягне за собою вищий ступінь довіри з боку туристів і підвищує привабливість місця для подієвого туризму.

Хоча сьогодні ІКТ відіграють центральну роль у сфері готельного бізнесу, за останні 20 років найбільші готельні мережі зазвичай використовують доволі специфічні розширення цієї технології. Ці розширення були зумовлені, з одного боку, потребою в управлінні складними мультимедійними об'єктами, а з іншого – широким використанням Інтернету та вебдодатків, які сприяли розвитку підходів до взаємодії, таких як XML та вебсервіси, а також стало можливим обмінюватися даними між різними доменами адміністрування.

Основною вимогою, що лежить в основі всіх цих готельних (або якщо точніше туристичних) розширених систем і інструментів керування даними, є потреба в належній безпеці та, зокрема, в індивідуальних моделях і системах контролю доступу.

Відповідні функції, які повинна забезпечувати ІКТ готельних підприємств включають:

- гнучкі моделі авторизації;
- гнучкі механізми специфікації;
- адаптація до стратегій розповсюдження даних і архітектур сторонніх публікацій.

Гнучкі моделі авторизації використовують для складних мультимедійних об'єктів. Наприклад, більшість просунутих ІКТ характеризуються об'єктами, структура яких значно складніша, ніж типова для реляційних даних. Це стосується, наприклад, даних XML і мультимедійних даних. Оскільки додатки можуть безпосередньо отримувати доступ до даних клієнтів та готельного підприємства на різних рівнях деталізації від наборів об'єктів даних до певних частин одного об'єкта даних, необхідні механізми для контролю доступу на різних рівнях деталізації та для підтримки обмеженої в часі авторизації. Розширення, запропоновані для вирішення таких вимог, включають поняття позитивних/негативних авторизацій та неявних/явних авторизацій.

Враховуючи, що для більшості готелів характерна популяція клієнтів, яка є набагато більш неоднорідною та динамічною, ніж популяція користувачів, типова для звичайних інформаційних систем, традиційні механізми ідентифікації, засновані на логіні або іменах користувачів, для визначення суб'єктів системи більше не підходять, оскільки вони вимагатимуть специфікації та керування великою кількістю політик. Таким чином, існує необхідність використання інших властивостей суб'єктів (наприклад, віку, національності, посади), крім їхніх імен для входу, у системи готельних підприємств. Такі властивості, які можна вважати формою часткової цифрової ідентифікації, часто кодуються в профілях користувачів і сертифікуються за допомогою облікових даних і

сертифікатів атрибутів. Хоча варто зазначити, що готелі зазвичай використовують більш узагальнені механізми, які ефективно підтримують використання кількох властивостей цифрової ідентифікації в політиках контролю доступу.

Важливою вимогою до сучасних готельних ІКТ, зокрема вебдодатків є підтримка різноманітних стратегій розповсюдження даних. Стратегія розповсюдження регулює, як джерело даних передає дані суб'єктам. У звичайних системах баз даних дані доставляються відповідно до стратегії, відомої як стратегія вилучення. Відповідно до такої стратегії дані доставляють суб'єктам за явним запитом суб'єктів. Однак у готельних підприємствах часто використовують альтернативну стратегію, яка є більш придатною, коли дані потрібно доставити великій спільноті суб'єктів. Відповідно до такої стратегії, яка називається стратегією прощтовхування або публікації-підписки, джерело даних періодично (або коли відбуваються певні заздалегідь визначені події) надсилає дані авторизованим суб'єктам без необхідності явного запиту на доступ з боку суб'єктів. У деяких випадках дані, які надсилаються суб'єктам, також залежать від конкретних інтересів суб'єктів, які записуються в деяких спеціальних профілях суб'єктів, якими керує джерело даних. Підтримка різних стратегій розповсюдження може вимагати застосування різних методів контролю доступу залежно від прийнятої стратегії розповсюдження даних. Таким чином, комплексна система контролю доступу повинна забезпечувати велику різноманітність методів контролю доступу, здатних забезпечити дотримання певної політики за допомогою різноманітних стратегій розповсюдження.

При цьому під час проектування ІКТ для готельного господарства існує певний ряд функцій та вимог, які потрібно задовольнити. Наприклад, при роботі зі складними об'єктами можна дозволити доступ до цілих об'єктів або лише до їх частин.

Модель ІКТ готельного підприємства також повинна мати поняття негативної авторизації. Основною метою цього типу авторизації є підтримка винятків. Наприклад, припустимо, що робітник готелю має бути авторизований для доступу до певної групи документів з виключенням одного екземпляру. Відповідно, готелю потрібно ввести лише дві авторизації: позитивну авторизацію для класу (групи документів), яка автоматично поширюватиметься на всі екземпляри, і негативну авторизацію для екземпляра, який потрібно виключити. Крім того, винятки можуть виникати на різних рівнях ієрархічної організації об'єкта захисту, таким чином, винятки можуть мати власні винятки.

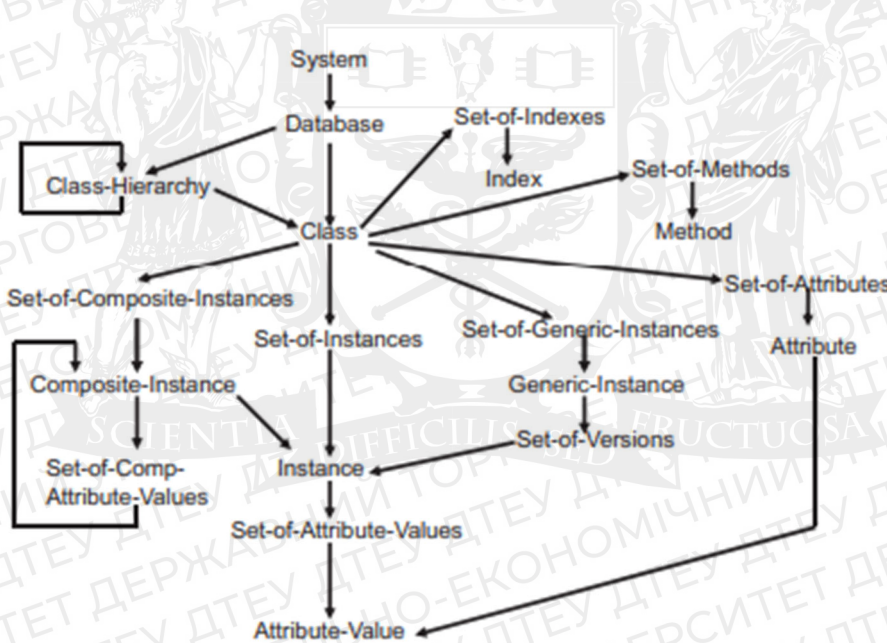


Рис. 1.3. Схема об'єкта авторизації для систем контролю доступу готельних підприємств

Джерело: [18].

Іншою цікавою особливістю організації ІКТ у готельних підприємствах є поняття схеми об'єкта авторизації (АОС). Така схема, змодельована як граф, представляє всі одиниці гранулярності захисту бази даних, змодельовані як вузли, і структурні зв'язки між цими типами гранул, змодельовані як ребра. На рисунку 1.3 представлено АОС для типового

готельного підприємства, яке включає всі конструкції семантичного моделювання об'єктної моделі, такі як складені об'єкти та версії, а також інші захищені об'єкти, такі як індекси. Таким чином, AOS визначає, як авторизації одного об'єкта поширюються на авторизації об'єктів, семантично пов'язаних з ним. Проте розповсюдження авторизації відповідно до AOS залежить від типу режиму доступу та від того, чи є авторизація негативною, чи позитивною.

Таким чином, розвиток інформаційно-комунікаційних технологій (ІКТ) значно вплинув на готельну індустрію. Впровадження ІКТ у готельній індустрії призвело до покращень у різних сферах, включаючи зовнішні операції, внутрішні операції та обслуговування гостей.

Однією з основних практичних сфер, де ІКТ мали значний вплив на готельну індустрію, є зовнішні операції. Це включає використання комп'ютеризованих систем для бронювання та керування бронюванням, таких як системи управління майном (PMS) і центральні системи бронювання (CRS). Ці системи дозволяють отримувати оновлення в реальному часі та точно відстежувати бронювання та наявність номерів, підвищуючи ефективність і знижуючи ризик надмірного бронювання. Крім того, використання платформ онлайн-бронювання, таких як Booking.com і Expedia, значно збільшило охоплення та доступність бронювання готелів для клієнтів.

Іншою сферою, де ІКТ мали значний вплив на готельну індустрію, є серверні операції. Це включає використання систем для управління запасами та закупівлями, управління заробітною платою та бухгалтерським обліком, а також управління взаємовідносинами з клієнтами (CRM). Ці системи дозволяють покращити відстеження та управління запасами, фінансовими даними та інформацією про клієнтів. Використання цих систем може підвищити ефективність, зменшити витрати та забезпечити краще розуміння потреб клієнтів.

На обслуговування гостей також значно впливає впровадження ІКТ у готельній індустрії. Це включає використання систем для реєстрації заїзду та виїзду, управління номерами та зручності в номері, такі як розваги в номері та доступ до Інтернету. Ці системи дозволяють автоматизувати процеси реєстрації заїзду та виїзду, зменшуючи потребу в ручних процесах і підвищуючи ефективність. Крім того, використання мобільних додатків і онлайн-порталів для доступу гостей до готельних послуг і зручностей, таких як обслуговування номерів і запити на прибирання, значно підвищило якість і доступність готельних послуг для гостей.

Підводячи підсумки, одним із ключових аспектів організації системи ІКТ в готельному господарстві є інтеграція різних систем і технологій. Це включає в себе інтеграцію зовнішніх і внутрішніх систем, а також інтеграцію різних технологій для гостей, таких як мобільні додатки та зручності в номерах. Ця інтеграція забезпечує безперебійне спілкування та обмін даними між різними системами та покращує загальний досвід гостей.

Іншим важливим аспектом організації системи ІКТ в готельній індустрії є впровадження заходів безпеки для захисту конфіденційної інформації, такої як особисті та фінансові дані гостей і співробітників. Це включає використання шифрування та брандмауерів для захисту від кіберзагроз, а також впровадження політик і процедур для забезпечення безпеки фізичних пристроїв і зберігання даних.

Саме завдяки цим особливостям, впровадження ІКТ у готельній індустрії суттєво вплинуло на різні сфери діяльності, включаючи зовнішні, внутрішні та гостьові послуги.

1.3. Закордонний досвід та тренди у сфері інформаційно-комунікаційних технологій

Як вже було визначено раніше, інформаційно-комунікаційні технології (ІКТ) стали невід'ємною частиною сучасного суспільства,

впливаючи на різні аспекти людського життя, включаючи освіту, бізнес і політику. Сфера ІКТ постійно розвивається, тому будь-якій організації, зокрема готельному підприємству, важливо розуміти іноземний досвід і тенденції, щоб залишатися актуальними та конкурентоспроможними.

Однією з головних тенденцій у сфері ІКТ є збільшення використання технологій штучного інтелекту (AI) і машинного навчання (ML). У готельній індустрії цю тенденцію можна побачити у використанні чат-ботів для обслуговування клієнтів і реалізації прогнозової аналітики для управління доходами. Наприклад, Mandarin Oriental Hotel Group запровадила чат-боти на основі штучного інтелекту, які допомагають гостям бронювати номери та надають інформацію про готель та його послуги. Крім того, зараз багато готелів використовують прогнозу аналітику для прогнозування попиту та оптимізації стратегій ціноутворення, що сприяє покращенню управління доходами.

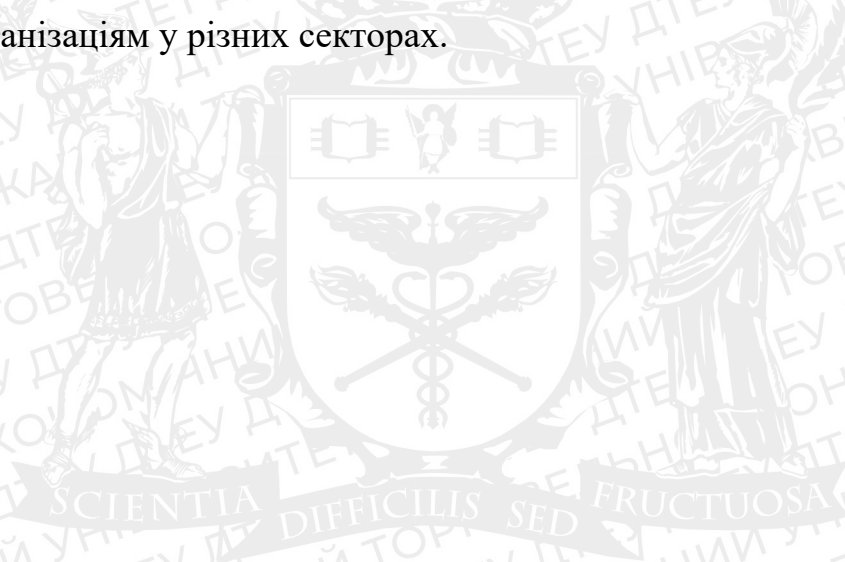
Ще однією тенденцією у сфері ІКТ є все більше використання технологій Інтернету речей (IoT). У готельній індустрії цю тенденцію можна побачити у використанні систем розумних номерів, таких як системи, які пропонують такі компанії, як Samsung і LG. Вони дозволяють гостям контролювати зручності в номері, наприклад освітлення та температуру, через мобільний додаток або кімнатний пристрій. Крім того, зараз багато готелів використовують технології IoT для підвищення енергоефективності та зниження витрат. Наприклад, InterContinental Hotels Group впровадила системи енергоменеджменту з підтримкою IoT у своїх готелях, забезпечивши економію електроенергії до 30% [16]. У транспортному секторі технології IoT використовуються для покращення транспортного потоку, зменшення викидів і підвищення громадської безпеки. Наприклад, місто Сінгапур впровадило інтелектуальні системи трафіку з підтримкою IoT, які використовують дані в реальному часі для оптимізації потоку трафіку та зменшення заторів. У виробничій промисловості технології IoT

використовуються для прогнозованого обслуговування, автоматизованого управління запасами та контролю якості. Наприклад, GE впровадила систему з підтримкою Інтернету речей для моніторингу продуктивності своїх вітряних турбін, що дозволяє завчасно виявляти потенційні проблеми та покращує загальну ефективність.

Технології віртуальної та доповненої реальності (VR/AR) також стають все більш популярними у сфері ІКТ. У готельній індустрії цю тенденцію можна побачити у використанні віртуальної реальності для віртуальних турів готельними номерами та об'єктами, а також у використанні доповненої реальності для покращених вражень у номері. Наприклад, мережа готелів Marriott запровадила технологію віртуальної реальності, щоб клієнти могли здійснювати віртуальні екскурсії номерами та зручностями готелю перед бронюванням. Це дозволяє клієнтам отримати краще уявлення про зручності та планування готелю, покращуючи процес бронювання. Крім того, деякі готелі зараз використовують технологію AR, щоб покращити враження від перебування в номері, наприклад, надати інтерактивну інформацію про визначні місця та ресторани поблизу.

Хмарні обчислення також є зростаючим трендом у сфері ІКТ. Ця технологія дозволяє зберігати та керувати даними та програмами на віддалених серверах, до яких можна отримати доступ через Інтернет. У готельній індустрії цю тенденцію можна побачити у використанні хмарних систем управління нерухомістю (PMS) і центральних систем бронювання (CRS). Ці системи дозволяють отримувати оновлення в реальному часі та точно відстежувати бронювання та наявність номерів, підвищуючи ефективність і знижуючи ризик надмірного бронювання. Крім того, зараз багато готелів використовують хмарні системи для управління запасами та закупівлями, управління заробітною платою та бухгалтерським обліком, а також управління взаємовідносинами з клієнтами (CRM).

Підсумовуючи, зарубіжний досвід і тенденції у сфері ІКТ постійно розвиваються, організаціям важливо залишатися актуальними та конкурентоспроможними. Готельна індустрія є одним із секторів, на який значно вплинув розвиток ІКТ із такими тенденціями, як використання штучного інтелекту та машинного навчання, Інтернету речей, VR/AR та хмарних обчислень. Ці технології дозволили вдосконалити різні сфери, і не лише в готельній індустрії, але й в інших секторах, таких як охорона здоров'я, роздрібна торгівля, транспорт, виробництво, освіта, розваги та фінанси. Розуміння та впровадження цих тенденцій може значно принести користь організаціям у різних секторах.



РОЗДІЛ 2. АНАЛІЗ СИСТЕМИ ТА РЕКОМЕНДАЦІЇ ЩОДО МОДЕРНІЗАЦІЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОГО КОМПЛЕКСУ ГОТЕЛЬНОГО ПІДПРИЄМСТВА «ПРЕЗИДЕНТ ГОТЕЛЬ»

2.1. Загальна характеристика готельного підприємства «Президент Готель» та аналіз його господарської діяльності

«Президент Готель» – чотиризірковий бізнес-готель, розташований в центрі Києва на вулиці Госпітальній 12.

Готель використовує сучасні засоби інформаційної підтримки, включаючи копіювальні апарати, факси, персональні комп'ютери з доступом до Інтернету, а також офіційний веб-сайт для потенційних клієнтів, на якому можна отримати інформацію про історію готелю та поточні послуги.



Як бізнес-орієнтований готель, «Президент-готель» націлений на людей із середнім і високим рівнем доходу, з акцентом на МІСЕ-туристів (зустрічі, інсентиви, конференції та виставки), які приносять компанії найбільший відсоток прибутку. Для роботи з цим сегментом ринку в готелі працює відділ корпоративного туризму та розміщення гостей, який надає консультації щодо підбору номерів та пакетів послуг, вибору конференц-залу та розробки розважальної програми.

«Президент-готель» має перевірену історію надійності та стабільності – понад 30 років успішної роботи (готель було засновано у 1990 році). Готель також є членом різноманітних туристичних і готельних асоціацій. У 2012 році в готелі була проведена масштабна реконструкція, яка призвела до оновлення номерного фонду до рівня 4 зірки та перепрофілювання банкетних і конференц-залів для одночасного проведення до 17 самостійних заходів.

Готель не пропонує особливих цін на свої послуги, натомість наголошує на якості та особистому досвіді, щоб виділитися серед

конкурентів. Такий акцент на престиж і якість позиціонує готель як бажаного партнера для великих туристичних операторів і закладає основу для майбутнього розвитку на міжнародних ринках.

На додаток до технологічних досягнень і стратегій, які реалізує Президент-Готель, також важливо відзначити, що готель також інвестував у різні практики сталого розвитку. Це включає реалізацію програми переробки, використання енергозберігаючих приладів та запровадження практик зеленого будівництва під час реконструкції 2012 року. Готель також пропонує гостям можливість відмовитися від послуг щоденного прибирання, щоб зберегти ресурси та сприяти екологічній відповідальності. Ці екологічні методи не тільки приносять користь навколишньому середовищу, але й узгоджуються з екологічними принципами готелю та можуть стати унікальною перевагою для соціально свідомих мандрівників.

Крім того, «Президент-готель» також інвестував в інноваційні маркетингові стратегії, такі як використання платформ соціальних мереж для досягнення потенційних клієнтів і пропонування програм лояльності для постійних клієнтів. Готель співпрацює з туристичними агентствами та платформами онлайн-бронювання, такими як Booking.com, Expedia та Agoda, щоб підвищити видимість і охопити ширшу аудиторію.

Це готельне підприємства також надає різноманітні послуги, щоб задовольнити потреби ділових мандрівників, такі як приміщення для проведення засідань, конференц-зали та бізнес-центри, обладнані найсучаснішими технологіями та такими послугами, як високошвидкісний Інтернет, послуги друку та сканування тощо. Подібний асортимент робить його ідеальним рішенням для своїх гостей.

Підсумовуючи, президент-готель запровадив низку технологічних досягнень, екологічних практик і маркетингових стратегій, щоб створити конкурентоспроможний продукт і залучити різноманітне коло клієнтів.

Прагнення готелю до екологічності, зручності та стійкості, а також інноваційні маркетингові та бізнес-орієнтовані послуги виділяють його серед конкурентів і зміцнюють його позиції як провідного постачальника високоякісних готельних послуг.

2.2. Структурно-функціональна схема інформаційно-комунікаційних технологій «Президент Готель»

У своїй організаційній діяльності використовує ІКТ систему за моделлю RBAC, яка є переважною моделлю недискреційного контролю доступу. RBAC не дозволяє користувачам бути безпосередньо пов'язаними з даними та дозволами. Натомість за допомогою RBAC дозволи в готелі надаються для ролей, а ролі – для користувачів. Таким чином, під час адміністрування RBAC необхідно керувати двома різними типами асоціацій: асоціаціями між користувачами та ролями та асоціаціями між ролями та дозволами.

Отже, коли посада користувача змінюється (наприклад, підвищення або трансфер робітника в інший відділ), змінюються лише асоціації користувача/ролі. Якщо посада представлена однією роллю, тоді, коли посада користувача змінюється, можна змінити лише два зв'язки користувача/ролі: видалити зв'язок між користувачем і поточною роллю користувача та додати зв'язок між користувачем і нова роль користувача.

Враховуючи, що зазвичай існує прямий зв'язок між вартістю адміністрування та кількістю зв'язків, якими необхідно керувати для адміністрування політики контролю доступу: чим більша кількість зв'язків, тим дорожче та більш схильне до помилок адміністрування контролю доступу; у більшості організацій використання RBAC зменшує кількість асоціацій, якими потрібно керувати. Посади зазвичай обіймають більше ніж одна особа, і більшість посад потребують кількох дозволів для того, щоб особа, яка займає посаду, могла виконувати обов'язки цієї посади. Можна описати асоціації, що надають дозволи особам, які виконують обов'язки

посади, як упорядковану пару, що складається з набору осіб і набору дозволів, тобто:

$$(U, P) \quad (2.1)$$

де, U – це набір осіб на посаді,

P – це набір дозволів, необхідних для виконання цієї посади.

Таким чином, кількість асоціацій, необхідних для прямого зв'язку осіб із цими дозволами, становить:

$$U \vee \times \vee P \vee \quad (2.2)$$

де $|U|$ – це кількість особин у множині;

P – це кількість дозволів у множині.

Обмежуючим фактором ефективного застосування систем контролю доступу є адміністративний інтерфейс. Система контролю доступу готелю надає адміністраторам контекст для специфікації та застосування складних політик безпеки, які часто непрактично застосовувати через пряме адміністрування механізмів контролю доступу нижчого рівня. На відміну від традиційно поширених серед готельних підприємств ACL, які підтримують лише специфікацію зв'язків користувач/дозвіл і група/дозволи, модель RBAC підтримує специфікацію зв'язків: користувач/роль і роль/роль. Зокрема, модель RBAC підтримує специфікацію:

- асоціації користувач/роль, тобто повноваження користувача для виконання ролей;
- ієрархії ролей, наприклад, рольовий менеджер готелю успадковує всі дозволи позицій нижче нього;
- обмеження поділу обов'язків (асоціації ролей/ролей, що вказують на конфлікт інтересів);

- обмеження на кількість користувачів, які можуть бути авторизовані для ролі (кардинальність ролей), наприклад, готель у Ганні має лише одного керівника відділення.

Для додатків веб-сервера «Президент Готель» ця система забезпечує адміністративні зручності, об'єднуючи, здавалося б, непов'язані та незрозумілі дані авторизації механізмів керування доступом нижчого рівня та інші дані у єдину базу даних та представляє цю базу адміністраторам інтрамережі в легкому та доступному форматі.

З точки зору адміністратора, ІКТ система «Президент Готель» служить інструментом візуалізації та обслуговування для організації політики контролю доступу. Однак, навіть із розширеним адміністративним інтерфейсом існують можливості для невідповідностей, які можуть призвести до небажаних наслідків та ризиків безпеки. Тому складність роботи з проблемами узгодженості не делегується адміністратору, а натомість обробляється адміністративним програмним забезпеченням автоматично.

Обсяг системи доступу «Президент Готель», обмежений тими властивостями, які вперше були встановлені ще у 2012 році після масштабної реконструкції готелю.

Так, актуальна модель безпеки готелю складається з двох компонентів MS0 і MS1. Компонент системи MS0 визначає властивості безпеки для авторизації в системі робітників готелю. Компонент системи MS1 визначає властивості безпеки для авторизації гостей готелю.

Крім того, у 2015 році в ІКТ було інтегровано нову структуру під назвою GuardMR, яка забезпечує захист даних за допомогою платформи MapReduce. Таким чином, будь-який неавторизований вміст, включений до аналізованого ресурсу, видаляється або маскується. Точніше, фільтри визначають передумови для обробки будь-якої пари ключ-значення, отриманої з цільового ресурсу, що аналізується. При цьому фільтри

призначаються суб'єктам на основі охоплених ролей, і пропонується формальний підхід специфікації до визначення фільтрів, який дозволяє вказувати критерії відбору та модифікації на дуже високому рівні абстракції за допомогою мови обмежень об'єктів.

Щодо програмного забезпечення, то ІКТ «Президент Готелю» адаптує розширений режим управління готелем відповідно до практичних характеристик готельного менеджменту. Система взяла на озброєння передовий міжнародний досвід управління готелями, інтегрувавши в наукові, стандартизовані, успішні міжнародні думки щодо сучасного управління доступом.

У поєднанні з передовою комп'ютерною технологією система управління забезпечує безпечну та надійну інформацію. При цьому вона використовує стандартизоване програмне забезпечення, яка охоплює:

- управління стійкою реєстрації;
- керування інформацією в Інтернеті;
- довідкову інформацію та використовував стабільну базу даних на основі SQLserver2000;
- архітектуру клієнт/сервер і браузер/сервер.

Усі меню, вікна, режими роботи програмного забезпечення є браузерними. Керівництво готелю, яке бере участь у проекті, може взаємодіяти з інтерфейсом у режимі реального часу прямо в інтерфейсі. А додаткові функції, такі як керування пароллями, резервне копіювання бази даних, відновлення, ініціалізація та шифрування забезпечують безпеку програмного забезпечення. Вбудована системна система журналювання, яка записує всі операції в системі, забезпечує стабільність та надійність системи, яка базується на потужному способі нечітких запитів і звітів та класичному програмному забезпеченні.

ІКТ готелю також інтегрована з передовим інформаційними системами провідних глобальних готельних мереж, наприклад home inns network. Вона адаптує трирівневу архітектуру на основі J2EE та полегшену структуру для формування програмного забезпечення та архітектури плагінів. Технологія AJAX покращує взаємодію з користувачем і збільшує можливості для маніпуляції системою внаслідок гнучкої розробки.

Архітектурою програмного забезпечення готелю є В/S на основі J2EE. В/S є аббревіатурою Browser/Server (Браузер/Сервер). Подібну ІКТ використовують такі компанії як Microsoft, IBM, HP і Lenovo, Founder, TongFang, Thunis. Основна частина ІКТ готелю розроблена на мові JAVA. Крім того, структура В/S «Президент Готелю» може бути встановлена в локальній мережі (LAN), а може базуватися на глобальній мережі. Через це, в клієнтів та робітників готелю нема потреби встановлювати спеціальний клієнт на їх девайси.

Паралельно компанія має спеціальний мобільний додаток підключений до системи. Цей додаток оновлюються разом із сервером, тому у клієнтів не виникає потреби у регулярній інсталяції оновлень. За допомогою центральної бази швидку реєстрацію (як зі сторони клієнта, так і зі сторони готелю) можна здійснити лише шляхом введення кількох необхідних даних, таких як дати заїзду та виїзду, що дозволяє не чекати гостей, а портъе готелю може ввести інформацію про гостей та інформацію про депозит, коли він чи вона не зайняті. А доступ до зовнішньої мережі передається шляхом аутентифікації та шифрування даних. Крім того, система управління доступом «Президент Готелю» має вбудоване середовище для SMS-маркетингу.

Таким чином, ІКТ готелю – це чиста технологія В/S з необмеженою кількістю плагінів та сайтів, яка безпосередньо встановлена на сервері готельного ланцюга.

У контексті систем доступу поняття ризику часто визначається в термінах поєднання ймовірності того, що загроза виникне, і серйозності результату впливу загрози. Враховуючи, наведений вище аналіз ІКТ готелю вважаємо, що ризик надання запиту на надання певного дозволу може загалом визначатися вартістю, яка буде понесена, якщо дозвіл буде авторизовано та згодом використано не за призначенням, а також імовірністю того, що дозвіл буде використано не за призначенням.

Своєю чергою вартість неправомірного використання дозволу визначається цінністю інформації. Однак, з іншого боку, важко визначити ймовірність неправомірного використання дозволів за своєю суттю, оскільки це вимагає здатності передбачити майбутні дії запитувачів.

Крім того, існує природна відповідність між надійністю та ймовірністю неправильного використання дозволів. У класичних моделях RBAC (і моделях контролю доступу загалом) авторизованим користувачам завжди довіряють, що вони не зловживатимуть дозволами, для яких вони авторизовані. Однак очевидно, що деякі авторизовані користувачі не заслуговують довіри. Інтуїтивно зрозуміло, що користувача, який має високу ймовірність зловживати своїми дозволами, можна просто вважати менш надійним. Наприклад, у системі готелю ми можемо забажати надати дозвіл персональну документацію робітникам готелю не тому, що це доцільно, а тому, що в екстреній ситуації може бути життєво важливо, щоб якийсь працівник мав доступ до персональної інформації клієнта (наприклад, міг зв'язатись з його рідними або визначити його тип крові в екстреній ситуації). Враховуючи роль, яка пов'язана з деякими менш відповідними дозволами щодо посадових обов'язків ролі, ми вважаємо, що будь-який користувач, авторизований для цієї ролі, має відносно високу ймовірність неправомірного використання цих дозволів.

Іншими загрозами є:

1. Зовнішні атаки: вони включають усі загрози у сценаріях, що передбачають використання загальнодоступних інфраструктур. Ці загрози можуть призвести до втрати конфіденційності та цілісності. Наприклад, хмарні платформи можуть готелю бути заражені шкідливим кодом. Прикладом є вірус Bluepill, яки інфікували хмарне сховище даних готелів в США у 2008 році, що надало хакерам доступ до керування віртуальними машинами (VM) підприємства.

2. Несправність системи: помилка у використовуваному програмному забезпеченні може мати несприятливі наслідки. Імовірність цієї загрози висока і відноситься до числа найбільш частих.

3. Переривання обслуговування: стихійні лиха, такі як землетруси, можуть призвести до переривання обслуговування системи. Іншим прикладом є перевантаження системи, що призводить до погіршення продуктивності або повної відмови системи.

Кожну з наведених вище загроз можна додатково проаналізувати з точки зору того, хто їх спричиняє, та інциденти, що призвели до них, які потім можуть бути пріоритетними залежно від цієї інформації. Залежно від пріоритету активів і ймовірності виникнення загроз, елементи загрози можна відобразити в матриці оцінки.

Так, всі загрози, пов'язані з конфіденційністю, класифікуються як високі, оскільки вони серйозно впливають на довіру та імідж готелю. Втрата конфіденційності також може перетворити низькі загрози, такі як крадіжка інформації, на дуже високі.

Ризик цілісності класифікується як низький, оскільки порівняно з конфіденційністю та доступністю вплив набагато менший. Втрата цілісності може бути спричинена помилкою програмного забезпечення, помилкою користувача, несправністю обладнання, а також із-за зміни даних злоумисником.

Здійснений аналіз загроз також показав загальні дослідницькі проблеми для кожної з загроз:

- масштабований детальний контроль доступу та конфіденційність даних;
- використання систем ідентифікація поведінки користувача для запобігання витоку даних;
- виявлення шкідливих програм на віртуальних машинах на рівні гіпервізора шляхом виконання статичного та динамічного аналізу;

В майбутньому ці пропозиції можуть бути розширено у повноцінні моделі та навіть самостійні системи контролю доступу. Так, детальний контроль доступу та доступу до конфіденційних даних частково розроблені у розділі 3 цієї роботи.

2.3. Рекомендації по удосконаленню інформаційно-комунікаційного комплексу технологій підприємства «Президент Готель»

Як ми вже розглядали вище, ІКТ готелю потребують високого рівня захисту даних. У цьому контексті пропонуємо нову систему перевірки особи (співробітника готельного підприємства) шляхом об'єднання перевірки онлайн-підпису, машинного навчання, ІОТ і блокчейну, щоб впоратися з ризиком крадіжки особистих даних клієнтів. У цій моделі сигнали значень крену, тангажу та ухилу, отримані від датчика MPU6050 (інерційного вимірювального пристрою), аналізуються за допомогою цифрового обгортання часу, щоб отримати мінімальну відстань DTW для перевірки особи користувача.

Загалом, письмові підписи є одним із найдавніших методів аутентифікації. Останнім часом біометрична аутентифікація здійснюється в електронному вигляді. Кілька способів автентифікації біометричної ідентичності – це сканування сітківки ока, розпізнавання райдужної оболонки ока, сканування відбитків пальців і розпізнавання обличчя. Усі ці

методи автентифікації є більш безпечними та надійними. Однак, всі ці методи біометричної автентифікації ігнорують один важливий фактор, а саме ситуацію під час автентифікації. Співробітника готелю можна змусити надати пароль до системи або його можуть вкрати через людські помилки. Відбитки пальців можна взяти у непритомної людини або змусити зробити пройти аутентифікацію проти її волі. Тоді як письмові підписи повинні бути зроблені особою в повній свідомості, і будь-який незначний психологічний тиск може призвести до зміни підпису, що може призвести до відмови в аутентифікації.

Безпосередньо перевірка підпису є важливою галуззю досліджень для експертів з розпізнавання образів і криміналістів. Зараз використовуються два типи методів перевірки підпису: офлайн і онлайн. Перевірка підпису в офлайн (автономному) режимі працює над обробкою зображень шляхом аналізу шаблону в підписі. Перевірка підпису онлайн є набагато кращою та надійнішою порівняно з офлайн, оскільки вона динамічно ідентифікує унікальну особу шляхом аналізу акселерометра, гіроскопа та значень тиску розумного пера. Більшість онлайн-досліджень щодо перевірки цифрових підписів проводилися на планшетах. Однак, у 1990 році для перевірки підписів почали активно використовуватися динамічне викривлення часу (DTW), регіональна кореляція та скелетне дерево, що було значним покращенням у порівнянні з попередньою роботою.

З розвитком технологій онлайн перевірка підпису була реалізована на електронному планшеті. Було проведено кілька досліджень з використанням різних алгоритмів машинного навчання. Так, у 2011 році була представлена апаратна модель прототипу для виконання динамічної перевірки підпису на папері за допомогою спеціального апаратного забезпечення, прикріпленого до пера.

Тож пропонуємо систему, де ключ доступу або пароль до системи та бази даних готелю ніде не зберігається, а генерується кожного разу за

допомогою методу, що включає біометричні дані та машинне навчання. Потім необхідні дані будуть надіслані в блокчейн за допомогою системи IOT для завершення транзакції.

Для отримання підпису можна використовувати MPU 6050, який складається з тривісного акселерометра та тривісного гіроскопа для отримання значень IMU (інерціальний вимірювальний блок) (Додаток А). Вихідні значення акселерометра та гіроскопа перетворюються на крен, тангаж і поворот за допомогою цифрового процесора руху (DMP), попередньо встановленого в MPU 6050. Дані з MPU 6050 дані надсилаються на Raspberry pi zero (мінікомп'ютер, який безпосередньо підключений до Інтернету для виконання всіх транзакцій), який вже активно використовується у готелі (Додаток Б).

Таким чином, для динамічної онлайн перевірки підпису використовується значення IMU, які спочатку передаються на міні-комп'ютер. Для початкового налаштування користувачеві потрібно надати 10 зразків однакової сигнатури, ці зразки використовуються для створення хвилі норми. Оскільки датчики подають сигнали, навіть коли перо не рухається, перед генеруванням нормальної хвилі нам потрібно витягти ті частини з показань датчика, які відповідають сигнатурі. Після нормалізації цілісність хвилі зберігається, однак вона покращує функції, щоб зробити дані більш надійними, що допомагає алгоритму DTW аналізувати подібність у кожному наступному підписі..

При цьому після налаштування параметрів повна функція, хеш і закритий ключ видаляються. Хеш, згенерований зі стандартного підпису, використовується для генерації закритого ключа. Цей закритий ключ безпосередньо надсилається до систему без будь-яких проміжних ланок між ними. Тобто, приватний ключ не зберігається ніде в системі ні в режимі онлайн, ні в автономному режимі, а генерується на основі письмової автентифікації підпису. Це дозволяє робітникам готелю отримувати доступ

до баз даних без фактичного вводу ключа чи паролю, тим самим покращуючи безпеку та захист від крадіжок цих даних.

Ще однією пропозицією щодо модернізації ІКТ готелю буде модель безключової системи доступу для клієнтів, яка генерує унікальний ідентифікатор (наприклад, код), який надсилається безпосередньо (наприклад, електронною поштою чи мобільною програмою) авторизованим користувачам (гостям готелю), які потім можуть використовувати ідентифікатор, щоб отримати доступ до певного набору послуг. У сервісному середовищі безключові системи мають потенціал для надання клієнтам бездоганного досвіду, уникаючи потенційних перебоїв, пов'язаних з системами з підтримкою ключів (наприклад, тривале очікування ключів, несправність електронних ключів, таких як смарт-карти, і ризик копіювання фізичного ключа попередніми користувачами), і, що більш важливо, надає можливість насолоджуватися плавним і безперервним досвідом під час перебування у готелі.

Однак реалізація цього потенціалу є складною, оскільки постачальники послуг повинні вибрати та впровадити відповідну технологію таким чином, щоб заохочувати використання та зменшувати опір клієнтів безключовим системам. Якщо говорити точніше, існують два основні обмеження здатності сучасних безключових.

По-перше, більшість безключових систем покладаються на передачу та прийом низькоенергетичних або радіосигналів (наприклад, Bluetooth з низьким енергоспоживанням BLE, ближній зв'язок NFC і технології радіочастотної ідентифікації RFID для з'єднання та зв'язку між користувачем і системою. Якщо постачальники послуг приймають системи без ключа, які покладаються на ці технології, їхні клієнти повинні володіти та/або використовувати відповідні розумні пристрої. Це створює проблему для постачальників послуг, які хотіли б обійтися без ключа, але мають клієнтів, які можуть не мати або не використовувати сумісні пристрої.

По-друге, безключові системи, які використовують низку технологій (або надають кілька опцій, наприклад, технологію швидкого реагування, тобто здатність сканувати та розпізнавати роздруківку чи цифрову копію QR-коду), є дуже обмеженими щодо обсягів інформації. Обидві ці проблеми обмежують ступінь, до якого безключові системи можуть надати клієнтам бездоганний досвід роботи в середовищі обслуговування.

На тлі цих проблем і дизайну наявних систем без ключа розроблена модель має на меті описати й проаналізувати сприйняття користувачами системи без ключа, яку постачальники послуг можуть використовувати, щоб запропонувати клієнтам бездоганний досвід роботи в готелі «Президент Готель».

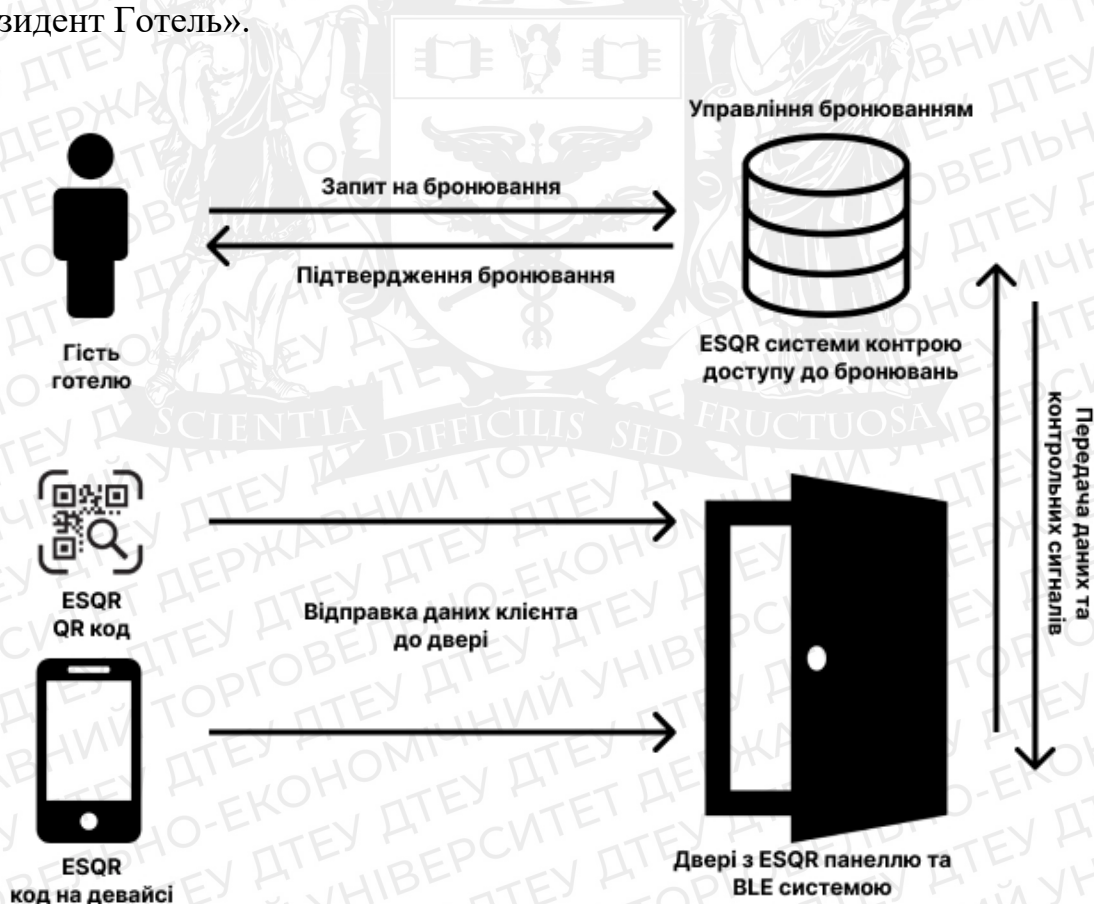


Рис. 2.1. Схема роботи системи UNAS для реєстрації гостей
Джерело: складено автором за матеріалами [18].

Ця модель (рис. 2.1) описує використання інженерного підходу до систем обслуговування для розробки уніфікованої системи контролю

доступу до готелю (UHACS), яка надає гостям готелю безключові можливості (тобто роздруківку або цифрову копію унікального коду) для реєстрації в готелі та доступу до номерів.

UHACS – це інженерами система для реєстрації гостей готелю та доступу до номерів за допомогою схеми ESQR. Схема ESQR в UHACS підтримується двома основними системами:

1. Система керування бронюванням готелю з підтримкою ESQR, яка керує процедурою бронювання готелю та генерує та перевіряє унікальні коди ESQR

2. Система керування дверима з підтримкою ESQR, яка використовує панель керування складається з Raspberry PI (тобто «мозок» UHACS, який декодує унікальні ESQR-коди та виконує операції, необхідні для реєстрації та доступу до кімнат через різні модулі), модуля плати камери (тобто для захоплення унікальних ESQR-кодів), мережевого модулю для забезпечення зв'язку між дверима з підтримкою ESQR і системами керування бронюванням готелів, модулю BLE для надсилання сигналу «розблокування» до дверних замків.

По суті, схема ESQR дозволяє надавати гостям готелю безперебійний досвід, оскільки вона дозволяє їм залишатися в готелі без ключів. На практиці це виглядає наступним чином:

1. Гість готелю розміщує бронювання, надає детальну інформацію про себе, методи оплати, вимоги до номерів і дати перебування у мобільному додатку, на вебсайті компанії, або через турагента.

2. Система керування бронюванням готелю з підтримкою ESQR отримує, зберігає та обробляє цю інформацію (наприклад, перевіряє деталі платежу та призначає номер) і генерує унікальний код ESQR для гостя (гостей) за умови, що немає проблем із наданою інформацією (наприклад, дані кредитної картки дійсні та запитані номери вільні). У разі виникнення

проблем унікальний код ESQR не генерується, і гостю буде запропоновано вирішити виявлені проблеми, щоб завершити бронювання.

3. Гість готелю отримує підтвердження бронювання, включаючи унікальний ESQR-код і номер кімнати.

4. Гість готелю прибуває в готель для заброньованого перебування, проходить до заброньованого номера та надає унікальний код ESQR (наприклад, роздруковану копію або такий, який відображається на портативному електронному пристрої, такому як смартфон) на панель керування система керування дверима з підтримкою ESQR.

5. Система керування дверима з підтримкою ESQR надсилає облікові дані гостя готелю, отримані з унікального коду ESQR, до системи бронювання керування готелем із підтримкою ESQR через локальну мережу (LAN) для перевірки початкової реєстрації та отримання дозволу на номер.

6. Якщо було подано дійсний унікальний код ESQR, система керування готелем із підтримкою ESQR надсилає контрольний сигнал до системи керування дверима через локальну мережу, підтверджуючі реєстрацію та дозволяючи розблокувати двері. Якщо унікальний код ESQR недійсний, гість готелю повинен буде підійти до стійки реєстрації готелю, щоб зареєструватися вручну та отримати дійсний унікальний код ESQR для доступу до номера після підтвердження його особи та бронювання.

Однак, ця модель має кілька обмежень.

По-перше, сфера застосування UNACS поки що обмежена реєстрацією в готелі та номері. Надалі слід провести дослідження, щоб інтегрувати цю систему в ширший спектр функцій і послуг (наприклад, доступ до конференц-залів і фітнес-залів, а також оплата обслуговування номерів).

По-друге, у цій моделі увага здебільшого приділяється лише функціональними аспектами системи, що склалися зі сприйняття її

простоти у використанні, корисності, однак не було досліджено ризикованості подібної системи.



ВИСНОВКИ

Еволюція ІКТ пройшла різні етапи розвитку, просуваючись від простого незахищеного обміну даними до реалізації складних систем, що охоплюють цифрові бази даних, технічне обладнання готелю та різноманітні аспекти сервісного обслуговування. Такий розвиток є прямим результатом зростання глибини та складності інформаційної сфери та становлення інформаційного суспільства.

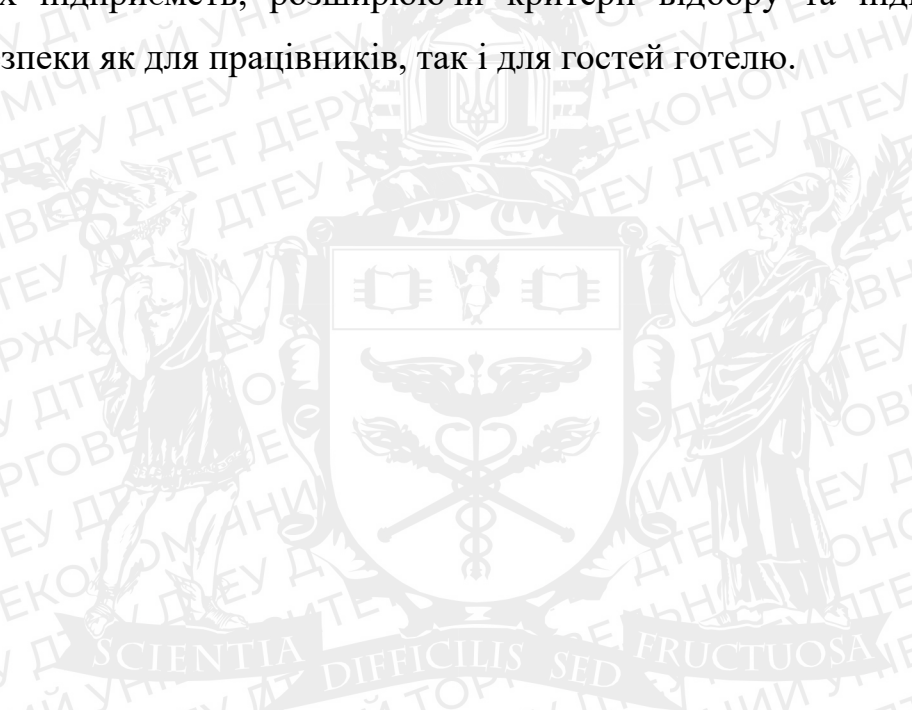
Як результат компанії, зокрема готельні підприємства, все більше зацікавлені у використанні таких систем не лише для захисту внутрішньої інформації, але й для проведення ефективних бізнес-операцій. Аналіз готельного сектору, зокрема, вказує на початок нової фази розвитку, коли системи контролю доступу перетворюються на передові технологічні продукти, які змінюють звичайні ринкові стратегії, підривають традиційну бізнес-практику та кидають виклик усталеним регуляторним перспективам – і все це на користь споживачів. Інтеграція багатосторонніх обчислень і великих даних також дозволила модернізувати репрезентативну достовірність, знизити витрати для організацій і підвищити довіру та прозорість у системі в цілому.

Було розроблено дві моделі модернізації ІКТ на прикладі розглянутого готельного підприємства, які засновані на криптографічному та інженерних підходах для створення уніфікованої системи контролю доступу до готелю (UNAS) та нової системи перевірки особи. Обидві моделі надають гостям та робітникам готелю безключові можливості для реєстрації, авторизації та доступу до різноманітних баз технічного облаштування, сервісних послуг та інформаційних потоків в готелі та поза його межами.

Наступним кроком дослідження має бути вивчення різних методів реалізації розроблених у цій роботі моделей. Це дозволить вивчити практичні вимоги до ІКТ та визначити їх переваги. Розроблені моделі

являють собою проекти високого рівня, які можуть слугувати основою для подальших досліджень практичних питань, з акцентом на вдосконалення процесів безключового доступу до систем управління та баз даних за допомогою використання криптографічних технологій.

Результати цього дослідження, зокрема використання методів шифрування, можуть бути інтегровані в системи ІКТ та політики безпеки готельних підприємств, розширюючи критерії відбору та підвищуючи рівень безпеки як для працівників, так і для гостей готелю.



СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гончар Л. О. Управлінський аналіз особливостей системи контролінгу в готельно-ресторанному бізнесі [Електронний ресурс] / Л. О. Гончар, А. В. Поплавська, О. В. Аухімік // Індустрія туризму і гостинності в Центральній та Східній Європі. – 2021. – № 3. – С. 12–17. – Режим доступу: <https://doi.org/10.36477/tourismhospsee-3-2> (дата звернення: 20.01.2023). – Назва з екрана.
2. Д'яченко Ю. Ю. Особливості управління інноваційними процесами на підприємствах готельно – ресторанного господарства [Електронний ресурс] / Ю. Ю. Д'яченко, А. В. Огар // ВІСНИК СХІДНОУКРАЇНСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ імені Володимира Даля. – 2021. – № 3 (267). – С. 53–57. – Режим доступу: <https://doi.org/10.33216/1998-7927-2021-267-3-53-57> (дата звернення: 20.01.2023). – Назва з екрана.
3. Леус Т. А. Інформаційно-комунікаційні технології / Т. А. Леус // Хімія. – 2017. – № 5/6 (377/378), берез. – С. 74–79.
4. Лопатюк Р. І. Перспективи розробки, впровадження та застосування інноваційних готельних концепцій [Електронний ресурс] / Р. І. Лопатюк // Herald of Lviv university of trade and economics economic sciences. – 2020. – № 61. – С. 112–117. – Режим доступу: <https://doi.org/10.36477/2522-1205-2020-61-17> (дата звернення: 20.01.2023). – Назва з екрана.
5. Половенко Л. П. Тенденції та проблеми розвитку інноваційних технологій в індустрії гостинності [Електронний ресурс] / Л. П. Половенко, С. В. Мерінова // Наукові праці Міжрегіональної Академії управління персоналом. Економічні науки. – 2021. – № 3 (62). – С. 74–81. – Режим доступу: <https://doi.org/10.32689/2523-4536/62-12> (дата звернення: 20.01.2023). – Назва з екрана.

6. Постова В. В. Особливості формування та підтримка іміджу підприємств готельно-ресторанного бізнесу [Електронний ресурс] / В. В. Постова, А. В. Лук'янець // Підприємництво та інновації. – 2020. – № 14. – С. 63–67. – Режим доступу: <https://doi.org/10.37320/2415-3583/14.12> (дата звернення: 20.01.2023). – Назва з екрана.
7. Президент-готель [Електронний ресурс]. – Режим доступу: https://youcontrol.com.ua/catalog/company_details/30058128/. – Назва з екрана.
8. Biles W. E. The engineering science of industrial engineering: a viewpoint of the industrial engineering curriculum [Electronic resource] / William E. Biles // IIE transactions. – 1991. – Vol. 23, no. 3. – P. 208–214. – Mode of access: <https://doi.org/10.1080/07408179108963855> (date of access: 20.01.2023). – Title from screen.
9. Carr N. Is google making us stupid? [Electronic resource] / Nicholas Carr // Teachers college record: the voice of scholarship in education. – 2008. – Vol. 110, no. 14. – P. 89–94. – Mode of access: <https://doi.org/10.1177/016146810811001427> (date of access: 20.01.2023). – Title from screen.
10. Electronic commerce 2018: a managerial and social networks perspective / Jae Kyu Lee [et al.]. – [S. l.] : Springer, 2018. – 664 p
11. Heeks R. Benchmarking e-Government: Improving the national and international measurement, evaluation and comparison of e-Government [Electronic resource] / R. Heeks // Evaluating information systems. – [S. l.], 2008. – P. 257–301. – Mode of access: <https://doi.org/10.1016/b978-0-7506-8587-0.50017-2> (date of access: 20.01.2023). – Title from screen.
12. Hotel for phototourists - a modern trend in the hospitality industry [Electronic resource] / Iryna Oleksandrivna Kalienik [et al.] // Geography and tourism. – 2019. – No. 52. – P. 10–16. – Mode of access:

<https://doi.org/10.17721/2308-135x.2019.52.10-16> (date of access: 20.01.2023). – Title from screen.

13. International Telecommunication International Telecommunication Union.

Measuring the information society report 2016 / International Telecommunication International Telecommunication Union. – [S. 1.] : United Nations Fund for Population Activities, 2017. – 290 p.

14. Jan A. G M. van Dijk. Deepening divide: inequality in the information society / Jan A. G M. van Dijk. – [S. 1.] : SAGE Publications, Incorporated, 2012.

15. Krupinski E. Practical applications of perceptual research [Electronic resource] / Elizabeth Krupinski // Handbook of medical imaging, volume 1. physics and psychophysics. – 1000 20th Street, Bellingham, WA 98227-0010 USA. – P. 895–929. – Mode of access: <https://doi.org/10.1117/3.832716.ch20> (date of access: 20.01.2023). – Title from screen.

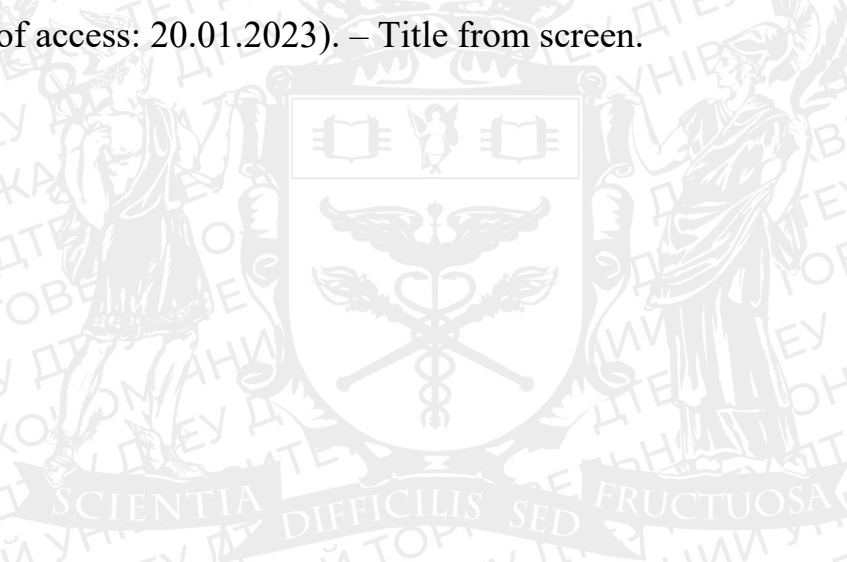
16. Park H.-S. Introduction of directive 2002/44/EC [Electronic resource] / Hee-Sok Park // Journal of the ergonomics society of korea. – 2011. – Vol. 30, no. 2. – P. 375–379. – Mode of access: <https://doi.org/10.5143/jesk.2011.30.2.375> (date of access: 20.01.2023). – Title from screen.

17. President hotel kyiv [Electronic resource] // Facebook. – Mode of access: <https://www.facebook.com/PresidentHotelKyiv/> (date of access: 20.01.2023). – Title from screen.

18. Reintroducing industrial engineering in hotel management [Electronic resource] / Stephanie Marie Villanueva-Pérez [et al.] // Científica. – 2021. – Vol. 25, no. 1. – P. 47–53. – Mode of access: <https://doi.org/10.46842/ipn.cien.v25n1a04> (date of access: 20.01.2023). – Title from screen.

19. Rumiantseva I. V. Основні складові діяльності готельних підприємств в умовах сьогодення [Електронний ресурс] / I. V. Rumiantseva // The actual problems of regional economy development. – 2019. – Т. 1, № 15. – С. 53–58. – Режим доступу: <https://doi.org/10.15330/apred.1.15.53-58> (дата звернення: 20.01.2023). – Назва з екрана.

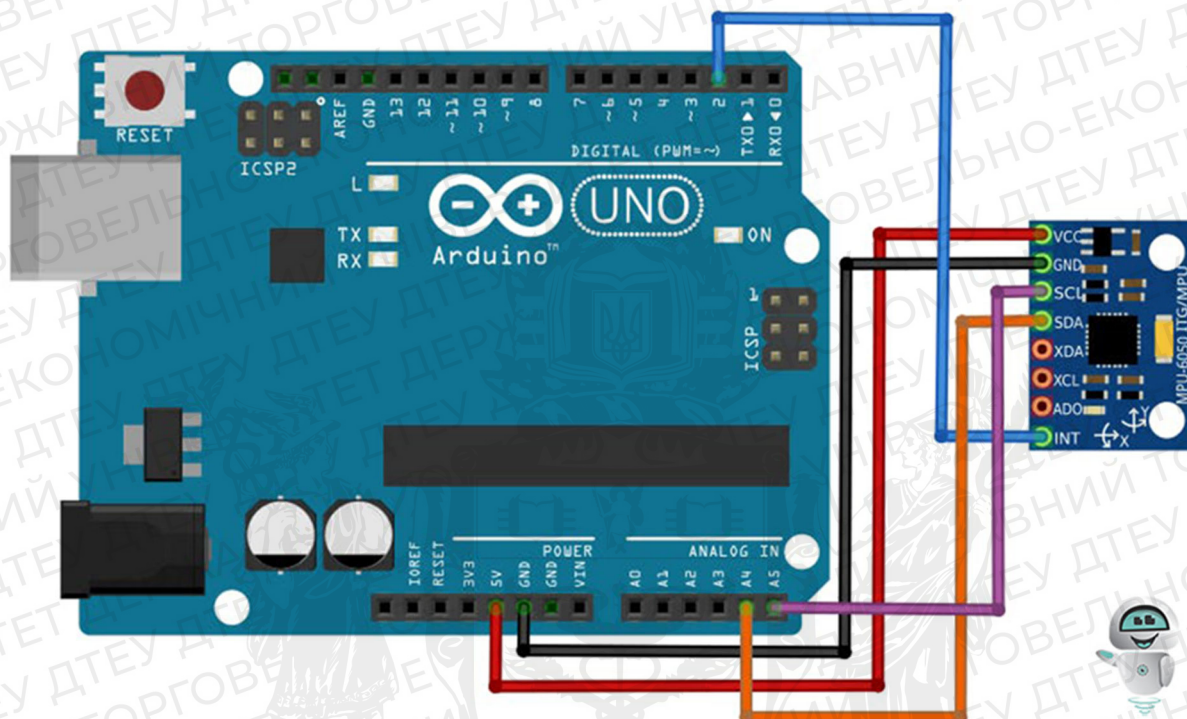
20. Transforming our world: implementing the 2030 agenda through sustainable development goal indicators [Electronic resource] / Bandy X. Lee [et al.] // Journal of public health policy. – 2016. – Vol. 37, S1. – P. 13–31. – Mode of access: <https://doi.org/10.1057/s41271-016-0002-7> (date of access: 20.01.2023). – Title from screen.



ДОДАТКИ

Додаток А

Акселерометр і гіроскоп MPU-6050



Міні-комп'ютер Raspberry pi zero