Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система контролю доступу готельного комплексу "Coliseum"
Назва теми

КРКБ.189130.19.01.07 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *125 «Кібербезпека»*
Шифр, назва

Освітня програма *«Кібербезпека»*
Назва

Виконав: студент IV курсу, група КБ–19–1 _____ Р.Л. Житнік
Підпис Ініціали, прізвище

Керівник _____ 07.06.2023 В.С. Орленко
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ 07.06.2023 С.В. Мостовий
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки та _____ Ю.П. Кльоц
Підпис *Ініціали, прізвище*

« 7 » червня 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ БАКАЛАВРІВ

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Ю. Кисоч

1 03 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Житніку Роману Леонідовичу

Прізвище, ім'я, по батькові студента

1 Тема роботи Система контролю доступу готельного комплексу "Coliseum"

Керівник роботи к.т.н, доц. Орленко В.С.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від 01.03.2023 № 5 додаток 11

2 Строк подання студентом роботи на кафедру: 3.06.2023

3 Вихідні дані до роботи план будівлі готельного комплексу "Coliseum", іноформаційна система, кадри.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Дослідження предметної області та постановка задачі, створення моделей загроз та порушника, розробка системи фізичного захисту внутрішніх приміщень та контролю периметру ,проєктування БД

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) «Модель загроз», «Модель порушника», «Система відеоспостереження», «Модель БД», «Функціональна схема мережі та системи контролю доступу».

6 Консультанти розділів курсового проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завда прий

7 Дата видачі завдання 01 березня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Пр
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	20.02.2023	ви
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження	01.03.2023	ви
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	10.03.2023	ви
4	Робота над розділом 2 – проектування та розробка загальної архітектури і структури системи.	20.04.2023	ви
5	Робота над розділом 3 – проєктування БД, аналіз результатів і оцінювання прийнятих рішень	30.04.2023	ви
6	Оформлення пояснювальної записки згідно вимог	20.05.2023	ви
7	Попередній захист ВКР	25.05.2023	ви
8	Підготовка до захисту та захист кваліфікаційної роботи на засіданні ЕК	Червень 2023 року	

Студент _____ Р.Л. Житнік
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ В.С. Орленко
Підпис Ініціали, прізвище

№ рядка	Формат	Позначення	Найменування	Кількість	№ екземпляру	Примітка
			Текстові документи			
1	А4	КРКБ.189130.19.01.07 ПЗ	Пояснювальна записка	78		
			Графічні матеріали	1		
2	А2	КРКБ.189130.19.01.07 Е8	Інформаційна структура	1		
3	А2	КРКБ.189130.19.01.07 Е8	Модель загроз	1		
4	А2	КРКБ.189130.19.01.07 Е8	Модель порушника	1		
5	А2	КРКБ.189130.19.01.07 Е8	Функціональна схема мережі	1		
			та системи контролю доступу			
6	А2	КРКБ.189130.19.01.07 Е8	Система відеоспостереження	1		
7	А2	КРКБ.189130.19.01.07 Е8	Система відеоспостереження	1		

Зм.	Аркуш	№ докум.	Підп.	Дата	КРКБ.189130.19.01.07 ВП		
Розроб.		Житнік Р.Л.		7.06.25	Система контролю доступу готельного комплексу "Coliseum"	Літера	Аркуш	Аркушів
Перевір.		Орленко В.С.		7.06.25		Н	1	1
Н. Контр.		Мостовий С.Б.		7.06.25	Відомість проекту	ХНУ, КБ-19-1		
Затверд.		Кльоц Ю.П.		7.06.25				

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система контролю доступу готельного комплексу "Coliseum"

Автор роботи: Житнік Р.Л.

Керівник роботи: к.т.н., доц. Орленко В.С.

Пояснювальна записка: 78 с., 17 рис., 7 табл., 2 дод., 40 джерел.

Ключові слова: система контролю доступу, інформаційна мережа готелю.

Метою кваліфікаційної роботи було проведення комплексного безпекового аналізу фізичної та інформаційної структури готельного комплексу "Колізей". Результати аналізу були використані для розробки індивідуальної системи захисту інформації, яка забезпечує безпечне функціонування готелю відповідно до його комерційного призначення.

Мною була проведена систематизація теоретичної інформації, досліджено корпоративну, державну та міжнародну нормативно-правову базу з питань захисту інформації. Запропоновано архітектуру мережі готелю та розроблено програмне забезпечення для персоналу та адміністрації.

07.06.23р.

ANNOTATION

Topic of qualification work: Access control system of the hotel complex "Coliseum".

Author of the work: Zhytnik R.L.

Head of work: Ph.D., Assoc. Orlenko V.S.

Explanatory note: 78 pp., 17 figures, 7 tables, 2 appendices, 40 sources.

Keywords: access control system, hotel information network.

The purpose of the qualification work was to carry out a comprehensive security analysis of the physical and informational structure of the Colosseum hotel complex. The results of the analysis were used to develop an individual information protection system that ensures the safe operation of the hotel in accordance with its commercial purpose.

I systematized theoretical information, researched the corporate, state, and international legal framework on information protection. Proposed hotel network architecture and developed software for staff and administration.

07.06.23 р.

ЗМІСТ

ВСТУП 4

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ 6

1.1 Аналіз предметної області і виявлення наявних проблем і завдань .. 6

1.2 Первинне дослідження об'єкту 7

1.3 Аналіз інформаційної структури об'єкту захисту 9

1.4 Постановка задачі 14

2 РОЗРОБКА КОМПОНЕНТІВ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ..... 16

2.1 Обгрунтування об'єктів захисту 16

2.2 Створення моделі загроз та моделі порушника, на основі проаналізованих даних 21

2.3 Розробка системи фізичного захисту внутрішніх приміщень та контролю периметру 29

2.4 Висновок..... 40

3 ОЦІНКА ФУНКЦІОНАЛЬНИХ ХАРАКТЕРИСТИК СИСТЕМИ ... 42

3.1 Проектування захищеної корпоративної мережевої системи готельного комплексу 42

3.2 Інтеграція спроектованих компонентів в єдину систему 45

3.3 Проєктування бази даних..... 49

3.4 Оцінка собівартості системи 53

3.5 Розробка рекомендацій для реалізації системи 55

3.6 Висновок..... 57

ВИСНОВКИ..... 59

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ..... 60

ДОДАТОК А Фрагменти програмного коду клієнтської частини …… 64
ДОДАТОК Б Копія графічної частини…..…….. 74

ВСТУП

Розвиток інформаційних технологій та глобалізація інформаційного простору створюють серйозні виклики для безпеки інформаційної інфраструктури. Застосування різноманітних засобів обміну інформацією та комп'ютеризація усіх сфер життєдіяльності призводять до того, що захист інформації є надзвичайно актуальним питанням, особливо для організацій, які обробляють значні обсяги інформації різного рівня конфіденційності. У зв'язку з цим, захист інформації від несанкціонованого доступу, зберігання та незаконного використання є надзвичайно важливим завданням для керівництва бізнес установ. Використання сучасних інформаційних технологій на підприємствах може створювати різні загрози, пов'язані з використанням комп'ютерної техніки, тому необхідно серйозно відноситись до питань інформаційної безпеки компанії.

У будь-якій сучасній організації, комерційній чи державній установі, є необхідність у захисті, оскільки будь-яка система може бути вразливою для зловмисників, що може спричинити серйозні збитки, втрату клієнтів, тимчасову чи повну припинення діяльності, судові тяжби та проблеми з законом, які можуть бути спричинені недбалістю до персональних даних та інших вразливих інформаційних ресурсів.

Традиційний підхід до захисту включає охорону периметру, контроль входу, виходу та переміщення по території, а також розбиття внутрішніх приміщень на зони з різним рівнем доступу. Однак у сучасних організаціях важливіше захистити їх інформаційні системи, що передбачає захист від кібератак та використання найновіших технологій та розробок для забезпечення надійності та безпеки.

Навіть бездротовий роутер Wi-Fi, може стати джерелом витоку критичної інформації про діяльність підприємства, його працівників та клієнтів, якщо не буде налаштований належним чином.

Важливо зрозуміти, що недбале ставлення до захисту може спричинити створення критичних вразливостей та загроз діяльності, тоді як занадто високий рівень безпеки на програмному та мережевому рівні без належного фізичного захисту може також виявитись недостатнім.

У підсумку, єдиним ефективним рішенням для забезпечення повноцінного захисту підприємства, організації або будь-якої іншої установи є проведення загального аналізу їх діяльності, інформаційних процесів, структури та внутрішніх зв'язків, а також класифікація інформації, що обробляється, створюється та передається. Необхідно виявити потенційні та реальні вразливості та оцінити загрози, які вони створюють. На цій основі потрібно розробити комплексну систему безпеки яка враховуватиме індивідуальні особливості конкретної організації, буде комплексним і підходитиме до всіх видів діяльності. Ця система повинна класифікувати та встановлювати пріоритети серед виявлених загроз, як програмно-мережевого, так і фізичного характеру. Крім того, вона має мати інтегровані системи моніторингу, контролю та сигналізації.

Ці підходи до забезпечення інформаційної безпеки є ефективними та можуть бути застосовані в будь-яких типах організацій незалежно від їх розміру та виду діяльності. При цьому алгоритм дій при аналізі та розгортанні комплексних систем захисту буде загалом однаковим.

Завдяки впровадженню розробленої системи контролю доступу, готельний комплекс зможе безпечно та ефективно працювати, реагувати на можливі загрози та запобігати їх виникненню. Крім того, використання цієї системи забезпечить надійний захист даних та допоможе уникнути перебоїв у роботі інформаційних ресурсів та всього готельного комплексу в цілому. Інвестування у систему контролю доступу є важливою складовою стратегії готелю для забезпечення високої репутації та запобігання можливим фінансовим втратам.

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз предметної області і виявлення наявних проблем і завдань

У моїй кваліфікаційній роботі я обрав готельний комплекс «Coliseum», він ще має назву готельний комплекс «Колізей» як об'єкт захисту, оскільки покращення безпеки на такому об'єкті є важливим фактором для його подальшого розвитку та успішної роботи. Фізична реалізація комплексної системи захисту, яку я розробляю для готелю, буде мати повсякденне практичне застосування та є актуальною для поточного етапу його функціонування.

Мій проект передбачає створення системи керування доступу для готельного комплексу «Колізей», яка забезпечить безпечне функціонування відповідно до його комерційного призначення. Метою проекту є проведення безпекового аналізу фізичної та інформаційної структури готельного комплексу та створення індивідуальної системи захисту інформації, яка відповідатиме ресурсним можливостям готелю та забезпечить його захист від пріоритетних загроз.

Перед тим, як розпочати розробку системи контролю доступу готельного комплексу «Колізей», необхідно обов'язково детально ознайомитись з теоретичними підходами та інформацією, яка є доступна у відкритому доступі, а також скласти план дій. Крім того, важливо дослідити та проаналізувати нормативно-правову базу, яка встановлює вимоги щодо систем захисту інформації та опрацювання персональних даних в Україні та Європі [1].

Для захисту інформації в готельному комплексі "Колізей" необхідно провести організаційні заходи, що включають адміністративно-організаційні заходи з регулювання та контролю фізичного доступу до приміщень та розробку правил та алгоритмів дій персоналу у різних ситуаціях [2]. Крім цього, надзвичайно важливою є нормативно-правова база, на основі якої функціонує

система захисту інформації. Ця база складається з внутрішньої (корпоративної) нормативної бази та загальної нормативно-правової бази [3, 4].

При проектуванні системи контролю доступу в готельному комплексі також потрібно звернути особливу увагу на захист персональних даних клієнтів та персоналу. З метою забезпечення відповідності європейському стандарту GDPR, який регулює обробку персональних даних жителів Європейського Союзу, необхідно провести обов'язкову обробку персональних даних згідно з цим стандартом [5]. При цьому важливо пам'ятати, що хоча Україна не входить до Європейського Союзу, ряд положень GDPR є обов'язковими до виконання на її території, якщо український комерційний або некомерційний суб'єкт збирає або обробляє персональні дані жителів країн, що входять до Євросоюзу.

1.2 Первинне дослідження об’єкту

Після вивчення теоретичної інформації та нормативно-правової бази комплексних систем захисту інформації, ми переходимо до початкової оцінки безпеки готельного комплексу "Колізей". Для цього ми проведемо первинне дослідження об'єкту захисту, аналізуючи такі характеристики, як фізичне місцеположення та місцевість, розмір території, планування, відмежованість та сусідство, стан будівлі готелю, висоту будівлі, кількість постійного персоналу та наявність позаштатних працівників, перелік підведених комунікацій та засобів протипожежної безпеки. Для забезпечення максимальної достовірності результатів дослідження ми відправимось в готельний комплекс та, з отриманням дозволу адміністрації, проведемо необхідний огляд (рис. 1.1).

Рисунок 1.1 – Зовнішній вигляд готельного комплексу «Колізей»

З використанням сервісу Google Earth, проведемо додатковий пошук інформації у відкритих джерелах, зокрема для одержання аерофотознімків готелю (рис. 1.2). Далі співставимо та повторно проаналізуємо отриману нами інформацію.

Рисунок 1.2 – Аерознімок з сервісу Google Earth

Комплекс розташований на ділянці площею 3000 квадратних метрів, де знаходиться одна капітальна будівля з площею приблизно 1000 квадратних метрів, а також декоративні елементи. Його територія оточена з усіх сторін кам'яним парканом висотою 2 метри, а вхід обладнаний міцними воротами, інші виходи та входи відсутні.

З заходу та півночі готель межує з промисловою зоною, з півдня та сходу - з житловими зонами, багатоповерхівками та дорогою. Будівля готелю побудована з газоблоку та знаходиться в гарному стані. Вона має 2-3 поверхи заввишки, а також підвал. До готельного комплексу підведене водопостачання, каналізація та газопостачання.

Цей комплекс вже має систему протипожежної сигналізації, сертифіковану МНС, а також автоматизовану систему пожежогасіння.

1.3 Аналіз інформаційної структури об’єкту захисту

У будь-якому готелі важливу роль відіграє персонал, який зустрічає гостей та забезпечує їхній комфорт. При виборі готелю люди звертають увагу не лише на його інтер'єр, але й на працівників. В залежності від розміру та рівня готелю, персонал може складатися з адміністраторів, менеджерів, покоївок, кухарів, офіціантів, охоронців, аніматорів, медиків, круп'є в казино, масажистів, перукарів та фахівців манікюру. У сучасному світі, додатково до цих професій, в штаті готелю може бути PR-менеджер та спеціалісти для підтримки веб-сторінки готелю [6].

Згідно з рекомендаціями Всесвітньої туристської організації, мінімальна кількість персоналу для готелю повинна залежати від його статусу. Наприклад, в трьохзірковому готелі повинні працювати не менше ніж 8 людей, в чотирьохзірковому - не менше ніж 12 професіоналів, а в п'ятизірковому - не менше ніж 20. Однак, мінімальний штат готелю повинен становити не менше ніж 4 людини [7].

У готелі різні професії відіграють важливу роль. Директор, менеджер та керуючий готелем можуть мати одну посаду та відповідають за керування всією інфраструктурою. Покоївки відіграють важливу роль у підтримці чистоти та забезпеченні комфорту гостей. Адміністратор - перша людина, яку зустрічають відвідувачі при вході в готель, тому він повинен бути дружелюбним. Адміністратор має бути готовий відповісти на будь-які запитання постояльців та оперативно вирішувати будь-які проблеми, що виникають. До обов'язків адміністратора входить також прийом дзвінків та ведення списку постояльців, які заселяються або виїжджають з готелю.

У відомих готелях рівня чотири та п'ять зірок, зазвичай працюють швейцари. Вони зустрічають гостей на вході та відкривають двері. Одним з обов'язків портьє є отримання пошти.

Постійний персонал комплексу «Колізей» складає 13 чоловік, з них 2 адміністратора, бухгалтер, 2 менеджера, 4 прибиральниці, 2 охоронця, кухар, та садівник.

Після проведення першого етапу дослідження об’єкту захисту, ми переходимо до аналізу інформаційної структури готельного комплексу. Зважаючи на невелику кількість постійних працівників, наша першочергова мета полягає в побудові ієрархічної схеми відносин між ними (рис. 1.3).

За результатами аналізу ми можемо зробити кілька висновків, включаючи той, що всіх працівників готелю можна умовно поділити на дві категорії: тих, хто працює з клієнтами та їхніми даними, та тих, хто не має такого доступу. Першу групу складають адміністратор, менеджер та бухгалтер, а другу - всі інші працівники.

Рисунок 1.3 – Схема персоналу готельного комплексу

У майбутньому, при розробці системи, необхідно враховувати ці фактори, оскільки вони безпосередньо впливають на рівні доступу для різних груп користувачів. Також потрібно виділити базові інформаційні процеси, що є специфічними для готельного комплексу. Деякі з них залежать від внутрішньої мережі та інформаційних накопичувачів, тоді як інші потребують зовнішнього з'єднання з мережею Інтернет (рис. 1.4.).

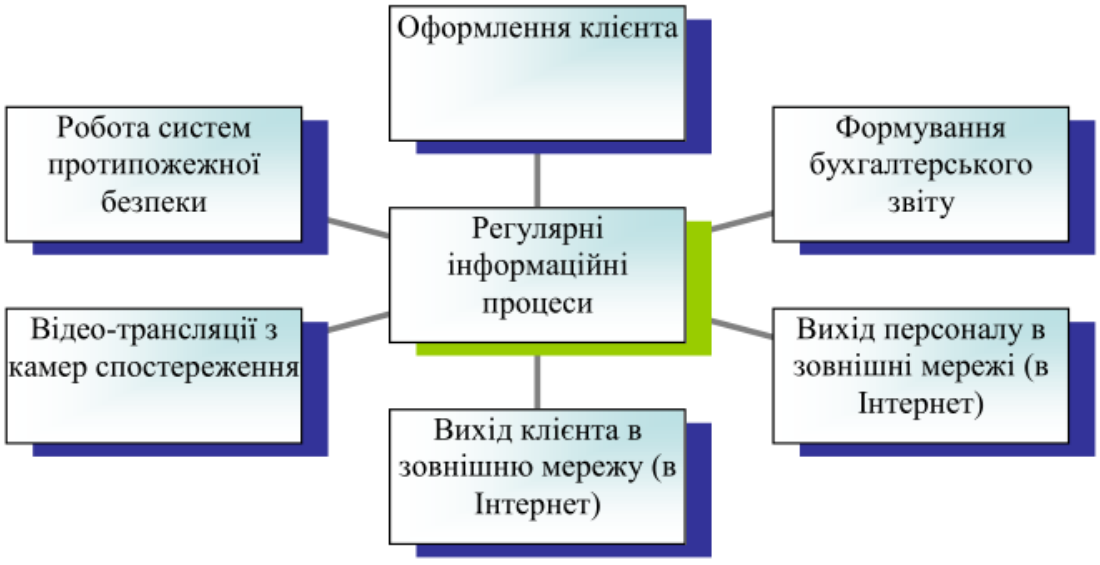


Рисунок 1.4 – Основні інформаційні процеси готельного комплексу

Необхідно зауважити, що підключення до Інтернету є необхідним як для персоналу, так і для клієнтів готелю. Проте, такі з'єднання повинні бути розділені або захищені за допомогою екранування гостьової та робочої мереж, або підключені до глобальної мережі через окремих провайдерів. На сьогодні гостьова та робоча мережі готелю не розділені, що може створювати потенційні вразливості.

Крім того, для подальшої розробки системи контролю доступу, необхідно створити список комп'ютеризованих робочих місць та інших елементів робочої мережі готелю, з вказанням того, хто, згідно зі своїми робочими обов'язками та правами доступу може користуватися ними (табл. 1.1).

Таблиця 1.1 - Перелік вимог до комп'ютеризованих робочих місць готелю

Назва	Доступ	Опис
Робоче місце адміністратора	Комп'ютер, який належить черговому адміністратору, підключений до корпоративної мережі та має доступ до Інтернету	Адміністратор
Робоче місце на рецепції	Комп’ютер, що призначений для обслуговування клієнтів, підключений до корпоративної мережі та має доступ до Інтернету	Менеджер Адміністратор
Робоче місце менеджера	ПК під’єднаний до робочої мережі та має вихід у Інтернет	Менеджер Адміністратор
Робоче місце бухгалтера	Робочий комп’ютер бухгалтера забезпечений підключенням до корпоративної мережі та має доступ до Інтернету	Адміністратор, Бухгалтер
Сервер контролю доступу	Відокремлений сервер для забезпечення потреб контролю доступу та сигналізацій	Адміністратор

Розглянемо загальні рекомендації для побудови системи контролю доступу [8, 9]. Система контролю доступу повинна бути розроблена для контролю та моніторингу доступу гостей, персоналу та іншого персоналу до готелю. Ця система повинна включати централізовану базу даних, яка зберігає інформацію про кожного гостя, співробітника та інший персонал, включаючи їх контактну інформацію, призначення кімнат, права доступу тощо.

Система автентифікації повинна бути реалізована, щоб гарантувати, що лише авторизований персонал може отримати доступ до приміщень готелю. Ця система повинна включати засоби біометричної автентифікації, такі як сканування відбитків пальців або розпізнавання обличчя, щоб перевірити особу кожної особи, яка намагається потрапити в готель.

Пристрої контролю доступу, такі як зчитувачі карток або клавіатури, повинні бути встановлені на всіх входах і виходах з готелю, щоб обмежити вхід і вихід на основі попередньо визначених правил і норм, встановлених адміністрацією. Ці пристрої також мають бути інтегровані з системою автентифікації для додаткової безпеки [10].

Камери відеоспостереження повинні бути встановлені на всіх входах і виходах з готелю, а також у зонах загального користування, таких як вестибюлі, коридори тощо, щоб контролювати будь-яку підозрілу діяльність у приміщеннях.

Слід запровадити систему звітності, щоб відстежувати будь-які несанкціоновані спроби проникнення в готель або будь-яку підозрілу діяльність у його приміщеннях. Ця система повинна надавати сповіщення в реальному часі щоразу, коли буде виявлено інцидент, щоб можна було негайно вжити відповідних заходів [11].

Система автентифікації готелю повинна відповідати наступним вимогам [12-14]:

– безпека;

– повинна працювати швидко та ефективно, щоб не викликати затримок для користувачів та працівників готелю;

– повинна бути надійною та стійкою до витоку інформації та інших загроз;

– мати можливість розширення та зміни залежно від потреб готелю;

– бути простою та зручною для використання для всіх користувачів готелю;

– бути сумісною з іншими системами, що використовуються в готелі, наприклад системою управління бронюванням номерів;

– повинна зменшувати кількість адміністративних завдань для працівників готелю.

1.4 Постановка задачі

Для вирішення поставленої мети кваліфікаційної роботи потрібно провести комплексний безпековий аналіз фізичної та інформаційної структури готельного комплексу "Колізей". Результати аналізу мають бути використані для розробки індивідуальної системи захисту інформації, яка забезпечує безпечне функціонування готелю відповідно до його комерційного призначення. Отже, на підставі теоретичної інформації та результатів первинного дослідження об’єкту захисту та інформаційної структури, ми визначили перелік вимог до системи контролю доступу готельного комплексу «Колізей»:

– система повинна захищати об’єкт, його інформаційні ресурси, інформаційні сховища, працівників та клієнтів від найбільш імовірних загроз зсередини та ззовні;

– система повинна містити засоби відеоспостереження, моніторингу та реагування, які негайно сповіщатимуть персонал про виникнення загроз на території готельного комплексу або в його інформаційному просторі;

– система повинна бути розроблена на основі наявних елементів, комп’ютеризованих робочих місць та інформаційних відносин, доповнюючи їх, але не змінюючи радикально;

– система повинна бути захищеною та не виходити з ладу навіть за аварійних умов в готелі;

– система має бути максимально невидимою для клієнтів, але не втрачати ефективності та надійності при цьому;

– система повинна бути економічно доцільною, доступною для повного розгортання та простою для використання персоналом.

Відповідно до цих вимог, ми розробимо систему контролю доступу готельного комплексу «Колізей».

2 РОЗРОБКА КОМПОНЕНТІВ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

2.1 Обгрунтування об’єктів захисту

Необхідно провести детальний аналіз структури та вивчити інформаційні процеси, включаючи суб’єктів та канали зв’язку. Основою для нашого аналізу будуть результати досліджень інформаційної та фізичної структури підприємства, які були проведені в першому розділі.

Захист інформації передбачає комплекс заходів, які мають на меті запобігти витоку, розкраданню, втраті, несанкціонованому знищенню, спотворенню, модифікації, підробці, несанкціонованому копіюванню, блокуванню інформації та іншим загрозам [10, 15].

Окрім цього, для проведення аналізу структури підприємства необхідно визначити дві основні категорії персоналу:

– працівники, які здійснюють роботу з клієнтами та адміністративне керування комплексом (до цієї крупи відносяться менеджери та бухгалтери);

– працівники, які займаються технічною роботою та обслуговуванням систем готелю (до цієї групи відносяться охоронці, прибиральники, кухарі та садівники).

Ці дві категорії персоналу відрізняються своєю роботою та повсякденними обов'язками.

Розглянемо характеристики для кожної з цих груп персоналу, з метою визначення необхідних повноважень представників цих груп, ресурсів та приміщень, з якими вони взаємодіють та занесемо їх у таблиці 2.1 та 2.2

Таблиця 2.1 - Працівники, які здійснюють роботу з клієнтами та адміністративне керування комплексом

Можливості	Представники груп	Повноваження
Збір персональних даних від клієнтів та їх реєстрація в інформаційній системі	Менеджери	Взаємодія з клієнтами з метою збору їх персональних даних та отримання доступу до робочого місця на стійці реєстрації
Обробка персональних даних клієнтів	Всі	Одержання та обробка персональних даних клієнтів з доступом до комп'ютеризованих робочих місць
Отримання доступу до фінансових рахунків, звітів та інформації про надходження, витрати, податки та інші бухгалтерські документи	Бухгалтери	Можливість доступу до комп'ютеризованих робочих місць та ресурсів готелю, таких як банківські, податкові, бухгалтерські тощо, включаючи Інтернет
Отримання поточної інформації про стан справ у готелі, зокрема про проживання клієнтів, терміни перебування та стан оплати	Всі	Можливість доступу до комп'ютеризованих робочих місць та інших інформаційних ресурсів готелю, зокрема до персональної інформації клієнтів
Управління бронюванням кімнат та підтримка зв’язку з постійними та потенційними клієнтами	Адміністратор Менеджери	Можливість доступу до комп'ютеризованих робочих місць та Інтернету

Таблиця 2.2 - Працівники, які займаються технічною роботою та обслуговуванням систем готелю

Можливості	Представники груп	Повноваження
Проведення робіт з підтримки чистоти та порядку у номерах готелю	Прибиральник	Доступ до готельних номерів
Дозвіл на використання кухні та інших приміщень, призначених для приготування та подачі їжі клієнтам	Прибиральник, кухар	Фізичний доступ до кухонних та інших приміщень, пов’язаних з харчуванням
Користування готельною територією, включаючи будівлі та приміщення для службового використання	Всі	Можливість доступу до службових приміщень готельного комплексу, а також до систем, ресурсів, інструментів тощо
Дозвіл на користування матеріально-технічною та ресурсною базою готелю	Всі	Можливість доступу до систем готелю згідно своїх професійних повноважень

Проаналізувавши інформацію з таблиць, зробимо висновок, що основними повноваженнями працівників, які займаються роботою з клієнтами та адміністративним управлінням готельним комплексом, є комунікація з клієнтами та доступ до їх персональних даних, доступ до внутрішніх інформаційних ресурсів готельного комплексу та систем фінансового моніторингу та звітності через систему Інтернет.

У свою чергу, працівники, які займаються технічною роботою та обслуговуванням систем готелю, мають фізичний доступ до приміщень готелю,

включаючи готельні номери клієнтів, а також можливість використання профільного готельного матеріально-технічного забезпечення. При розробці системи контролю доступу готелю необхідно враховувати ці повноваження.

Необхідно виділити чергового адміністратора, який має повну відповідальність за контроль за оперативною обстановкою в закладі, діями іншого персоналу, клієнтів та реагування на не штатні ситуації. Як ми бачимо, його повноваження є найширшими, оскільки він може отримувати доступ до будь-яких службових приміщень готелю та обробляти необхідні персональні дані клієнтів і працівників.

Хоча адміністратор має багато повноважень, їх необхідно контролювати, щоб уникнути порушення безпеки інформації. Всі дії адміністратора повинні бути фіксовані, наприклад, за допомогою системи логування [16, 17]. Крім того, вони повинні бути необхідними та виправданими відповідно до ситуації.

Також варто врахувати роль клієнтів у функціонуванні готелю, оскільки вони можуть виступати як порушники, так і об’єкти загрози. Враховуючи ці фактори, розробка системи контролю доступу готельного комплексу повинна включати заходи з контролю за діями адміністратора та іншого персоналу, а також механізми захисту персональних даних клієнтів та інших конфіденційних інформаційних ресурсів.

Для того, щоб готельний комплекс зміг здійснювати свою діяльність, обробка персональних даних є необхідною, тому клієнт повинен дати згоду на їх збір та обробку, або відмовитися від користування послугами готелю. Клієнт має право вимагати переліку інформації, яка стосується його персональних даних, що збирається та використовується готельним комплексом, а також вимагати їх припинення або повного видалення [18].

Крім того, клієнт повинен вчасно та в повній мірі оплатити отримані послуги відповідно до умов договору. Він має право на фізичний доступ до готельного номеру та його ресурсів, а також на гарантії безпеки, конфіденційності проживання та контролю доступу до визначеного готельного номеру. Клієнт може використовувати публічні локації на території готельного

комплексу та гостьові складові інформаційних мереж готелю для задоволення своїх потреб згідно з умовами підписаного договору.

Наскільки важливо забезпечити безпеку інформації в готельному комплексі "Колізей", ми можемо визначити, враховуючи характеристики його структурних елементів та виділивши об'єкти критичної інформаційної структури.

Згідно з законодавством України, такі об'єкти - це комунікаційні або технологічні системи, на які можуть вплинути кібератаки, що призведуть до зупинки діяльності комплексу [19, 20]. Для розробки системи захисту інформації готельного комплексу "Колізей" ми визначимо критичні об'єкти як інформаційні ресурси, порушення цілісності, конфіденційності або доступності функціонування яких можуть призвести до повної зупинки діяльності комплексу, безпосередньої загрози цій зупинці та значних фінансових, ресурсних або репутаційних збитків. Серед критичних об'єктів інформаційної структури готелю першочергово необхідно віднести комп'ютеризовані робочі місця, корпоративну мережеву систему, центральний сервер та системи моніторингу, зокрема систему відеоспостереження, протипожежну систему, які безпосередньо впливають на професійну діяльність персоналу.

На підставі цього ми визначимо об'єкти захисту готельного комплексу "Колізей". Отже, враховуючи перелічені критичні складові інформаційної структури готелю, до об'єктів захисту належать:

– територія готелю, включаючи службові приміщення та готельні номери;

– особиста інформація клієнтів та працівників готелю;

– фінансова інформація готелю, включаючи бухгалтерський облік, електронний та паперовий документообіг;

– інформація, що зберігається на комп'ютеризованих робочих місцях персоналу;

– інформація, яка пересилається по корпоративній мережевій системі готелю.

Керуючись цим, ми переходимо до дослідження та класифікації інформаційних потоків об'єкту захисту

2.2 Створення моделі загроз та моделі порушника, на основі проаналізованих даних

Щоб створити модель загроз на основі результатів аналізу структури готельного комплексу, проведемо дослідження інформаційних потоків готелю та класифікуємо їх за суб'єктами, що їх ініціюють [21, 22]. Для зручності можна виділити наступні групи інформаційних процесів за їх ініціаторами:

– інформаційні процеси, здійснювані персоналом готелю, такі як процес реєстрації нового клієнта, використання комп’ютеризованих робочих місць та внутрішньої автоматизованої інформаційно-комунікаційної мережевої системи;

– інформаційні процеси, здійснювані клієнтами, такі як використання гостьових інформаційних ресурсів;

– інформаційні процеси, здійснювані третьою стороною.

Для побудови моделі загроз необхідно проаналізувати ці інформаційні процеси та визначити можливі загрози для їх безпеки.

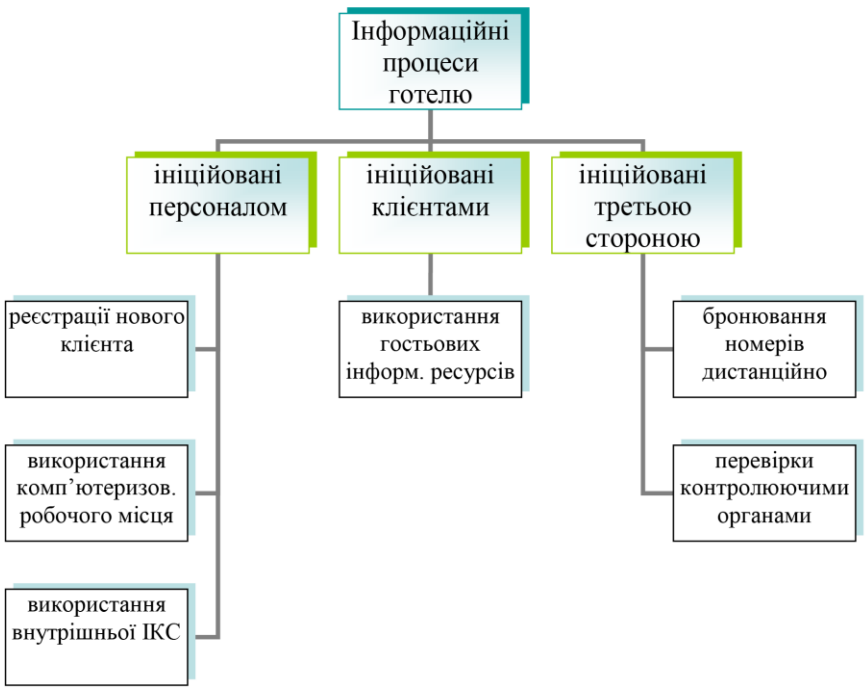


Рисунок 2.1 – Структура інформаційних процесів готелю

На основі виділених інформаційних процесів можна скласти загальну схему інформаційних потоків готельного комплексу [23]. Схема включає такі елементи:

– клієнти готелю, які ініціюють інформаційні процеси, такі як бронювання номерів, взаємодія з персоналом готелю тощо;

– внутрішня автоматизована інформаційно-комунікаційна мережева система, яка забезпечує обмін інформацією між різними відділами готелю, такими як бухгалтерія, кадри, ресторани, прибирання номерів тощо;

– комп'ютеризовані робочі місця персоналу, які використовуються для обробки даних, бронювання номерів, реєстрації клієнтів, управління запасами тощо;

– система електронного документообігу, яка забезпечує обробку документів в електронному вигляді, таких як договори, рахунки, звіти тощо;

– комунікація з клієнтами: персонал готелю може зв'язуватися з клієнтами через електронну пошту, телефон або систему повідомлень в гостьовій кімнаті;

– облік використання готельних послуг: інформація про використані послуги (наприклад, ресторан, сауна, масаж) також зберігається в інформаційній системі готелю;

– обмін даними між різними відділами готелю: інформація про бронювання, послуги, фінансові операції та інші деталі можуть передаватися між різними відділами готелю для координації роботи;

– інформаційна безпека: на різних етапах обробки та передачі інформації можуть бути використані заходи захисту даних, щоб запобігти несанкціонованому доступу до конфіденційної інформації;

– інші інформаційні системи, які можуть використовуватися готельним комплексом, наприклад, системи відеоспостереження, системи автоматизованого управління кондиціонерами тощо.

Список ключових інформаційних процесів, що були виділені на момент проведення дослідження, є базовим для створення системи захисту інформації. Проте при більш детальному вивченні можуть бути виявлені десятки інших процесів. Важливо враховувати, що з розвитком готельного комплексу можуть з'являтися нові процеси. На основі виділених ключових процесів можна скласти схему інформаційних потоків комплексу (рис 2.2).

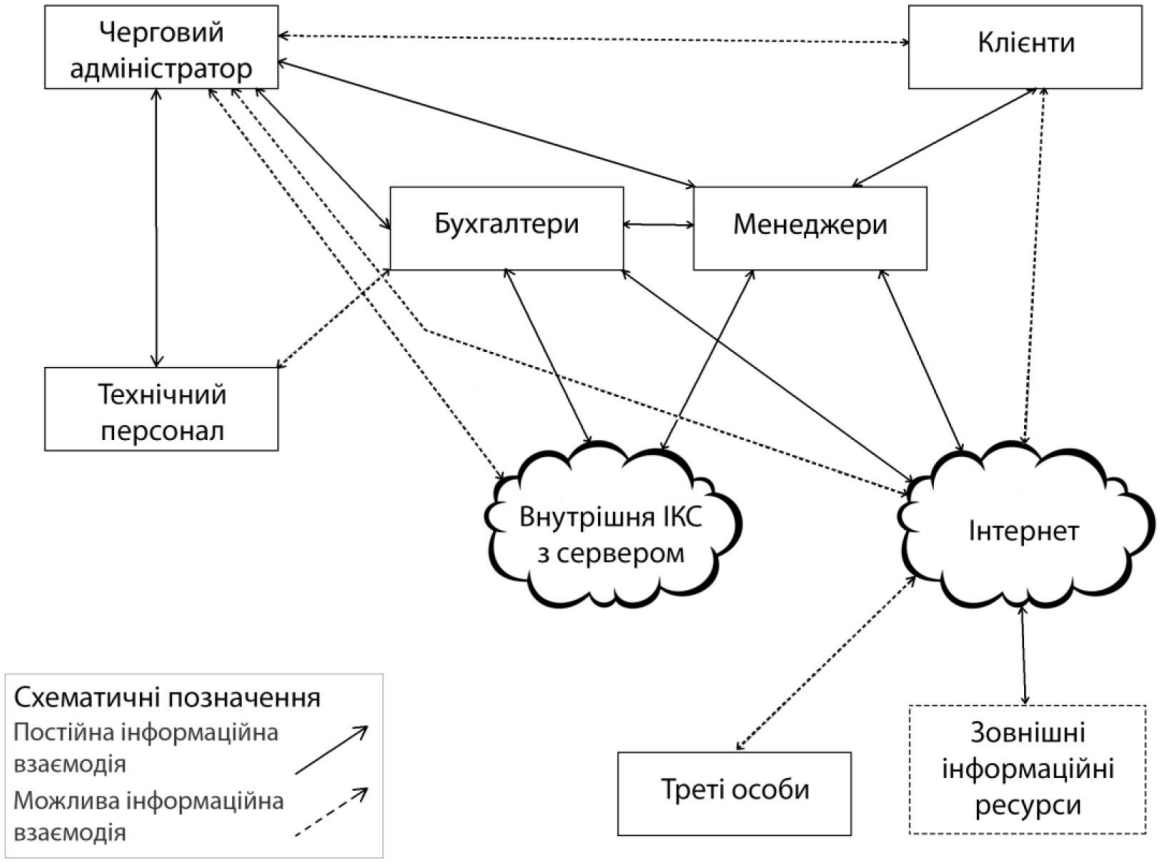


Рисунок 2.2 - Схема інформаційних потоків готельного комплексу

У цій схемі інформаційні потоки рухаються в обидві сторони між різними елементами системи. Наприклад, клієнти готелю можуть взаємодіяти з персоналом готелю через внутрішню автоматизовану інформаційно-комунікаційну мережеву систему, яка забезпечує обробку запитів і заявок клієнтів. Оновлення та розвиток системи: з часом готельний комплекс може розширюватися або додавати нові послуги, що можуть призвести до зміни потоків інформації.

В загальному, моделювання загроз застосовується в різноманітних системах організацій, таких як бізнес-процеси, інформаційні системи, розподілені підсистеми, мережева інфраструктура, додатки та сервіси [24]. Модель загроз може включати наступні елементи:

– опис, або архітектуру, модель критичних ресурсів інформаційної системи;

– список рекомендацій, що можуть бути перевірені або оскаржені в майбутньому;

– список потенційних загроз системи;

– список дій, що необхідно вжити для усунення зазначених загроз;

– стратегію тестування та перевірки успішності вжитих заходів.

Ми можемо побудувати модель загроз у вигляді таблиці, використовуючи дані, які були отримані в результаті попередніх досліджень.

Необхідно створити повний та деталізований перелік суттєвих загроз, що включає визначення спрямованості, джерела, механізму реалізації та можливих наслідків для кожної загрози. Також необхідно врахувати на які властивості інформації або інформаційно-технічної системи (ІТС) спрямована загроза, зокрема [21, 24]:

– конфіденційності (К), що включає несанкціоноване ознайомлення з інформацією;

– цілісності (Ц), що включає несанкціоновану модифікацію (спотворення, фальсифікацію, викривлення) інформації;

– доступності (Д), що включає порушення можливості використання ІТС або оброблюваної інформації (відмова в обслуговуванні користувача).

Загрози ІТС, залежать від багатьох факторів, таких як характеристики операційної системи, апаратного забезпечення, програмного забезпечення, фізичного середовища, персоналу, технологій обробки та інших чинників. Ці загрози можуть мати об'єктивну або суб'єктивну природу.

Таблиця 2.3 – Модель загроз готельного комплексу

№	Потенційні загрози для інформації	Ризики для:		
		К	Ц	Д
1	2	3	4	5
1 Загрози зі сторони персоналу				
1.1	Працівники можуть бути компрометовані третіми особами через підкуп або шантаж.	+	+	+
1.2	Нецільова діяльність, яка виходить за рамки повноважень	+	+	+
1.3	Надлишковість повноважень	+	+/-	+/-
1.4	Використання несанкціонованого робочого місця	+	+	-
1.5	Пошкодження ПК або мережевих пристроїв	-	+	+
1.6	Несанкціонована модифікація або пошкодження службової інформації	-	+/-	+/-
1.7	Передача службової інформації, включаючи персональні дані клієнтів та працівників	+	-	-
1.8	Несанкціоноване друкування та копіювання інформації	+	-	-
1.9	Шпигунство, збір персональних даних	+	-	-
2. Загрози зі сторони клієнтів готелю				
2.1	Подання неточних персональних даних	+	+	-
2.2	Використання корпоративних ресурсів, включаючи робочі місця працівників та внутрішню мережу	+	+	+
2.3	Нелегальне перехоплення розмов та відео-моніторинг працівників готелю або інших клієнтів	+	-	-

Кінець таблиці 2.3

1	2	3	4	5
2.4	Злочинне заволодіння внутрішніми документами у паперовому або електронному форматі	+	+/-	+/-
2.5	Нанесення шкоди комп'ютерному, мережевому або IoT обладнанню готелю	+/-	+	+
2.6	Нелегальне проникнення та користування службовими приміщеннями	+/-	+/-	+/-
2.7	Незаконне вторгнення та використання комп'ютерної техніки готелю	+	+	+
3. Загрози зі сторони третіх осіб				
3.1	Несанкціонований вхід на територію готельного комплексу	+	+	+
3.2	Віддалене зчитування оптичної та аудіо інформації	+	-	-
3.3	Неавторизований доступ до внутрішніх інформаційних ресурсів готелю	+	+	+
3.4	DDoS атака	+/-	+	+
3.5	Надмірна кількість спаму та флуду	-	+/-	+

З використанням розробленої моделі загроз ми зможемо аналізувати потенційні загрози та оцінювати рівень шкоди, яка може виникнути від їх реалізації. Це допоможе нам створити комплексну систему захисту інформації для готельного комплексу "Колізей", де будуть враховані всі виявлені загрози.

Варто зазначити, що модель загроз може змінюватись та доповнюватись залежно від розвитку та розширення готельного комплексу, введення нових вакансій, або розширення внутрішніх інформаційних ресурсів. Таким чином, ми будемо постійно моніторити потенційні загрози та вносити необхідні зміни до моделі для забезпечення максимального рівня захисту інформації.

На основі моделі загроз, ми плануємо розробити модель порушника, яка буде включати абстрактний опис можливих дій особи, що може отримати несанкціонований доступ до ІТС засобів готелю. Ця модель буде враховувати різні фактори, такі як мотивація, кваліфікація, можливості та обмеження порушника.

Ми розглянемо ключових суб'єктів, які можуть стати порушниками інформаційної структури готелю, а також потенційних зловмисників з середини та зовнішніх інформаційних загроз. Ми також розглянемо можливість третіх осіб отримати несанкціонований доступ до роботи з включеними до складу ІТС засобами.

При створенні моделі порушника ми дослідимо можливі мотивації та цілі, які можуть вести порушника до злочинних дій, а також оцінимо його кваліфікацію та знання, що дозволить нам прогнозувати його можливості подолати заходи захисту. Ми також врахуємо фізичні та географічні обмеження, а також можливості порушника щодо подолання заходів захисту відповідно до прийнятих специфікацій.

Оцінка загроз, які може створити порушник, допоможе нам розробити систему контролю доступу, яка буде враховувати різні сценарії нападу та можливі загрози. Модель порушника може змінюватись та доповнюватись в процесі діяльності, розвитку та розширення готельного комплексу, при створенні нових вакансій, або при розширенні внутрішніх інформаційних ресурсів.

Порушники поділяються на дві основні групи: зовнішні та внутрішні [25]. Для більш точного аналізу порушників у моделі використовуються усі можливі категорії, ознаки та характеристики, при цьому рівень загрози кожної з них оцінюється за 4-бальною шкалою (табл 2.4).

Таблиця 2.4 – Модель порушника готельного комплексу

№	Порушник	Категорія порушника	Кваліфікація	Мотив	Можливості щодо подолання захисту	Можливості за місцем дії	Можливості за часом дії	Сума загроз
1. Внутрішні порушники, по необережності								
1.1	Адміністратор	ПВ4	К2	М1	З2	Д4	Ч3	15
1.2	Бухгалтер	ПВ3	К2	М1	З2	Д2	Ч3	12
1.3	Менеджер	ПВ3	К2	М1	З2	Д2	Ч3	12
1.4	Технічний персонал	ПВ1	К1	М1	З1	Д3	Ч3	10
2. Внутрішні порушники, з метою отримання вигоди								
2.1	Адміністратор	ПВ4	К2	М3	З2	Д4	Ч3	17
2.2	Бухгалтер	ПВ3	К2	М3	З2	Д2	Ч3	15
2.3	Менеджер	ПВ3	К2	М3	З2	Д2	Ч3	15
2.4	Технічний персонал	ПВ1	К1	М3	З1	Д3	Ч3	12
3. Зовнішні порушники, по необережності								
3.1	Хакер	ПЗ3	К4	М3	З4	Д1	Ч3	18
3.2	Клієнт	ПЗ1	К2	М2	З2	Д1	Ч3	11
3.3	Рекетир	ПЗ3	К1	М3	З1	Д4	Ч4	16
4. Зовнішні порушники, з метою отримання вигоди								
4.1	Хакер	ПЗ4	К4	М4	З4	Д1	Ч4	21
4.2	Клієнт	ПЗ1	К2	М3	З2	Д1	Ч3	12
4.3	Рекетир	ПЗ4	К2	М4	З1	Д4	Ч4	19

Модель порушника, яку ми розробили, дозволяє виявити деякі закономірності. По-перше, зовнішні порушники, такі як хакери та злочинці, становлять найбільші ризики для готелю, особливо якщо вони здійснюють фізичний напад. По-друге, адміністратор, як особа з розширеним доступом до

приміщень готелю, є одним з найбільш вразливих працівників. По-третє, мотивація порушника також має велике значення. Якщо персонал готелю має мало мотиву для порушення безпеки, загрози зменшуються.

Отримані результати досліджень дають змогу класифікувати та пріоритезувати загрози та порушників, а це дає можливість створити систему, з орієнтацією на найбільш пріоритетні загрози, з варіативним бюджетом. Розроблені нами моделі загроз та порушника використовуватимуться при проектуванні системи контролю доступу для готельного комплексу «Колізей».

2.3 Розробка системи фізичного захисту внутрішніх приміщень та контролю периметру

Найперше, ми зосередимося на фізичному захисті території та приміщень готелю, який є важливою складовою захисту інформаційних ресурсів готельного комплексу. Це необхідно через моделі загроз та порушників, які показують, що фізичне вторгнення може серйозно нашкодити або повністю зупинити функціонування готелю.

Що стосується створення системи захисту, то ми маємо перевагу у тому, що готельний комплекс уже має деякі безпекові системи, які можуть бути вдосконалені та оновлені. Наша задача полягає в систематизації та покращенні існуючих засобів захисту, виправленні вразливостей та розробці комплексного підходу до захисту.

Проте, першим негативним фактором, який виявився в існуючій структурі готелю, є відсутність штатного спеціаліста з питань безпеки. Також, охоронці не мають окремого статусу та працюють на рівні технічного персоналу, що потребує уваги та вдосконалення. Ми почнемо з оцінки та зміцнення захисту периметру готелю та вивчення всіх аспектів захисту, щоб забезпечити ефективний захист готельного комплексу в цілому.

Тому ми рекомендували власнику готелю провести реструктуризацію організаційної структури, виокремивши персонал забезпечення безпеки в окрему

категорію та створивши нову професійну вакансію - інженер безпеки. Однак, ще більш оптимальним рішенням було б створення посади керівника відділу безпеки, який би відповідав за розробку та впровадження стратегії захисту, надання консультацій та навчання персоналу, а також координацію роботи всіх відділів, пов'язаних з безпекою (рис. 2.3). Окрім того, необхідно забезпечити професійний рівень роботи зі збереження інформації та забезпечення фізичної безпеки, включаючи навчання персоналу та підвищення їхньої свідомості щодо можливих загроз і вразливостей готелю.

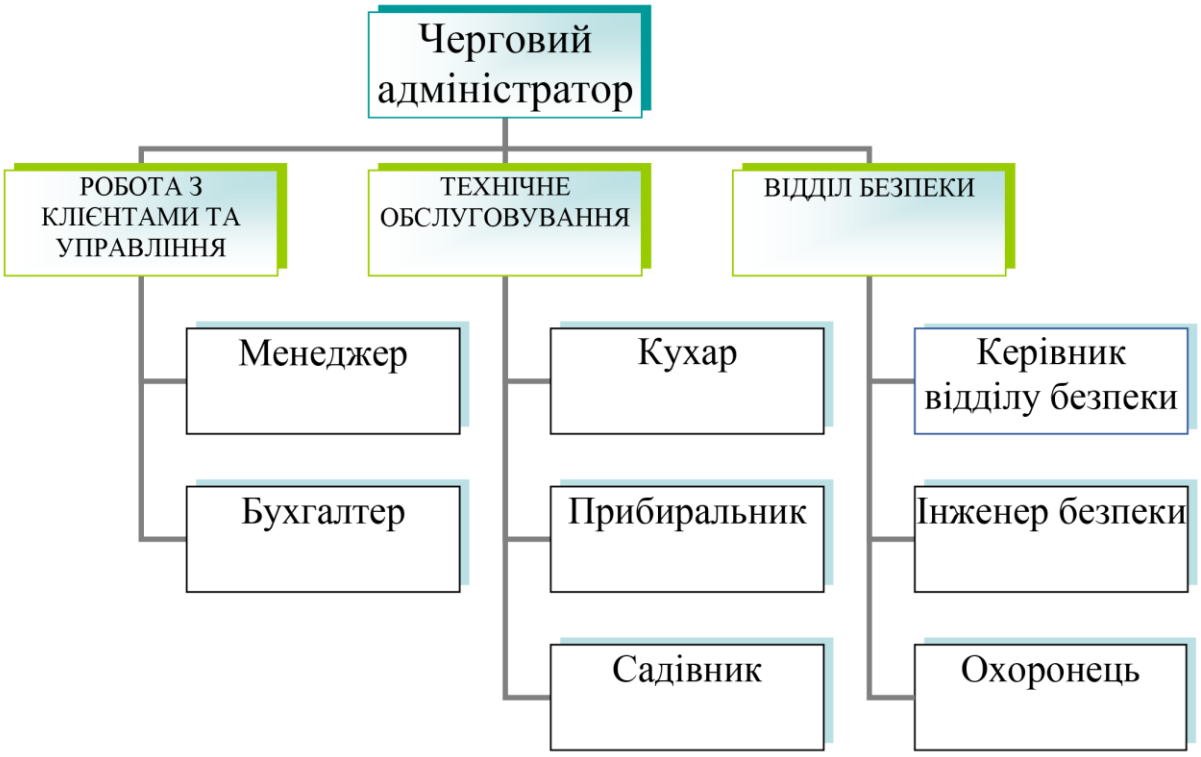


Рисунок 2.3 - Запропонована схема працівників готельного комплексу

Питання щодо необхідності окремої посади керівника відділу безпеки є предметом дискусій. З одного боку, така посада обов'язково повинна з'явитися при розширенні готельного комплексу або збільшенні технічного персоналу. Але на сьогоднішній день, це може стати додатковим фінансовим навантаженням. З іншого боку, окрема посада для інженера безпеки потрібна негайно. Це пояснюється тим, що нормальний рівень безпеки можливий лише при

постійному моніторингу стану систем контролю, записів та логів, а це потребує професійної роботи спеціаліста.

Для успішного впровадження будь-яких новітніх систем програмного, апаратного та іншого захисту, необхідний подальший супровід у експлуатації, який може бути забезпечений лише за умови роботи кваліфікованого спеціаліста.

Першою ключовою умовою для створення системи контролю доступу є реструктуризація організаційної структури готельного комплексу.

Щодо захисту території, слід відзначити, що це потребує рівносильних силових дій з боку персоналу закладу для протидії фізичним силовим діям порушника. Існує безліч можливих варіантів розвитку подій, таких як непомітне проникнення порушника на територію готелю, проникнення під виглядом клієнта, відкритий силовий напад або групова атака на готельний комплекс, захоплення заручників, обстріл з прилеглих ділянок, використання індивідуальної стрілецької зброї, ручних гранатометів, снайперських гвинтівок тощо. Важливо пам'ятати, що всі ці дії є незаконними, багато з них відносяться до особливо тяжких злочинів та можуть мати ознаки тероризму [26].

Готельний комплекс, як будь-який інший заклад, підприємство або організація, не можуть повністю захистити себе від терористичних атак самостійно. Створення силових структур в межах відділу безпеки готелю, які можуть дати реальну відсіч терористичним атакам, є непрактичним і вкрай важким з точки зору законності та витрат на створення та підтримання.

Найбільш оптимальним і доступним за ціною методом фізичного захисту інформації та матеріально-технічних ресурсів готельного комплексу є укладання договору з охоронною компанією, яка надає послуги з фізичного захисту. Інтеграція в технічні системи захисту готелю тривожних кнопок та сповіщення охоронної структури є необхідною, щоб забезпечити швидке реагування та адекватну відповідь на загрози.

Поліція охорони, Національної поліції України, є однією з кращих охоронних структур для захисту готельних комплексів. Використання послуг професійної охоронної структури забезпечує надійний рівень захисту при

надзвичайних ситуаціях та гарантує швидке реагування та адекватний супротив порушникам.

Крім договору з охоронною структурою, комплексна система захисту інформації повинна включати системи моніторингу та сповіщення, щоб персонал міг вчасно реагувати на потенційні загрози.

Щоб запобігти або ускладнити несанкціонований доступ потрібно встановити камери відеоспостереження. Їх розміщення має бути здійснене з урахуванням сліпих зон, які можуть бути використані для проникнення на територію готельного комплексу. З огляду на фізичну структуру комплексу, найбільш вразливою ділянкою є східна частина, де готель розташований неподалік від межі території. Східний напрямок має найвищий пріоритет для встановлення камер відеоспостереження, за ним слідують південний та північний напрямки, де фланги будівлі також наближаються до межі території. Оскільки територія комплексу велика, для забезпечення повного покриття всієї території камерами відеоспостереження знадобиться значна кількість камер. Розробляється план розстановки IP-камер, що враховує критично-необхідні камери та камери, встановлення яких можливе в середньо-тривалій перспективі, коли з'являться вільні кошти [27, 28].

IP Video System Design Tool є програмою, що допомагає встановлювати оптимальну кількість та розміщення камер для проектування відеоспостереження [29]. Під час розрахунків важливо визначити кути та зони огляду, щоб уникнути "мертвих" зон. Програма також допомагає оцінити навантаження на локальну мережу, якщо використовуються IP камери. Це дозволяє зекономити час і не виїжджати на об'єкт для проведення розрахунків. IP Video System Design Tool є досить простою у використанні, але містить достатньо основних функцій для ефективного проектування та планування систем відеонагляду. Використовуючи це спеціалізоване програмне забезпечення, розробимо схему розміщення камер відеоспостереження (рис 2.4).

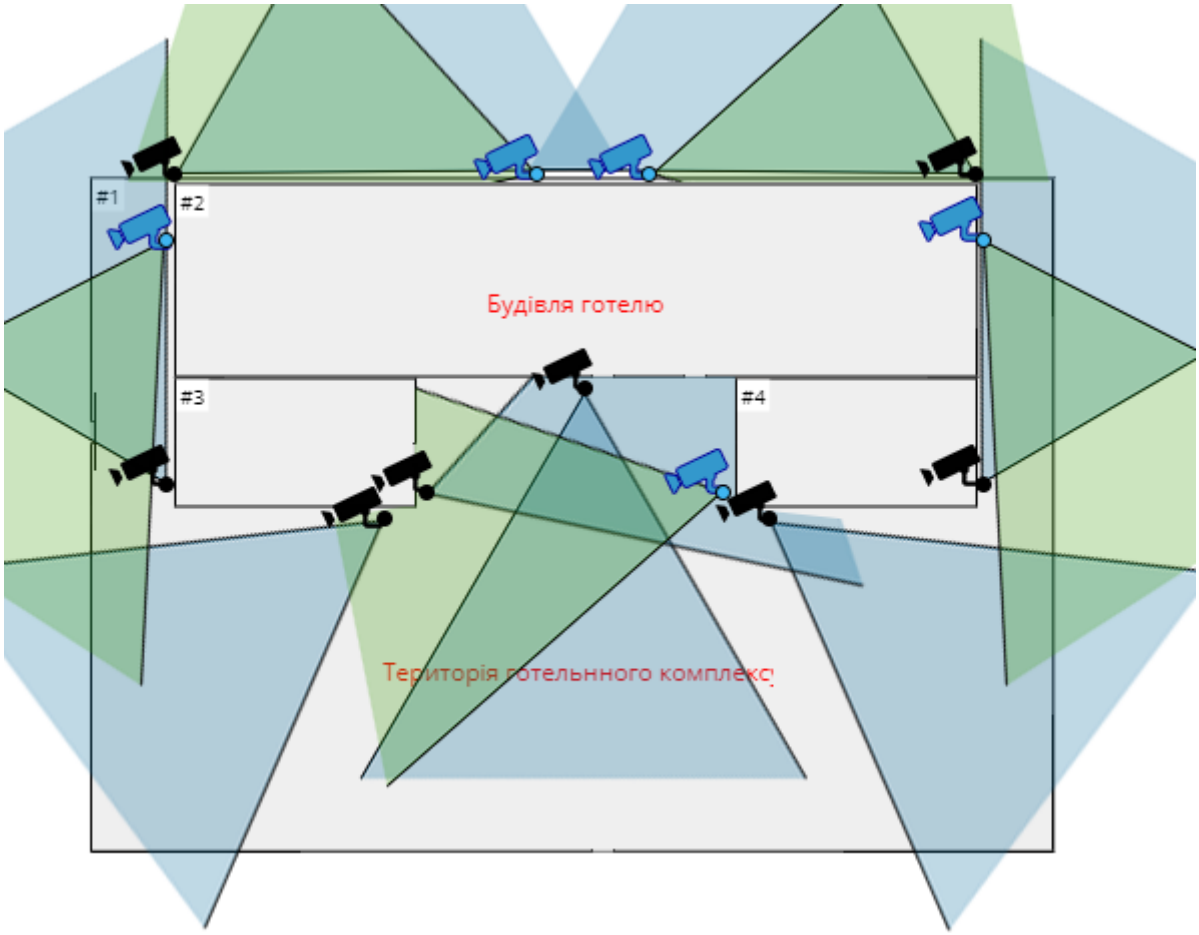


Рисунок 2.4 - Схема розміщення камер відеоспостереження на території готельного комплексу

На схемі позначено 13 камер відеоспостереження, які розташовані з урахуванням критеріїв необхідних для ефективного моніторингу території. З цих 13 камер 8 камер розташовані таким чином, щоб забезпечити більш-менш надійний моніторинг території готельного комплексу. Інші 5 камер розташовані в стратегічних місцях для повного перекриття всіх сліпих зон, перехресного спостереження найбільш небезпечних напрямків та забезпечення найкращого моніторингу. Крім того, ще одна камера буде розташована на ресепшені, для забезпечення контролю за вхідними воротами, а ще одна камера буде

встановлена на вході в адміністративне приміщення для забезпечення безпеки працівників та контролю доступу до важливих приміщень.

Такий розподіл камер відеоспостереження є критично важливим для забезпечення безпеки готельного комплексу, оскільки забезпечує покриття всіх найбільш вразливих ділянок, контроль доступу та реагування на небезпечні ситуації.

Ми обрали IP-камери Hikvision DS2CD2121G0-IS(C) для відеоспостереження, оскільки вони мають кут огляду 60 градусів та інфрачервону підсвітку, що дозволяє забезпечити надійне відеоспостереження на відстань до 30 метрів (рис 2.6). Ці камери є надійними та призначеними для використання на вулиці, що робить їх ідеальними для нашого відеоспостереження [30, 31].

Крім того, вони належать до середньої цінової категорії, що робить їх більш доступними з точки зору вартості в порівнянні з деякими іншими моделями на ринку. Використання цих камер не повинно створювати серйозних проблем на будь-якому етапі встановлення та експлуатації, що забезпечить ефективну та безперебійну роботу відеоспостереження нашого готельного комплексу.

Рисунок 2.5 – IP-камера Hikvision

Для ефективного моніторингу відеоряду з 13 камер, необхідно мати два широкоформатних монітора з діагоналлю не менше 27 дюймів. Це дозволить охоронцям більш комфортно спостерігати за подіями на території комплексу та забезпечити швидке реагування на небезпечні ситуації.

Рисунок 2.6 – Зображення з камери у приміщенні

Недостатнє число охоронців - це серйозна проблема для забезпечення безпеки на об’єкті. Рекомендується розширити штат охоронців, щоб забезпечити цілодобовий моніторинг та забезпечити максимальний рівень безпеки для персоналу та майна комплексу. Крім того, додаткові охоронці можуть займатися реагуванням на небезпечні ситуації, що значно зменшить час реакції та ризики для безпеки.

Для зберігання відеоматеріалу з камер необхідно мати відео-реєстратор з достатньою пропускною здатністю, що дозволяє опрацьовувати відео-сигнал з кількох камер одночасно в реальному часі. В даному випадку рекомендується придбати реєстратор Hikvision DS-7616NI-I2/16P, який здатен працювати з 16 камерами одночасно та забезпечувати запис відеоматеріалу ємністю до 8 Тб (рис. 2.7) [32].

Рисунок 2.7 – Мережевий відеореєстратор Hikvision

Це дозволить зберігати записи відеоматеріалів на досить тривалий період часу. Наприклад, якщо врахувати, що наш об'єкт потребує цілодобового відеоспостереження, то така ємність буде достатньою на декілька днів запису без перезапису старих матеріалів. Також слід врахувати, що для зручності перегляду відеоматеріалів на більшу кількість днів, необхідно регулярно виконувати резервне копіювання записів на зовнішні носії інформації, наприклад, на жорсткий диск.

Для додаткового забезпечення безпеки системи відеоспостереження можна розглянути використання хмарного сховища для збереження відеоматеріалів. Проте, це може призвести до певних ризиків, пов'язаних зі збільшенням навантаження на канал інтернет-з'єднання та можливістю віддаленого злому системи відеоспостереження. Тому на даний момент ми не будемо використовувати цей метод.

Ефективнішим рішенням є фізичне відключення системи відеоспостереження від мережі Інтернет, або її відмежування від інших інформаційних ресурсів готельного комплексу за допомогою створення режимних зон та їх чіткого відмежування. Це не вплине на функціональність системи відеоспостереження, проте максимально зменшить можливість

недобросовісного втручання у її роботу з боку сторонніх осіб, включаючи клієнтів готелю.

Врахування цих аспектів при розробці інформаційно-комунікаційної мережі готельного комплексу дозволить створити більш надійну та безпечну систему відеоспостереження.

На території готельного комплексу можна відрізнити різні зони з різним рівнем доступу та охорони. До режимних зон можна віднести ті, які містять:

– робочі приміщення персоналу, зокрема кімнати з комп’ютеризованими робочими місцями менеджерів, бухгалтерів та адміністратора, оскільки вони містять важливу інформацію про готельний комплекс та його гостей;

– господарські приміщення, в тому числі ті, що використовуються для зберігання матеріально-технічної бази, яка може бути привабливою для зловмисників;

– ділянки з підвищеним травматичним ризиком, які можуть становити небезпеку для гостей та персоналу готельного комплексу.

Для забезпечення безпеки в режимних зонах необхідно встановити системи контролю доступу, використовувати камери відеоспостереження та інші заходи з фізичного та технічного захисту. Важливо також навчати персонал готельного комплексу правилам безпеки та контролювати їх виконання.

Обмеження доступу до вказаних приміщень має на меті різні цілі. З одного боку, це допомагає попередити можливі травми чи пошкодження майна клієнтів та готелю, що є важливим для збереження репутації та підтримки безпеки готелю. З іншого боку, обмеження фізичного доступу до приміщень допомагає запобігти витоку інформації та комп'ютерним зламам, що може викликати серйозні наслідки для бізнесу та безпеки клієнтів. Крім того, обмеження доступу допомагає попередити можливі порушення з боку персоналу та фіксувати переміщення осіб на території готелю, що сприяє забезпеченню безпеки та підвищенню ефективності внутрішніх перевірок та розслідувань.

IP-замки, що працюють з картками радіо-частотної ідентифікації (RFID-картки), є ефективним рішенням для забезпечення вимог безпеки та контролю

доступу в готельному комплексі [33]. Особливо цікавою є можливість інтеграції таких замків з внутрішньою мережевою інформаційно-комунікаційною системою готелю, що дозволяє забезпечити більш високий рівень безпеки та контролю доступу. Важливо зазначити, що обладнання з RFID-модулями доступне за різною ціновою категорією та має різні конструкції та різновиди.

Порівняльний аналіз замків дозволяє обрати найбільш оптимальний варіант, яким є дверний RFID-модуль ORBITA E3041 (рис. 2.8) [34]. Цей модуль має високу надійність та стійкість до зовнішніх факторів, простий у використанні та може працювати як в мережевому так і в автономному режимі. Такий замок забезпечує високий рівень безпеки та контролю доступу, що є дуже важливим для готелю як для місця проживання клієнтів, так і для забезпечення безпеки майна та персоналу готелю.

Рисунок 2.8 - Мережевий дверний замок ORBITA E3041

Цей замок може функціонувати у двох режимах - мережевому та автономному. У мережевому режимі, він може з’єднуватися з сервером через Wi-Fi маршрутизацію та передавати інформацію про відкриття дверей, включаючи ідентифікатор ключ-карти та час відкриття.

Встановлення цих замків на входах та виходах з режимних зон, разом з відеоспостереженням, забезпечить високий рівень безпеки та обмежить доступ до цих зон. Крім того, система зможе відслідковувати стан справ в режимі реального часу та реагувати на можливі порушення. Обраний замок ORBITA E3041 є найбільш оптимальним варіантом за результатами порівняльного аналізу, оскільки він є доступним за ціною, зручним для інтеграції з інформаційно-комунікаційною системою готелю та простим у експлуатації.

У готельному комплексі є п'ять дверей, які потребують встановлення IP-замків, а саме: двері в адміністративну кімнату, кухонні приміщення, дві двері в підвал та двері в технічно-підсобне приміщення. Також, необхідно встановити такий механізм захисту на вхід до серверної кімнати. Важливо зауважити, що встановлення подібних замків на двері готельних номерів є рекомендованим, що забезпечить безпеку клієнтів та збільшить їхню зручність. Всього в готельному комплексі є 17 номерів. Встановлення IP-замків на всі ці двері забезпечить контроль над доступом до різних приміщень та номерів, дозволить обмежити доступ до неавторизованих осіб та забезпечить безпеку готельного комплексу в цілому.

Для ефективної роботи систем безпеки, які були описані раніше, а також інших систем, що вже розгорнуті в готельному комплексі, необхідно мати спеціально обладнану серверну кімнату. Україна має нормативні документи, що встановлюють вимоги до таких кімнат, наприклад, наказ Державної служби з надзвичайних ситуацій України. Ці вимоги повинні дотримуватись, щоб забезпечити надійність та стабільність роботи систем.

2.4 Висновки

Ми провели детальний аналіз структури готельного комплексу та визначили складові критичної інформаційної інфраструктури, які потребують особливої уваги щодо захисту. Також було виконано класифікацію інформаційних потоків та складені схеми інформаційних процесів готелю. На основі цих даних була розроблена модель інформаційних порушень, в якій були враховані можливі джерела загроз та модель порушника з урахуванням його мотивації та кваліфікації. За результатами аналізу, найбільша загроза серед персоналу становить черговий адміністратор, а серед зовнішніх порушників - хакер. Їх рівень загрози залежить від ступеню мотивації. Ці дані дали можливість розробити ефективні заходи захисту та запобігти можливим інформаційним порушенням

Згідно розглянутого в розділі, готельний комплекс «Колізей» є значною будівлею, яка потребує системи безпеки для захисту від різних загроз, включаючи злочинні вторгнення, викрадення даних та інші подібні ризики.

Для забезпечення безпеки готельного комплексу пропонується використовувати, систему контролю доступу та інші, яка можуть забезпечити захист від різних видів загроз.

Встановлення всіх рекомендованих систем забезпечення безпеки в готельному комплексі може дозволити не тільки зменшити ризики вторгнень та інших подібних загроз, але також покращити якість обслуговування для клієнтів.

Відповідно, використання сучасних технологій і систем захисту може значно підвищити безпеку та якість обслуговування в готельному комплексі та забезпечити захист від різних загроз.

Важливо також навчати персонал готельного комплексу правилам безпеки та контролювати їх виконання.

Встановлення розглянутої системи контролю доступу допоможе значно підвищити рівень безпеки в готельному комплексі «Колізей» та запобігти багатьом потенційним загрозам, які ми визначили у нашій моделі інформаційних

загроз. Проте, для того, щоб системи функціонували належним чином, потрібно правильно спроектувати та налаштувати інформаційно-комунікаційну систему, і ми маємо перейти до цього етапу.

3 ОЦІНКА ФУНКЦІОНАЛЬНИХ ХАРАКТЕРИСТИК СИСТЕМИ

3.1 Проектування захищеної корпоративної мережевої системи готелю

Однією з важливих складових системи контролю доступу в готельному комплексі є безпека комп'ютеризованих робочих місць персоналу. Для забезпечення елементарного рівня безпеки необхідно встановити антивірусну програму на всі робочі місця без винятку. Вірусна загроза є однією з найбільш критичних для будь-якої інформаційної системи, тому встановлення спеціалізованих програм-антивірусів є базовим заходом для її захисту.

Порівнявши різні антивірусні програми, було обрано ESET для встановлення на всі комп'ютеризовані робочі місця персоналу. Ця програма демонструє високий рівень захисту від вірусів, шпигунського ПО та інших загроз, що можуть виникати в кіберпросторі [35].

Важливо також пам'ятати, що належне функціонування антивірусної програми залежить від її налаштувань, регулярного оновлення баз даних та вчасного реагування на попередження про загрози. Тому необхідно забезпечити відповідну підтримку та обслуговування програми в рамках системи контролю доступу в готельному комплексі.

Для забезпечення безпеки мережі, необхідно авторизувати всіх користувачів, що мають доступ до неї. У рамках нашої комплексної системи захисту інформації в готелі, ми будемо використовувати корпоративну політику паролів. Ми вважаємо, що кожен співробітник готелю має працювати тільки зі свого персонального робочого місця, за винятком менеджерів та адміністраторів, які можуть працювати з робочого місця на ресепшені. Доступ до робочих місць буде обмежено за допомогою стандартних засобів операційної системи Windows, яка встановлена на робочих місцях. Кожен користувач зможе знати лише пароль від свого робочого місця.

Проте, зважаючи на те, що паролі можуть застарівати та бути складними для керування, ми впровадимо програмний комплекс 1Password [36]. Це

дозволить полегшити та автоматизувати процес управління паролями, а також забезпечить зручність для інженера забезпечення безпеки та співробітників готелю.

1Password - це програма для управління паролями та іншими конфіденційними даними. Вона пропонує широкий спектр функціональних можливостей, що роблять її однією з найкращих програм у своєму класі. Деякі з переваг та функціоналу 1Password включають:

– всі дані зберігаються в зашифрованому вигляді, за допомогою сильного шифрування AES-256;

– програма автоматично заповнює паролі та інші дані веб-сайтів, що збережені в базі даних 1Password, що робить використання веб-сайтів більш зручним та ефективним;

– дозволяє синхронізувати дані між різними пристроями, що дозволяє отримати доступ до паролів та інших даних з будь-якого місця та на будь-якому пристрої;

– може генерувати складні та надійні паролі для веб-сайтів, що зберігаються в базі даних 1Password;

– може зберігати не тільки паролі, але й інші конфіденційні дані, такі як номери кредитних карт, адреси, номери соціального страхування та інші.

– програма дозволяє відстежувати рівень безпеки паролів та інших даних, та попереджує користувача, якщо дані вважаються недостатньо безпечними.

Завдяки використанню програмного комплексу 1Password, працівники зможуть використовувати складні паролі, які є більш безпечними в порівнянні зі слабкими паролями, що легко можуть бути розгадані зловмисниками методом брутфорсу. Крім того, за допомогою 1Password буде впроваджено двофакторну автентифікацію, що значно підвищить рівень безпеки мережі. Також, за допомогою цього програмного комплексу буде забезпечена централізована періодична зміна паролів, що дозволить забезпечити постійний рівень безпеки мережі та запобігти можливим атакам на мережеві ресурси.

Внутрішня інформаційна мережа готелю має низку серйозних проблем, що потребують негайного вирішення. На даний момент, гостьова та робоча мережі не відокремлені, що створює небезпеку для захисту інформації готелю від зовнішніх загроз. Додатково, відсутність міжмережевого екрана та фільтрації трафіку ускладнює контроль за вхідними та вихідними даними, що збільшує ризик для захисту конфіденційної інформації готелю.

Для вирішення цих проблем, рекомендується встановити міжмережевий екран та фільтр трафіку, що дозволить контролювати всі вхідні та вихідні з'єднання [37]. Також, необхідно відокремити гостьову мережу від робочої та використовувати різні маршрутизатори та підмережі для кожної з них.

Для збільшення рівня захисту інформації, рекомендується використовувати спеціально призначені сервери з підвищеною захищеністю та моніторингом стану системи. Крім того, необхідно створити цілісну інформаційну мережу та забезпечити її моніторинг та підтримку для забезпечення максимальної безпеки готелю.

Усі ці кроки дозволять готелю підвищити рівень захисту інформації та зменшити ризик втрати даних. Важливо не забувати про необхідність постійного моніторингу та оновлення заходів забезпечення мережевої безпеки, щоб забезпечити постійний захист від потенційних загроз.

Ми плануємо вжити ряд заходів, які допоможуть покращити захищеність інформаційних ресурсів готелю. Серед них будуть такі дії:

– створимо цілісну корпоративну мережеву комп'ютерну систему, реструктуруючи різнорідні інформаційні системи;

– придбаємо профільне мережеве обладнання, яке замінить тимчасові рішення, наприклад центральний сервер на основі звичайного ПК;

– відокремимо гостьову мережу від робочої, створивши окремі підмережі з різним діапазоном адрес. Крім того, ми забезпечимо відокремлення деяких внутрішніх систем від Інтернету, зокрема системи відеоспостереження.

Ці заходи допоможуть усунути порушення безпеки, зазначені в описі структури внутрішньої інформаційної мережі готелю. Нова структура мережі

буде міцнішою і більш стійкою до атак, що підвищить загальний рівень захищеності інформаційних ресурсів готелю

Розробимо інформаційну систему, використовуючи середовище Cisco Packet Tracer, яке надає нам можливість моделювати мережі та тестувати їх ефективність [38]. Окрім цього, Cisco Packet Tracer дозволяє нам створювати віртуальні пристрої та налаштовувати їх параметри, що дає нам можливість емулювати реальну мережу.

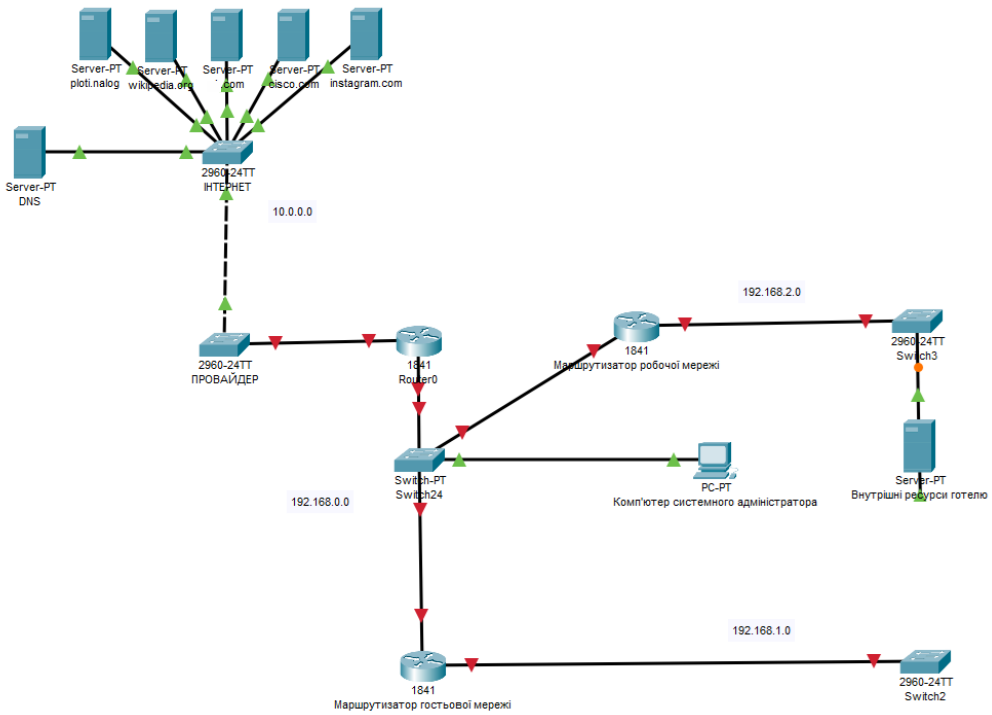


Рисунок 3.1 - Інформаційна система готелю

В результаті, ми зможемо оцінити ефективність та безпеку нашої інформаційної системи та внести необхідні зміни для її вдосконалення перед впровадженням в реальній мережі.

3.2 Інтеграція спроектованих компонентів в єдину систему

Ця система є легко модифікованою та розширюваною, що дозволяє їй бути більш гнучкою у відповіді на зміну вимог до захисту. Вона не потребує значних

ресурсів та може бути побудована з використанням наявних ресурсів. На даний момент, наш готельний комплекс має різні інформаційні системи, такі як система відеоспостереження, система дверних замків з RFID-модулями, пожежна сигналізація та можливо, згодом з'явиться охоронна система з тривожною кнопкою. Кожна з цих систем може працювати автономно, але більш ефективним буде їх інтеграція в єдину централізовану систему з єдиною політикою безпеки. Це дозволить підвищити загальний рівень безпеки готельного комплексу, дозволить більш ефективно керувати процесами та забезпечить легку масштабованість системи в майбутньому. Використання Cisco Packet Tracer дозволить нам розробити таку систему з урахуванням всіх вимог та потреб нашого готельного комплексу.

Щоб забезпечити максимальний рівень захисту інформації у готельному комплексі «Колізей», ми об'єднаємо окремі системи захисту в єдину цілісну систему, яка буде готова до повномасштабного впровадження (рис 3.2).

Наша система буде складатися з корпоративної мережевої системи, системи відеоспостереження та системи дверних замків з RFID-модулями та існуючої протипожежної системи.

Ця модульна будова системи дозволить нам легко об’єднати різні системи захисту в єдину, забезпечуючи високий рівень безпеки та захисту інформації. Крім того, ми забезпечимо цілісну політику безпеки, яка буде використовуватися в усіх системах, що дозволить уникнути розбіжностей та збільшити ефективність захисту.

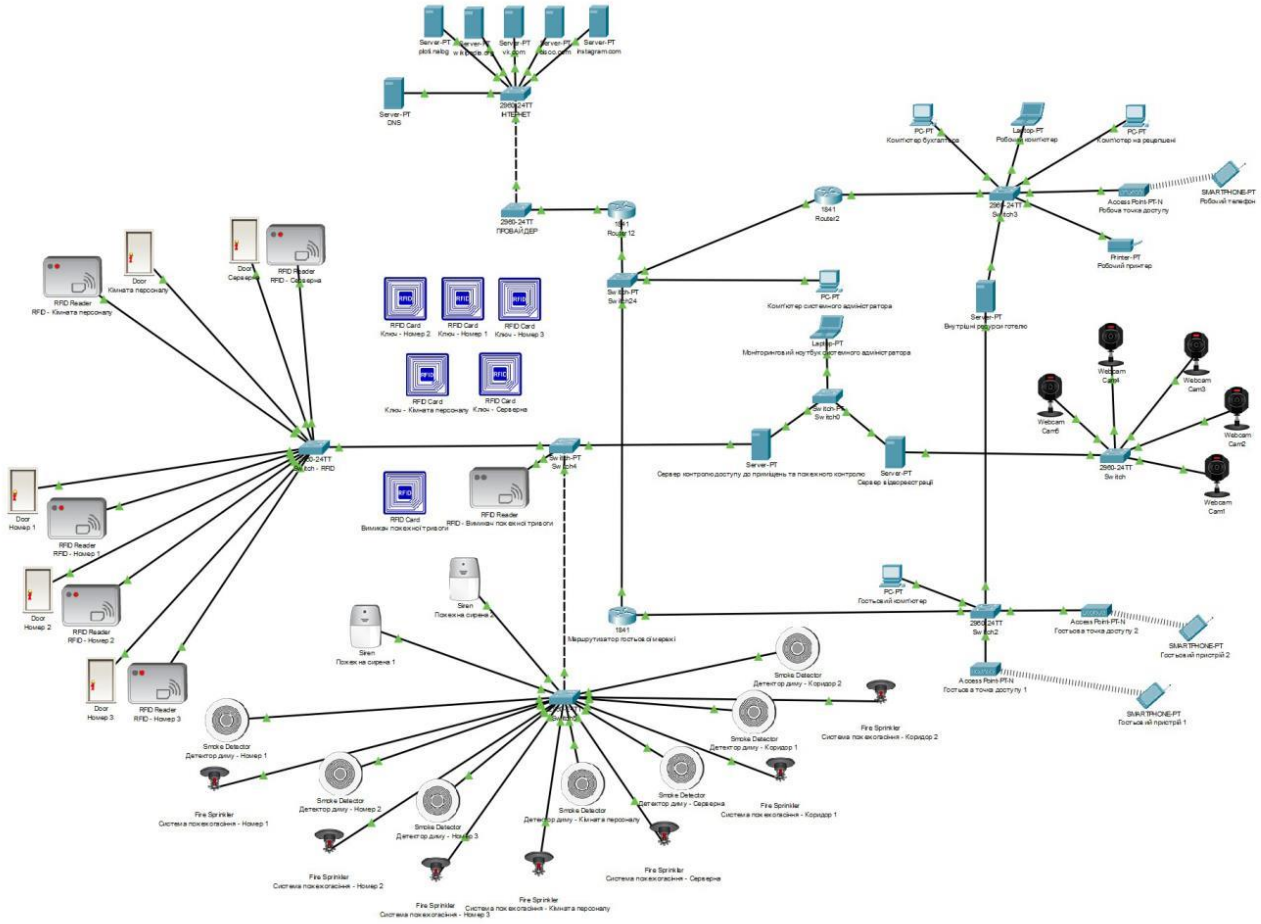


Рисунок 3.2 - Загальна функціональна схема СКД готельного комплексу

Відзначимо, що розробка кожної з окремих систем захисту відбувалася з урахуванням подальшого об’єднання їх в єдину цілісну систему, тому процес об'єднання не повинен викликати жодних серйозних труднощів. Застосування такої комплексної системи захисту інформації дозволить готелю «Колізей» підвищити рівень безпеки та забезпечити захист конфіденційної інформації клієнтів.

За допомогою раніше розглянутих рекомендацій та розробленої схеми, ми успішно створили систему контролю доступу. Для кращого опису складових системи ми зведемо їх в одну таблицю.

Таблиця 3.1 – Компоненти системи контролю доступу

Складова системи контролю доступу	Опис
Електронні замки	Забезпечують фізичний контроль доступу та замінюють звичайні ключі
RFID-карти	Використовуються для ідентифікації особи та надсилання сигналу до електронних замків
Контролер доступу	Керує системою контролю доступу та обробляє інформацію з RFID-карт
База даних користувачів	Зберігає дані про користувачів та їхні права доступу
Система відеоспостереження	Забезпечує нагляд та захист території, об'єктів і людей шляхом запису відеоінформації в реальному часі. Вона може використовуватись для попередження злочинів, виявлення порушень безпеки, контролю доступу
Корпоративна мережа	Для забезпечення зв'язку між комп'ютерами та іншими пристроями, що використовуються в готелі,, а також забезпечує безпеку даних, що передаються по мережі. Відокремлена від зовнішньої мережі інтернет та має відповідні засоби захисту від зовнішніх загроз.
Протипожежна система	Реалізована, не потребує модифікації

Дана система контролю доступу дозволяє забезпечити безпеку об’єкту та контролювати доступ до окремих приміщень. Вона може бути легко встановлена та налаштована з використанням сучасних технологій, таких як електронні замки та RFID-карти. База даних користувачів забезпечує гнучкість та можливість швидкого редагування прав доступу для окремих користувачів. Ця система є надійним та ефективним рішенням для забезпечення безпеки приміщень.

Організаційні заходи, які необхідно провести для впровадження системи контролю доступу в готельному комплексі «Колізей», включають реструктуризацію кадрової структури, проведення професійного інструктажу та створення режимних зон. Також необхідно виділити службову інформацію для внутрішнього використання та навчити персоналу діяти у надзвичайних ситуаціях. Після впровадження системи захисту інформації можна забезпечити повну безпеку інформаційних ресурсів готельного комплексу.

При впровадженні системи інформації необхідно врахувати ресурси, які будуть потрібні для її функціонування. Це може включати в себе фінансові та технічні ресурси, які необхідно виділити для закупівлі та встановлення обладнання, а також для підготовки персоналу та проведення реструктуризації кадрової структури. Оцінка ресурсів допоможе забезпечити успішне впровадження системи контролю доступу в готельному комплексі «Колізей»

3.3 Проєктування бази даних

Microsoft SQL Server Management Studio (SSMS) та Visual Studio 2022 є потужними інструментами для створення баз даних готелю. Використання SSMS дозволяє зручно управляти базою даних, створювати таблиці, визначати зв'язки між ними та виконувати різноманітні операції з даними [39]. SSMS також надає можливість виконувати складні запити SQL та оптимізувати продуктивність бази даних. Visual Studio 2022 є інтегрованою середовищем розробки, яке має підтримку для розробки баз даних та забезпечує широкий набір інструментів для моделювання, створення та управління базою даних готелю. Ви можете

використовувати Visual Studio для розробки схеми бази даних, виконання SQL-запитів, налагодження та оптимізації запитів, а також для інтеграції з іншими компонентами системи готелю, такими як розробка веб-додатків або мобільних додатків. Інфологічна модель бази даних наведено на рисунку 3.3.

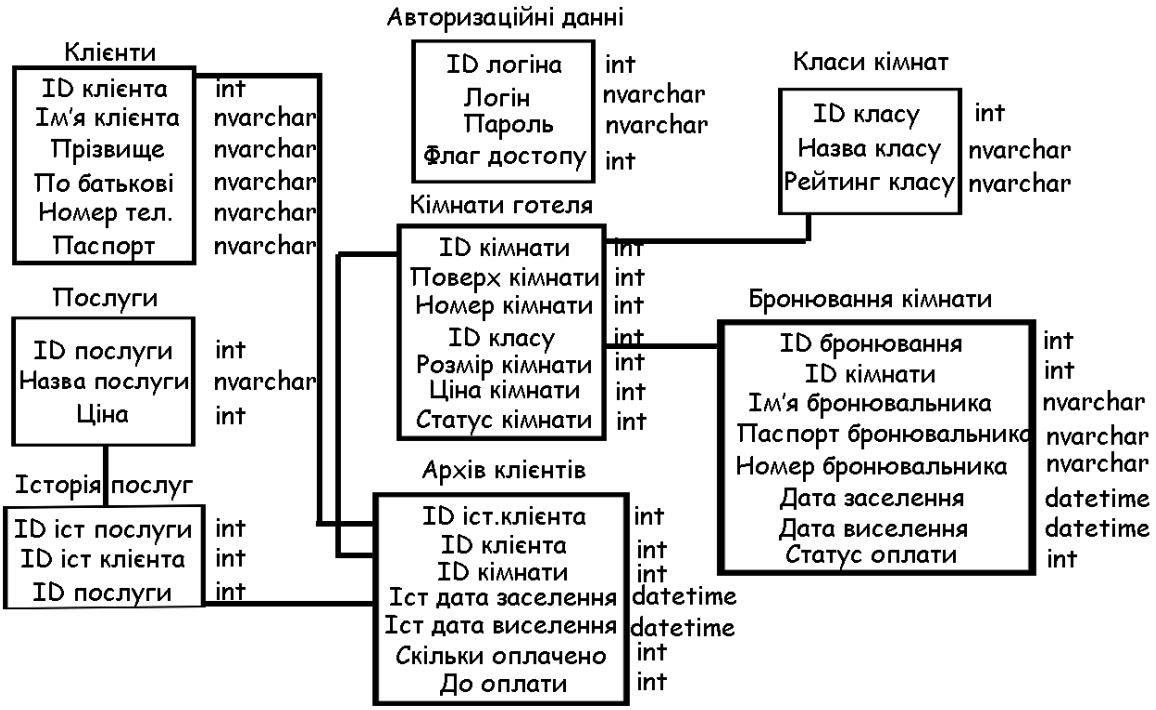


Рисунок 3.3 - Інфологічна модель бази даних

Під час виконання завдання було створено 8 таблиць, які повністю використовувалися в подальшій роботі програми. Перша з цих таблиць була незалежною від інших і була створена для реалізації авторизації в першій формі проекту.

У цю таблицю було додано 3 стовпці. Перший стовпець відповідав за логін користувача, другий - за його секретний пароль, а третій регулював рівень доступу авторизованого користувача. Всього в програмі було реалізовано 2 рівні доступу: "1" - рівень адміністратора і "0" - рівень працівника ресепшн. Користувач з рівнем доступу "1" мав повні права на користування та перегляд інформації.

Для прикладу розглянемо таблицю бронювання. Для бронювання номеру було створено таблицю, до якої вносяться такі поля: ім'я клієнта, його паспортні дані, номер телефону, дата заселення і виселення, а також сума передплати, яку клієнт вніс.

Ці поля мають наступні переваги та доцільність:

– ім'я клієнта, служить для збереження імені клієнта дозволяє персоналу готелю ідентифікувати кожного клієнта та надати персоналізоване обслуговування;

– паспортні дані, для забезпечення документальної ідентифікації клієнта і може бути важливим для забезпечення безпеки та виконання законодавчих вимог;

– номер телефону, для зв'язку з клієнтом щодо підтвердження бронювання, важливих повідомлень або для розробки готельної програми лояльності.

– дата заселення і виселення, дозволяє контролювати наявність і доступність номерів, розраховувати тривалість перебування гостей та оптимізувати процес прийому та виїзду.

– сума передплати, дозволяє готелю контролювати фінансові операції, забезпечувати внесення передплати перед заселенням та розраховувати залишок платежів після виїзду.

Ці поля допомагають створити повну та детальну інформацію про бронювання номерів, що полегшує управління готельними операціями, забезпечує високу якість обслуговування клієнтів.

Приклад реалізації таблиці бронювання наведено на рисунку 3.4.

	Booking_ID	Room_ID	B_Name	B_Passport	B_Number	B_Data_Start	B_Data_End	B_Imprest
▶	1	3	Васько	221231	0681744459	2020-05-23 00:0...	2020-05-29 00:0...	1000
*	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Рисунок 3.4 – Таблиця бронювання

Фізичну реалізацію бази даних наведено на рисунку 3.5.

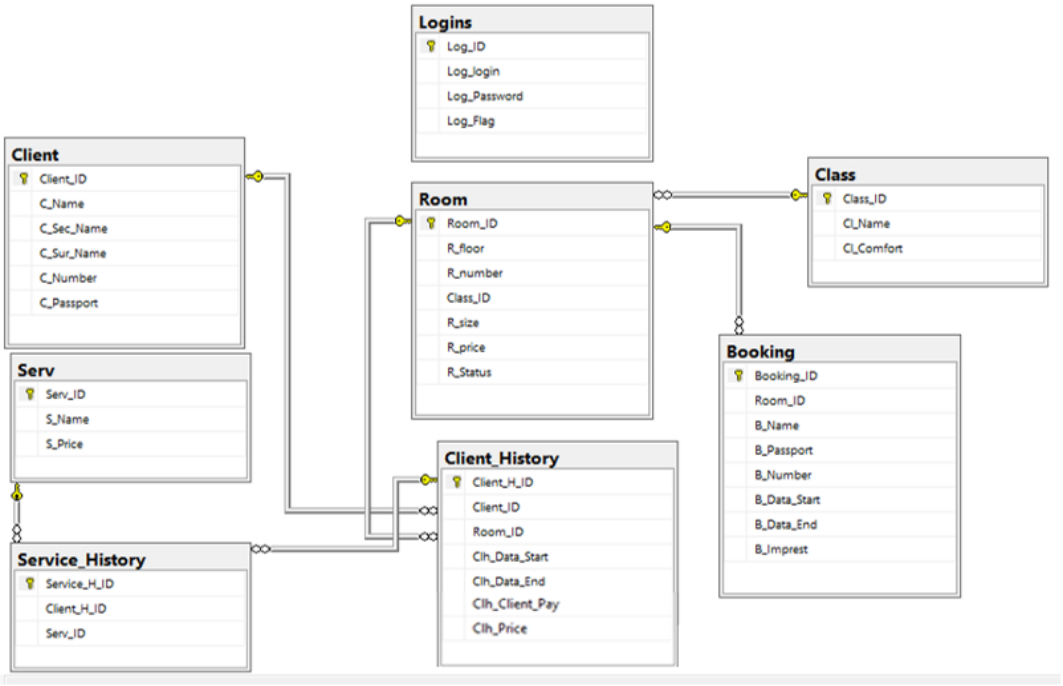


Рисунок 3.5 – Фізична реалізація бази даних

Програмну реалізацію меню «Виселити клієнта» для працівника рецепції наведено на рисунку 3.6.

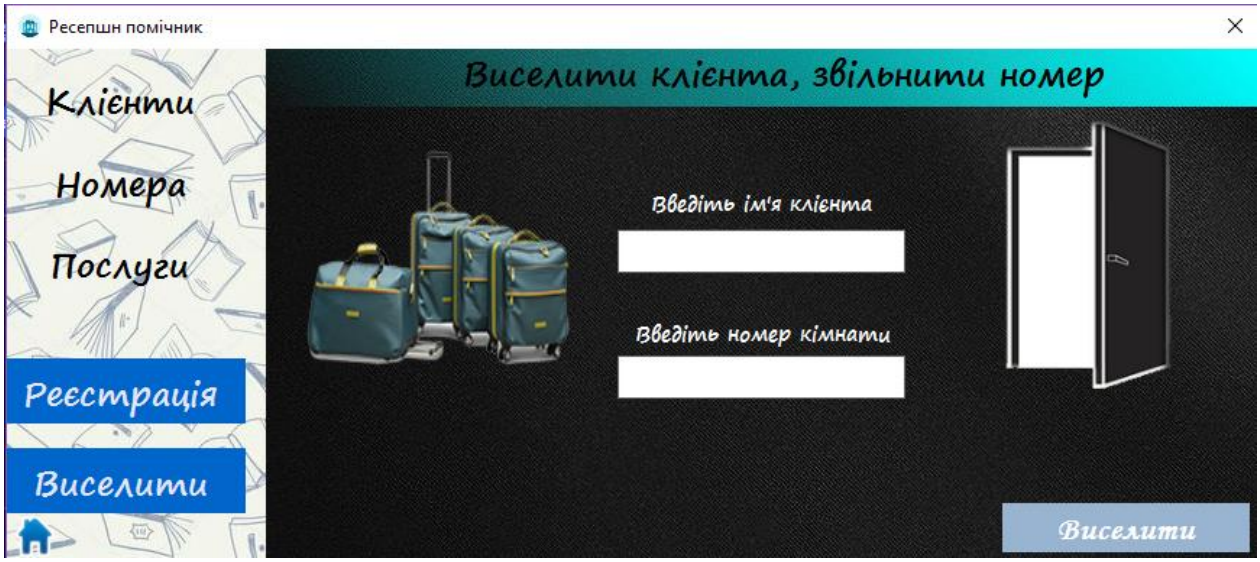


Рисунок 3.6 – Загальний вигляд вкладки Виселити

Розроблений програмний продукт проходить тестування на захищеність та пошук вразливостей.

3.4 Оцінка собівартості системи

Першим кроком в реалізації системи керування доступом є вибір оптимальної цінової категорії з точки зору разових інвестицій і щомісячної оплати. Після вибору компонентів та інших ресурсів, можна розпочати розгортання системи захисту. Процес розгортання не повинен повністю або частково призупиняти діяльність готельного комплексу. Розгортання нових систем здійснюється паралельно з функціонуванням вже існуючих засобів. Якщо деякі елементи використовуються як в старій, так і в новій системі, слід знайти тимчасове рішення, наприклад, орендувати необхідне обладнання.

Однією з головних складових вартості системи керування доступом є вартість обладнання. Під час проектування було враховано ряд факторів, що впливають на вартість обладнання, таких як його функціональні можливості, якість та марка виробника, обсяги та терміни поставки тощо. Також, було враховано необхідність додаткових робіт з монтажу та підключення обладнання до системи, які можуть здійснювати фахівці зі зв’язку та інформаційних технологій.

Другим важливим фактором, що впливає на вартість системи захисту інформації, є необхідність проведення реструктуризації кадрової структури та додаткового навчання персоналу. Ці витрати пов’язані з необхідністю залучення додаткових фахівців та охорони, а також з організацією тренінгів та інструктажів для персоналу.

Нарешті, важливим фактором є необхідність постійного технічного обслуговування та підтримки системи контролю доступу. Вартість цих послуг може бути залежною від рівня складності та обсягу робіт, а також від термінів та умов контракту.

Таблиця 3.2 – Розрахунок собівартості

№	Назва	Кількість, загальна вартість, грн		Обслуго-вування, місяць
		Мінімальна	Рекомендована	
1	Мережевий реєстратор Hikvision DS-7616NI-I2/16P	1, 13280	1, 13280	-
2	IP-камера Hikvision DS- 2CD2121G0-IS(C)	10, 29230	15, 43845	-
3	Флешка	1, 1000	1, 1000	-
4	Монітор	2, 8000	3, 12000	-
5	Дверний замок з RFID-модулем ORBITA E3041	6, 27588	23, 105754	-
6	RFID-ключі	15, 150	75, 750	-
7	Мережева система	~98000	~179000	-
8	Антивірус ESET	7 ,3500	9, 4500	1000
9	Бізнес-ліцензія 1Password	-	-	2500
10	Встановлення тривожної системи Поліцією охорони	7000	7000	6000
11	Інженер безпеки	-	-	20000
12	Охоронець	-	-	20000
Загальний підсумок		174468	367129	49500

Важливо відзначити, що оцінка вартості проектування системи буде лише приблизною і залежатиме від наявних ресурсів та вимог до системи захисту, які були встановлені. Крім того, вартість системи може змінюватися в залежності від рівня складності її інтеграції з наявною інформаційною інфраструктурою готелю.

Необхідність заміни або оновлення наявного обладнання, встановлення додаткових програмних засобів та залучення фахівців для цих робіт можуть вплинути на вартість проекту. Всі ці фактори потребують детального аналізу та розрахунків, щоб забезпечити точну оцінку вартості проекту.

3.5 Розробка рекомендацій для реалізації системи

Політика безпеки готельного комплексу «Колізей» - це сукупність заходів та правил, спрямованих на забезпечення безпеки клієнтів, працівників та інших користувачів об'єкту. Головна мета політики безпеки - захист інформації та забезпечення безпеки в цілому.

До основних заходів, що входять до політики безпеки готельного комплексу «Колізей» входять: використання системи контролю доступу, регулярне проведення навчань та тренувань для персоналу щодо дій в надзвичайних ситуаціях, створення режимних зон, реструктуризація кадрової структури та збільшення штату охорони.

Політика безпеки готельного комплексу «Колізей» є динамічною та піддається постійному аналізу та оновленню з метою вдосконалення та підвищення рівня безпеки. Для цього регулярно проводяться аудити, перевірки та оцінки ризиків, що дозволяє оперативно вносити необхідні зміни та доповнення до політики безпеки [40].

Крім того, політика безпеки готельного комплексу «Колізей» передбачає дотримання всіх законів та нормативно-правових актів щодо захисту персональних даних та конфіденційної інформації. Також у готелі діє система

внутрішнього контролю та перевірок, що дозволяє виявляти та запобігати порушенням правил безпеки.

Отже, політика безпеки готельного комплексу «Колізей» є важливим елементом в забезпеченні безпеки готелю та збереженні інформації. Ця політика є динамічною та постійно оновлюється з метою вдосконалюється.

Однією з ключових складових політики безпеки є захист інформації. Окрім того, готельний комплекс «Колізей» дотримується політики контролю доступу, яка включає в себе встановлення режимних зон та обмеження доступу до окремих приміщень, де зберігається конфіденційна інформація. З метою забезпечення безпеки персоналу та гостей, на території готельного комплексу розміщені системи відеоспостереження, які функціонують цілодобово.

Політика безпеки також включає в себе профілактичні заходи, спрямовані на запобігання негативних наслідків надзвичайних ситуацій. У готельному комплексі «Колізей» проводяться регулярні навчання та тренування персоналу, щоб вони могли ефективно діяти у випадку пожежі, землетрусу чи іншої надзвичайної ситуації.

З метою забезпечення безпеки гостей та персоналу, готельний комплекс «Колізей» також дотримується всіх необхідних норм і правил щодо пожежної безпеки та гігієни. Для цього на території готельного комплексу розміщені вогнегасники, знаки пожежної безпеки та засоби індивідуального захисту, а також персонал регулярно проводить перевірки та інструктажі.

Усі ці заходи забезпечують високий рівень безпеки та захисту для персоналу та гостей готельного комплексу «Колізей».

Впровадження системи керування доступом в готельному комплексі «Колізей» є складним процесом, що потребує наявності відповідної настанови для реалізації цієї системи. Ці настанови повинні включати в себе опис процедур інсталяції та налаштування системи, рекомендації з її експлуатації та обслуговування, а також процедури дій в надзвичайних ситуаціях.

Нижче наведені основні кроки, які необхідно виконати для успішного впровадження системи керування доступом в готелі:

– враховуючи потреби готельного комплексу, необхідно визначити, які типи дверей та приміщень потребують контролю доступу, а також скільки карток доступу буде потрібно;

– при виборі постачальника необхідно звернути увагу на досвід роботи, якість обладнання та послуг, а також наявність сертифікатів та гарантій на обладнання та послуги;

– необхідно встановити спеціальні двері, які підтримують роботу системи керування доступом, а також провести кабелювання, що забезпечить передачу даних між компонентами системи;

– встановити та налаштувати обладнання та псля підготовки приміщення необхідно встановити обладнання та налаштувати його на відповідні функції;

– після встановлення та налаштування системи необхідно провести навчання персоналу з її використання.

Після встановлення та налаштування системи необхідно забезпечити її регулярне обслуговування та технічну підтримку. Для цього можна використовувати внутрішні ресурси компанії або звернутися до зовнішніх сервісних компаній.

Також необхідно розробити процедури дій в надзвичайних ситуаціях, наприклад, в разі відмови системи або випадку порушення безпеки. Для цього потрібно провести навчання персоналу та розробити відповідний план дій.

3.5 Висновок

Розгортання системи керування доступом є важливим етапом в підвищенні рівня безпеки готельного комплексу. Оптимальний вибір компонентів і ресурсів, а також паралельне розгортання системи з використанням існуючих засобів є ключовими факторами успішної і безпечної реалізації цього проекту.

Після встановлення всіх компонентів нової системи, проведення відповідної перевірки та тестування, здійснюється плавний перехід зі старої системи на нову. Після цього всі компоненти нової системи повинні бути піддані

тестуванню в умовах штатного режиму роботи. Якщо ніяких проблем не виявлено, стара система може бути поступово вилучена. Отже, розробка комплексної системи захисту інформації для готельного комплексу «Колізей» завершена успішно, оцінена та описана процедура її впровадження.

ВИСНОВКИ

Під час виконання бакалаврської роботи було проведено дослідження та аналіз предметної області, об'єкта захисту, його фізичної та інформаційної структури. На основі цього аналізу була розроблена система контролю доступу для готельного комплексу "Колізей".

Метою проекту було проведення комплексного безпекового аналізу фізичної та інформаційної структури готельного комплексу "Колізей". Результати аналізу були використані для розробки індивідуальної системи захисту інформації, яка забезпечує безпечне функціонування готелю відповідно до його комерційного призначення.

Цей проект мав на меті забезпечити високий рівень безпеки готельного комплексу шляхом ідентифікації та контролю доступу до різних зон та ресурсів. Результати бакалаврської роботи допоможуть готельному комплексу "Колізей" захищати свою інформацію від пріоритетних загроз та використовувати ресурси ефективно.

Під час виконання бакалаврської роботи була проведена систематизація теоретичної інформації, досліджено різні види захисту інформаційних ресурсів та безпекові властивості інформації. Була також проведена аналіз корпоративної, державної та міжнародної нормативно-правової бази з питань захисту інформації. Було проведено серію досліджень з метою збору інформації для подальшої розробки системи керування доступом готелю. Запропоновано архітектуру мережі готелю та розроблено програмне забезпечення для персоналу та адміністрації. Було проведено дослідження та класифікація інформаційних потоків в готелі.

Отже, результати досліджень та аналізу, проведені в рамках бакалаврської роботи, були використані для розробки ефективної системи контролю доступу, що забезпечує захист інформації в готельному комплексі "Колізей"

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Про захист інформації у інформаційно-комунікаційних системах : Закон України від 04.07.2020 р. №80/94 -ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 15.02.2023)

2. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.

3. Джулій В. М., Муляр І. В., Чешун В. М. Кваліфікаційна робота : методичні вказівки щодо її підготовки і виконання для студентів спеціальності 125 «Кібербезпека». Хмельницький : ХНУ, 2021. 54 с.

4. Дикий О. В. Стандарти інформаційної безпеки: компаративне дослідження / О. В. Дикий, М. О. Флюнт // Право та державне управлінняю – 2019. – № 2 (35), том 1. – С. 80-87

5. Загальний регламент про захист даних. URL: https://uk.wikipedia.org/wiki/ Загальний_регламент_про_захист_даних (дата звернення: 01.04.2023).

6. Мальська М.П., Білоус С.В. Менеджмент готельно-ресторанного господарства: методичні рекомендації. - Львів 2020. – 55 с.

7. Всесвітня туристська організація. URL: http://lvivmun.sii.org.ua/unwto/ (дата звернення: 02.03.2023).

8. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. – Чинний від 28 квітня 1999 р. – Київ : ДСТСЗІ СБ, 1999. – [35] с.

9. Системи контролю доступу: що це таке і як працює. URL: https://zakarpattya.net.ua/News/200909-Systemy-kontroliu-dostupu-shcho-tse-take-i-iak-pratsiuie (дата звернення: 11.02.2023).

10. Система контролю і управління доступом - Вікіпедія. URL: https://uk.wikipedia.org/wiki/Система_контролю_і_управління_доступом (дата

звернення 13.08.2019).

11. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level / Editors : Robert M. Clark, Simon Hakim. – Cham, Switzerland : Springer, 2016. – 360 p.

12. Safeguarding the Information Systems in an Organization through Different Technologies, Policies, and Actions/ Hend K. Alkahtani. – Computer and Information Science. – Vol. 12, No. 2; 2019. – Published by Canadian Center of Science and Education. – P. 117-125.

13. Fundamentals of InformationSystems Security / Editors : David Kim, Michael G. Solomon. – Burlington, Massachusetts : Jones & Bartlett Learning, 2018. – 548 p.

14. ДСТУ ISO/IEC 27032:2016. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. – Чинний від 2016-27-12. – Київ : ДП «УкрНДНЦ», 2018. – [50] с.

15. Baranov O.A. Internet of Things (IoT): A Review of Legal Issues // Internet of Things: Scientific Conference. October 24, 2017, Kyiv. / Order. VM Furashev, S. Yu. Petryayev. - K .: NTUU "Igor Sikorsky Kyiv Polytechnic Institute" Publishing House "Polytechnic". 2017

16. Гапак О. М., Болога С.І. Захист інформації в комп'ютерних системах : підручник. Ужгород : ДВНЗ «Ужгородський національний університет», 2021. 184 с.

17. Захист інформації в комп'ютерних системах: підручник. / В.Д. Козюрата інші. Ніжин: ТПК «Орхідея», 2020. – 236 с.

18. Інформаційна безпека держави: навчальний посібник/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.

19. Про основні засади забезпечення кібербезпеки України : ЗаконУкраїни від 01.08.2021р. №2163-VIII. URL: https://ips.ligazakon.net/document/JH1N268B (дата звернення: 23.04.2023)

20. Information Security Standard: Information Technology Resource

Management. Virginia Information Technologies Agency (VITA), 2016. – 183 p.

21. Гребенніков В.В. Комплексні системи захисту інформації: проєктування, впровадження, супровід. / В.В. Гребенніков – Ужгород: Ужгородський національний університет, 2013. – 161 с.

22. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Чинний від 25 березня 2011 р. – Київ : Адміністрація Державної служби спеціального зв'язку та захисту інформації України, 2011. – [130] с.

23. Інформаційна та кібербезпека: соціотехнічний аспект: підручник/ В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

24. Practical Information Security Management: A Complete Guide to Planning and Implementation/ Tony Campbell. – Australia: Burns Beach, 2016. – 253 p.

25. Defense Counterintelligence and Security Agency Assessment and Authorization Process Manual – Quantico, Virginia : Defense Counterintelligence and Security Agency, 2020. – 163 p.

26. Cyber Security for Cyber Physical Systems / Saqib Ali, Taiseera Al Balushi, Zia Nadir, Omar Khadeer Hussain. – Cham, Switzerland : Springer, 2018. – 174 p.

27. Законність встановлення відеоспостереження у ресторанах URL: https://joinposter.com/ua/post/zakonnist-vstanovlennya-videosposterezhennya-u-restoranakh (дата звернення: 01.04.2023).

28. Як встановити камеру зовнішнього спостереження у: URL: https://secur.ua/ua/articles/ua_jak-vstanoviti-kameru-zovnishn-ogo-sposterezhennja.html (дата звернення: 10.04.2023)

29. Програма для проєктування. URL: https://www.jvsg.com/ (дата звернення: 10.05.2023)

30. IP-камери Hikvision DS2CD2121G0-IS URL: https://hikvision.co.ua/hikvision-ds-2cd2121g0-28-mm (дата звернення: 10.05.2023)

31. 2МП IP камера Hikvision DS-2CD2121G0-IS

URL:https://control.ua/hikvision-ds-2cd2121g0-c-28-mm.html (дата звернення: 10.05.2023)

32. 16-канальний 4K мережевий відеорегістратор Hikvision DS-7616NI-I2/16P URL: https://hikvision.co.ua/hikvision-ds-7616ni-i216p (дата звернення: 10.05.2023)

33. Al-shawi M. Designing for Cisco Network Service Architectures (ARCH) Foundation Learning Guide: CCDP ARCH 300-320 / Marwan Al-shawi, André Laurent. – Indianapolis : Cisco Press, 2017. – 941 p.

34. Замок для готельних систем доступу Orbita E3041 URL: https://chime.com.ua/ua/orbita-e3041-zamok-dlya-otelnyh-sistem-dostupa (дата звернення: 11.04.2023)

35. Вараксін О. О. Кібербезпека мереж наступного покоління : навч. посіб. у галузі знань "Інформаційна безпека" за спец. - Системи технічного захисту інформації, автоматизація її обробки / О. О. Вараксін, Є. В. Василіу, С. М. Горохов, В. Й. Кільдішев, В. Г. Кононович; ред.: В. Г. Кононович; Одес. нац. акад. зв'язку ім. О.С. Попова. – Одеса : ОНАЗ ім. О. С. Попова, 2013. - 238 с

36. Програма 1password. URL: https://1password.com/ (дата звернення: 11.05.2023)

37. Контроль і управління доступом URL: https://amrita-cs.com/security_systems/systems-access-control/ (дата звернення: 26.03.2023)

38. Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice / Elias G. Carayannis, David F. J. Campbell, Marios Panagiotis Efthymiopoulos. – New York : Springer, 2014. – 360 p.

39. Програма Visual Studio 2022 IDE URL: https://www.google.com/search?client=firefox-b-d&q=Visual+Studio+2022+ (дата звернення: 12.05.2023)

40. Douglas J. Landoll Information Security Policies, Procedures, and Standards: A Practitioner’s Reference / Douglas J. Landoll. – Boca Raton : CRC Press Taylor & Francis Group, 2016. – 246 p.

ДОДАТОК А

(обов'язковий)

Фрагменти програмного коду клієнтської частини

1.Головне меню

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using WindowsFormsApp1.MyControls;
using WindowsFormsApp1.MyControls.Nomer;
using WindowsFormsApp1.MyControls.Poslygu;

namespace WindowsFormsApp1
{
    public partial class FormMain : Form
    {
        private int fl;
        public FormMain(int flag)
        {
            InitializeComponent();
            this.fl = flag;
        }

        private void FormMain_Load(object sender, EventArgs e)
        {
            this.servTableAdapter.Fill(this.hotelDataSet1.Serv);

            Info.flag = fl;

        }

        private void panel2_Paint(object sender, PaintEventArgs e)
        {

        }
        bool butNomer4 = false;
        private void button4_Click(object sender, EventArgs e)
        {
            if (!butNomer4)
            {
                nomerGolovna1.Visible = false;
                klentGolovna1.Visible = false;
                poslyguGolovna1.Visible = false;
                registerGolovna1.Visible = true;
                vuselGolovna1.Visible = false;
                butNomer4 = true;
            }
            else
            {
                nomerGolovna1.Visible = false;
                klentGolovna1.Visible = false;
                poslyguGolovna1.Visible = false;
                registerGolovna1.Visible = false;
                vuselGolovna1.Visible = false;
                butNomer4 = false;
```

```
    }
}
bool butNomer3 = false;
private void button3_Click(object sender, EventArgs e)
{
    if (!butNomer3)
    {
        nomerGolovna1.Visible = false;
        klentGolovna1.Visible = false;
        poslyguGolovna1.Visible = true;
        registerGolovna1.Visible = false;
        vuselGolovna1.Visible = false;
        butNomer3 = true;
    }
    else
    {
        nomerGolovna1.Visible = false;
        klentGolovna1.Visible = false;
        poslyguGolovna1.Visible = false;
        registerGolovna1.Visible = false;
        vuselGolovna1.Visible = false;
        butNomer3 = false;
    }
}


bool butNomer1 = false;
private void button1_Click_1(object sender, EventArgs e)
{
    if (!butNomer1)
    {
        klentGolovna1.Visible = true;
        nomerGolovna1.Visible = false;
        poslyguGolovna1.Visible = false;
        registerGolovna1.Visible = false;
        vuselGolovna1.Visible = false;
        butNomer1 = true;
    }
    else
    {
        klentGolovna1.Visible = false;
        nomerGolovna1.Visible = false;
        poslyguGolovna1.Visible = false;
        registerGolovna1.Visible = false;
        vuselGolovna1.Visible = false;
        butNomer1 = false;
    }
}
bool butNomer2 = false;

private void button2_Click(object sender, EventArgs e)
{
    if (!butNomer2)
    {
        nomerGolovna1.Visible = true;
        klentGolovna1.Visible = false;
        poslyguGolovna1.Visible = false;
        registerGolovna1.Visible = false;
        vuselGolovna1.Visible = false;
        butNomer2 = true;
    }else
    {
        nomerGolovna1.Visible = false;
        klentGolovna1.Visible = false;
        poslyguGolovna1.Visible = false;
```

```
                registerGolovna1.Visible = false;
                vuselGolovna1.Visible = false;
                butNomer2 = false;
            }
        }

        private void button5_Click(object sender, EventArgs e)
        {
            nomerGolovna1.Visible = false;
            klentGolovna1.Visible = false;
            poslyguGolovna1.Visible = false;
            registerGolovna1.Visible = false;
            vuselGolovna1.Visible = false;
        }

        bool butNomer6 = false;
        private void button6_Click(object sender, EventArgs e)
        {
            if (!butNomer6)
            {
                nomerGolovna1.Visible = false;
                klentGolovna1.Visible = false;
                poslyguGolovna1.Visible = false;
                registerGolovna1.Visible = false;
                vuselGolovna1.Visible = true;
                butNomer6 = true;
            }
            else
            {
                nomerGolovna1.Visible = false;
                klentGolovna1.Visible = false;
                poslyguGolovna1.Visible = false;
                registerGolovna1.Visible = false;
                vuselGolovna1.Visible = false;
                butNomer6 = false;
            }
        }

    }
}
```

2. Виселення клієнта

```
private string[] RemoveBooking(int floor, int num)
{
    string mes = "Рахунок за проживання\n";
    string sql1 = "SELECT Client_History.Client_H_ID, Client_History.Clh_Client_Pay,
Client_History.Clh_Price, Room.R_Status FROM Client_History INNER JOIN Room ON
Client_History.Room_ID = Room.Room_ID  WHERE Room.R_floor = " + floor + ", AND Room.R_number
= " + num + " ORDER BY Client_History.Client_H_ID";
    string Clh_Id = "";
    int price, pay;

    using (SqlConnection connection = new SqlConnection(Myclass.connectionString))
    {
        connection.Open();
        SqlCommand command = new SqlCommand(sql1, connection);
        SqlDataReader reader = command.ExecuteReader();
        if (reader.HasRows)
        {



            while (reader.Read())
            {
```

```
                if(reader.GetValue(3).ToString() == "1")
                {
                    Clh_Id = reader.GetValue(0).ToString();
                    pay = (int)reader.GetValue(1);
                    price = (int)reader.GetValue(2);
                }
                else
                {
                    MessageBox.Show("Помилка! В даному номері ніхто не зареєстрований",
"Виселення клієнта");
                    reader.Close();
                    connection.Close();
                    return null;
                }
            }
        }
        else
        {
            MessageBox.Show("Помилка! Вказані не вірні дані, або відсутній зв'язок з базою
даних", "Виселення клієнта");
            reader.Close();
            connection.Close();
            return null;
        }

        reader.Close();

        mes += "Сума за проживання: " + price + "\n";


        string sql2 = "SELECT Serv.S_Price, Serv.S_Name From Serv INNER JOIN Service_History
ON Service_History.Serv_ID = Serv.Serv_ID WHERE Service_History.Client_H_ID = " + Clh_Id;

        command = new SqlCommand(sql2, connection);
        SqlDataReader reader = command.ExecuteReader();
        if (reader.HasRows)
        {
            while (reader.Read())
            {
                price += (int)reader.GetValue(0);
                mes += reader.GetValue(1).ToString() + ": " + prive + "\n";
            }
        }
        else
        {
            MessageBox.Show("Помилка", "Виселення клієнта");
            reader.Close();
            connection.Close();
            return null;
        }
        reader.Close();
        mes += "-----------------------------------\nЗагальна вартість: " + price + "\n";
        mes += "Сплочено клієнтом: " + pay + "\n";
        mes += "-----------------------------------\nПідсумок" + (price - pay) + "\n";

        MessageBox.Show(mes, "Рахунок");

        string d_now = DateTime.Now.ToString("yyyy-MM-dd HH:mm:ss.fff");
        string sql3 = "UPDATE Client_History SET Client_History.Clh_Data_End = " + d_now + "
WHERE Client_History.Client_H_ID = " + Clh_Id;



        command = new SqlCommand(sql3, connection);
        SqlDataReader reader = command.ExecuteReader();
        if (reader.HasRows)
```

```
        {
            while (reader.Read())
            {
            }
        }
        reader.Close();

        string sql4 = "UPDATE Room SET Room.R_Status = 0 WHERE Room.R_floor = " + floor + ",
AND Room.R_number = " + num + " ORDER BY Client_History.Client_H_ID";

        command = new SqlCommand(sql3, connection);
        SqlDataReader reader = command.ExecuteReader();
        if (reader.HasRows)
        {
            while (reader.Read())
            {
            }
        }
        reader.Close();
        connection.Close();

        MessageBox.Show("Клієнта виселено");
    }
}
```

2. Бронювання

```
private int CheckPrice()
{
    // textBox1 - номер поверха
    // textBox2 - номер кімнати
    // textBox3 - поле для виводу вартості проживання

    DateTime start = dateTimePicker1.Value;
    DateTime end = dateTimePicker2.Value;
    TimeSpan diff = end - start;
    int time = (int)diff.TotalDays;
    string sql1 = "R_price FROM Room WHERE Room.R_floor = " + textBox1.Text + ", AND
Room.R_number = " + textBox2.Text;
    int R_pr;
    using (SqlConnection connection = new SqlConnection(Myclass.connectionString))
    {
        connection.Open();
        SqlCommand command = new SqlCommand(sqlExpression, connection);
        SqlDataReader reader = command.ExecuteReader();
        if (reader.HasRows)        {
            while (reader.Read())
            {
                R_pr = (int)reader.GetValue(0);
            }
        }
        else
        {
            return;
        }
        reader.Close();
        connection.Close();
        textBox3.Text = (R_pr * time).ToString();
        return;



   }
}
```

```
private void Booking()
{
    // textBox1 - номер поверха
    // textBox2 - номер кімнати
    // textBox4 - ім'я клієнта
    // textBox5 - паспорт
    // textBox6 - телефон
    // textBox7 - завдаток
    // dateTimePicker1 - заїзд
    // dateTimePicker2 - виїзд


    string sql1 = "SELECT Client_History.Clh_Data_End, Booking.B_Data_Start,
Booking.B_Data_End, Room.Room_ID, Room.R_price FROM Room INNER JOIN Client_History ON
Client_History.Room_ID = Room.Room_ID INNER JOIN Booking ON Booking.Room_ID = Room.Room_ID
WHERE Room.R_floor = " + textBox1.Text + ", AND Room.R_number = " + textBox2.Text;
    string R_Id = "";
    DateTime start = dateTimePicker1.Value;
    DateTime end = dateTimePicker2.Value;
    if(start > end){
        MessageBox.Show("Введіть коректні дати", "Бронювання");
    }
    bool R_fr;
    int R_pr;

    using (SqlConnection connection = new SqlConnection(Myclass.connectionString))
    {
        connection.Open();
        SqlCommand command = new SqlCommand(sql1, connection);
        SqlDataReader reader = command.ExecuteReader();
        if (reader.HasRows)
        {
            R_fr = true;
            while (reader.Read())
            {   R_Id = reader.GetValue(3).ToString();
                R_pr = (int)reader.GetValue(4);
                if((DateTime)reader.GetValue(0) > start)
                    R_fr = false;
                if((DateTime)reader.GetValue(1) > start && (DateTime)reader.GetValue(2) <
start)
                    R_fr = false;
                if((DateTime)reader.GetValue(1) > end && (DateTime)reader.GetValue(2) < end)
                    R_fr = false;
                if((DateTime)reader.GetValue(1) > end && (DateTime)reader.GetValue(2) <
start)
                    R_fr = false;
            }
        }
        else
        {
            MessageBox.Show("Помилка! Вказані не вірні дані, або відсутній зв'язок з базою
даних", "Бронювання");
            reader.Close();
            connection.Close();
            return;
        }
        reader.Close();

        string num = textBox2.Text;
        while(num.Length < 2)



      num = 0 + num;
```

```
        if(!R_fr){
            MessageBox.Show("Помилка! Кімната " + textBox1.Text + num + " вже зарезервована
на цей період. Оберіть інші дати.", "Бронювання");
            connection.Close();
            return;
        }

        string d_start = start.ToString("yyyy-MM-dd HH:mm:ss.fff");
        string d_end = end.ToString("yyyy-MM-dd HH:mm:ss.fff");

        string sql2 = "INSERT INTO Booking (Room_ID, B_Name, B_Passport, B_Number,
B_Data_Start, B_Data_End, B_Imprest) VALUES (" + R_Id + ", \'" + textBox4.Text + "\', \'" +
textBox5.Text + "\', \'" + textBox6.Text+ "\', \'" + d_start + "\', \'" + d_end + "\', " +
textBox7.Text + ")";

        command = new SqlCommand(sql2, connection);
        SqlDataReader reader = command.ExecuteReader();
        if (reader.HasRows)
        {
            while (reader.Read())
            {
            }
        }
        reader.Close();
        connection.Close();

        MessageBox.Show("Бронювання успішно створено", "Бронювання");
        return;
    }
}

private void RemoveBooking(string phone, int floor, int num)
{
    string sql1 = "SELECT Booking.Booking_ID, Booking.B_Data_Start, Booking.B_Data_End,
Booking.B_Imprest FROM Room INNER JOIN Booking ON Booking.Room_ID = Room.Room_ID  WHERE
Room.R_floor = " + floor + ", AND Room.R_number = " + num + ", AND Booking.B_Number LIKE \'"
+ phone + "\'";
    string B_Id = "";

    bool R_fr = false;
    string mes = "бронювань за цими даними не знайдено.";

    using (SqlConnection connection = new SqlConnection(Myclass.connectionString))
    {
        connection.Open();
        SqlCommand command = new SqlCommand(sql1, connection);
        SqlDataReader reader = command.ExecuteReader();
        if (reader.HasRows)
        {
            while (reader.Read())
            {   string d_s = (DateTime)(reader.GetValue(1)).ToString("dd.MM.yyyy");
                string d_e = (DateTime)(reader.GetValue(2)).ToString("dd.MM.yyyy");
                DialogResult dialogResult = MessageBox.Show("Бажаєте видалити бронювання ("
+ d_s + " - " + d_e + ")?", "Видалення бронювання", MessageBoxButtons.YesNo);
                if(dialogResult == DialogResult.Yes)
                {
                    MessageBox.Show("Внесений завдаток: " + reader.GetValue(3).ToString());
                    R_fr = true;
                    B_Id = reader.GetValue(0).ToString();
                }
                else
                {



    mes = "інших " + mes;
```

```
                }
                B_Id = reader.GetValue(0).ToString();
            }
        }
        else
        {
            MessageBox.Show("Помилка! Вказані не вірні дані, або відсутній зв'язок з базою
даних", "Видалення бронювання");
            reader.Close();
            connection.Close();
            return;
        }
        reader.Close();

        if(!R_fr){
            MessageBox.Show("Помилка, " + mes, "Видалення бронювання");
            connection.Close();
            return;
        }

        string sql2 = "DELETE FROM Booking WHERE Booking_ID = " + B_Id;

        command = new SqlCommand(sql2, connection);
        SqlDataReader reader = command.ExecuteReader();
        if (reader.HasRows)
        {
            while (reader.Read())
            {
            }
        }
        reader.Close();
        connection.Close();

        MessageBox.Show("Бронювання видалено", "Бронювання");
        return;
    }

}
```

4. Подробиці про клієнта

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Data.SqlClient;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.Windows.Forms.VisualStyles;
using WindowsFormsApp1.MyControls.Nomer;

namespace WindowsFormsApp1.MyControls.Client
{
    public partial class Podrobutsi : Form
    {
         int  UserID;
```

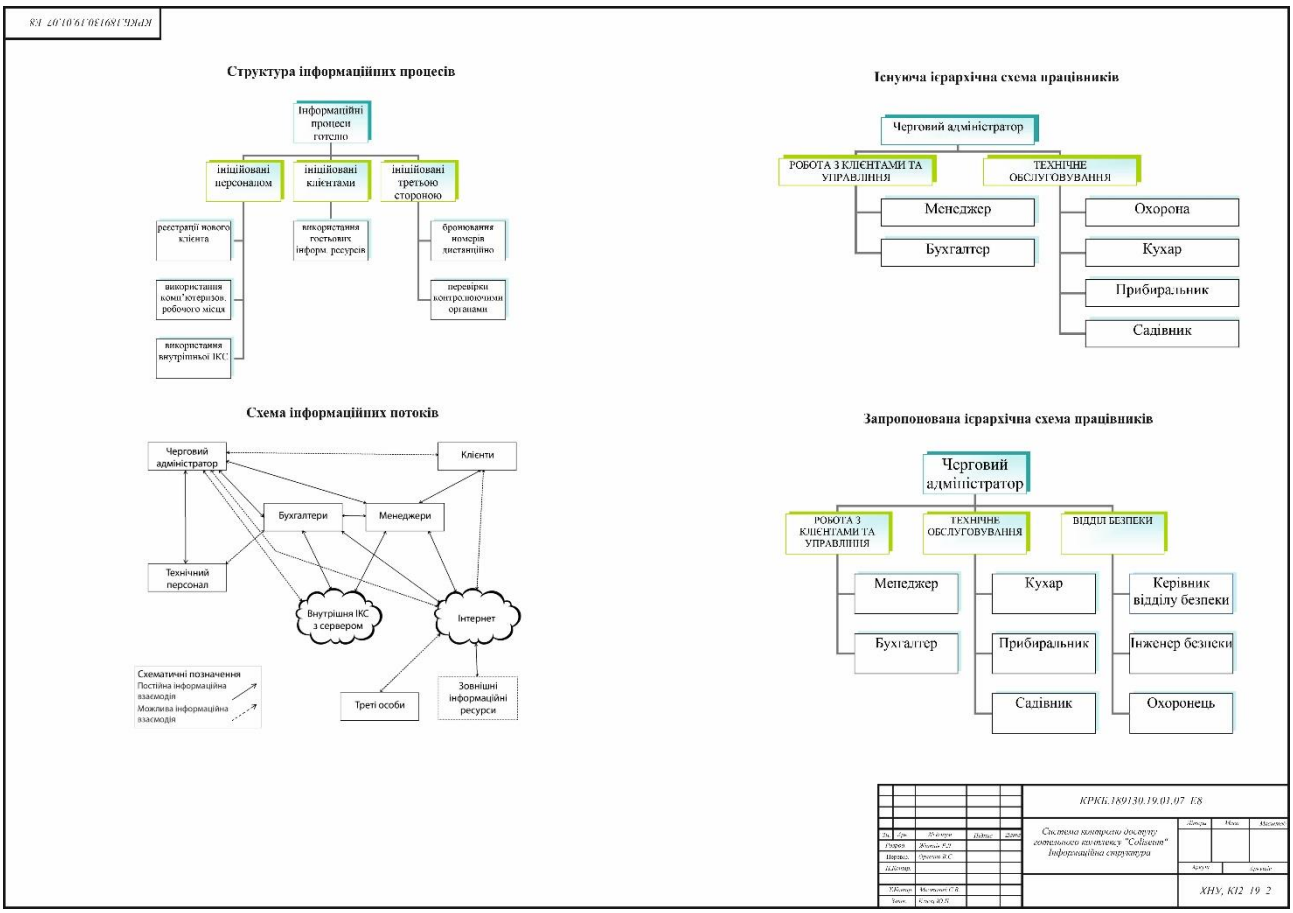
```
   string Sqlexception = "SELECT Client.C_Sec_Name, Client.C_Name, Client.C_Sur_Name,
Client.C_Number, Client.C_Passport FROM Client WHERE Client.Client_ID= " ;

        public Podrobutsi(int ID)
        {
            this.UserID = ID;
            InitializeComponent();

        }

        private void Podrobutsi_Load(object sender, EventArgs e)
        {
            Sqlexception += UserID.ToString();
            GetClients(Sqlexception);
        }

        private void label1_Click(object sender, EventArgs e)
        {

        }

        private void label5_Click(object sender, EventArgs e)
        {

        }

        private void label4_Click(object sender, EventArgs e)
        {

        }

        private void textBox4_TextChanged(object sender, EventArgs e)
        {

        }

        private void panel4_Paint(object sender, PaintEventArgs e)
        {

        }

        private void GetClients(string sqlExpression)
        {
            int i = 0;


            using (SqlConnection connection = new
SqlConnection(Connection.connectionString))
            {
                connection.Open();
                SqlCommand command = new SqlCommand(sqlExpression, connection);
                SqlDataReader reader = command.ExecuteReader();

                if (reader.HasRows)
                {
                    while (reader.Read())
                    {
                        textBox1.Text = reader.GetString(0);
                        textBox1.Text += " " + reader.GetString(1);
                        textBox1.Text += " " + reader.GetString(2);
                        if (Info.flag == 1)
                        {
                            textBox2.Text = reader.GetString(3);
```

```
                textBox3.Text = reader.GetString(4);
                            }
                            else
                            {
                                textBox2.Text = "Конфіденційна інформація";
                                textBox2.ForeColor = Color.Red;
                                textBox3.Text = "Конфіденційна інформація";
                                textBox3.ForeColor = Color.Red;
                            }
                        }
                    }
                    else MessageBox.Show("Помилка: немає зв'язку з базою данних", "Помилка");
                    reader.Close();
                    connection.Close();
                }



            }

            private void Podrobutsi_FormClosing(object sender, FormClosingEventArgs e)
            {
                Thread.Sleep(1000);
            }

            private void panel3_Paint(object sender, PaintEventArgs e)
            {

            }

            private void panel2_Paint(object sender, PaintEventArgs e)
            {

            }
        }
    }
```

ДОДАТОК Б

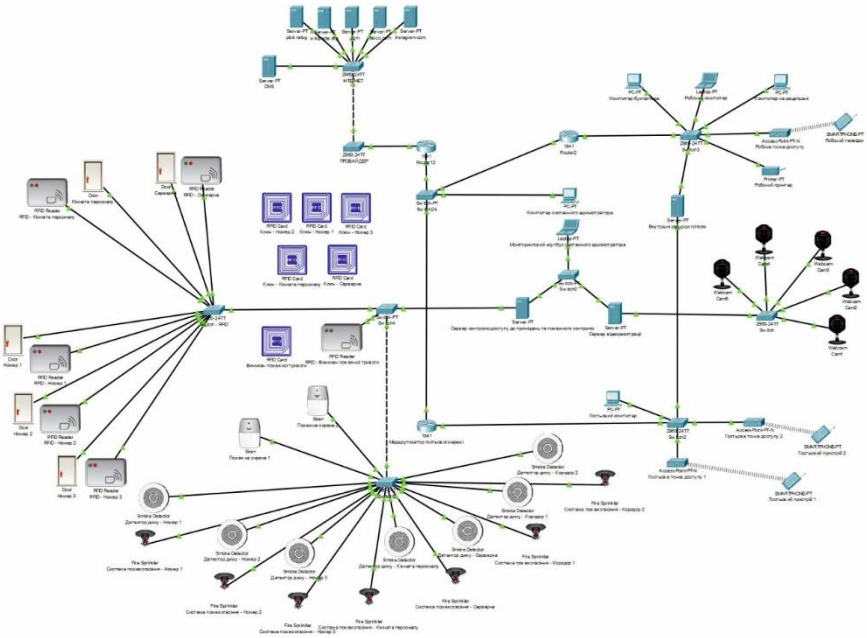
(обов’язковий)

Копія графічної частини



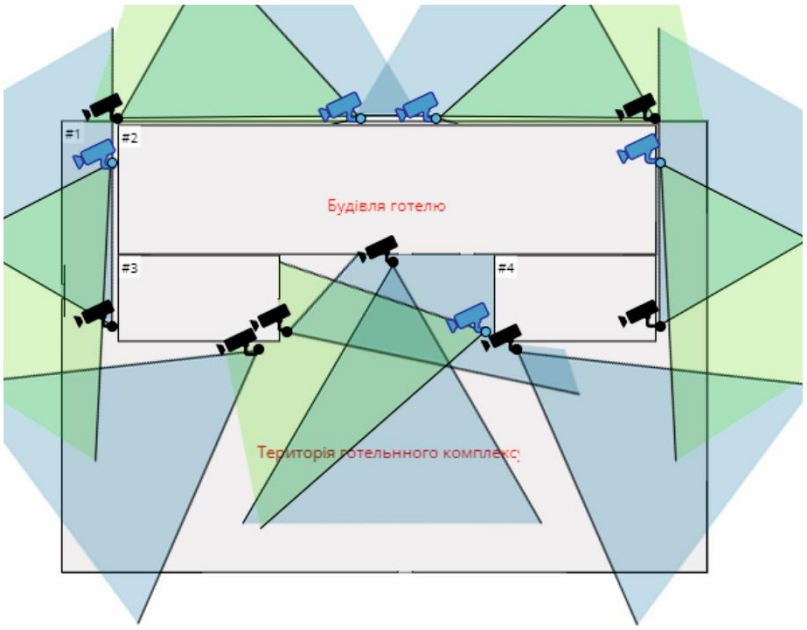
№	Потенційні загрози для інформації	Ризики для:		
		К	Ц	Д
	1 Загрози зі сторони персоналу			
1.1	Працівники можуть бути компрометовані третіми особами через підкуп або шантаж.	+	+	+
1.2	Нецільова діяльність, яка виходить за рамки повноважень	+	+	+
1.3	Надлишковість повноважень	+	+/-	+/-
1.4	Використання несанкціонованого робочого місця	+	+	-
1.5	Пошкодження ПК або мережевих пристроїв	-	+	+
1.6	Несанкціонована модифікація або пошкодження службової інформації	-	+/-	+/-
1.7	Передача службової інформації, включаючи персональні дані клієнтів та працівників	+	-	-
1.8	Несанкціоноване друкування та копіювання інформації	+	-	-
1.9	Шпигунство, збір персональних даних	+	-	-
	2 Загрози зі сторони клієнтів готелю			
2.1	Подання неточних персональних даних	+	+	-
2.2	Використання корпоративних ресурсів, включаючи робочі місця працівників та внутрішню мережу	+	+	+
2.3	Нелегальне перехоплення розмов та відео-моніторинг працівників готелю або інших клієнтів	+	-	-
1	2	3	4	5
2.4	Злочинне заволодіння внутрішніми документами у паперовому або електронному форматі	+	+/-	+/-

№	Порушник	Категорія порушника	Кваліфікація	Мотив	Можливості щодо подолання	Можливості за місцем дії	Можливості за часом дії	Сума загроз
1 Внутрішні порушники, по необережності								
1.1	Адміністратор	ПВ4	К2	М1	З2	Д4	Ч3	15
1.2	Бухгалтер	ПВ3	К2	М1	З2	Д2	Ч3	12
1.3	Менеджер	ПВ3	К2	М1	З2	Д2	Ч3	12
1.4	Технічний персонал	ПВ1	К1	М1	З1	Д3	Ч3	10
2 Внутрішні порушники, з метою отримання вигоди								
2.1	Адміністратор	ПВ4	К2	М3	З2	Д4	Ч3	17
2.2	Бухгалтер	ПВ3	К2	М3	З2	Д2	Ч3	15
2.3	Менеджер	ПВ3	К2	М3	З2	Д2	Ч3	15
2.4	Технічний персонал	ПВ1	К1	М3	З1	Д3	Ч3	12
3 Зовнішні порушники, по необережності								
3.1	Хакер	ПЗ3	К4	М3	З4	Д1	Ч3	18
3.2	Клієнт	ПЗ1	К2	М2	З2	Д1	Ч3	11
3.3	Рекетир	ПЗ3	К1	М3	З1	Д4	Ч4	16
4Зовнішні порушники, з метою отримання вигоди								
4.1	Хакер	ПЗ4	К4	М4	З4	Д1	Ч4	21
4.2	Клієнт	ПЗ1	К2	М3	З2	Д1	Ч3	12
4.3	Рекетир	ПЗ4	К2	М4	З1	Д4	Ч4	19

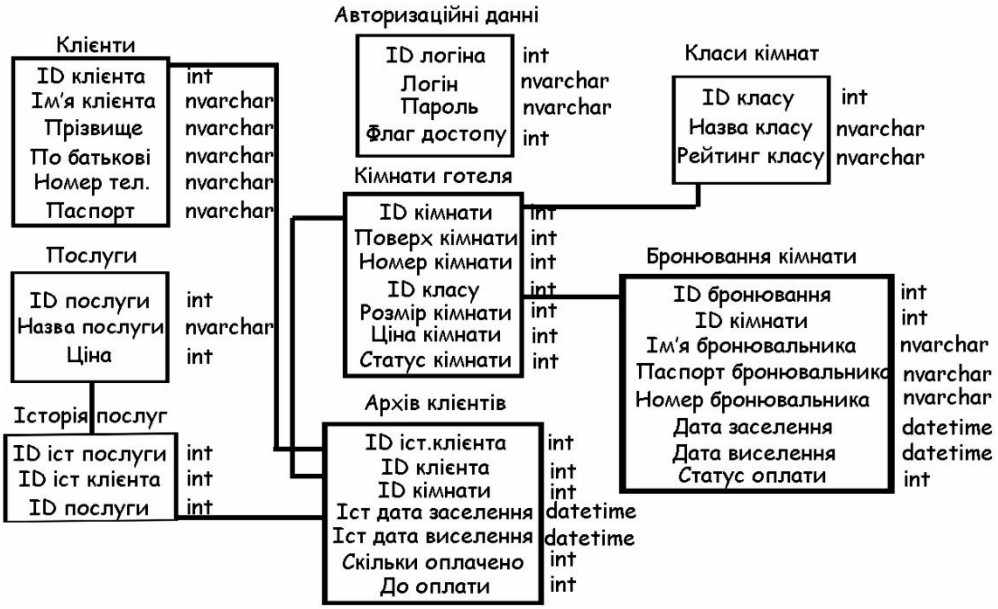


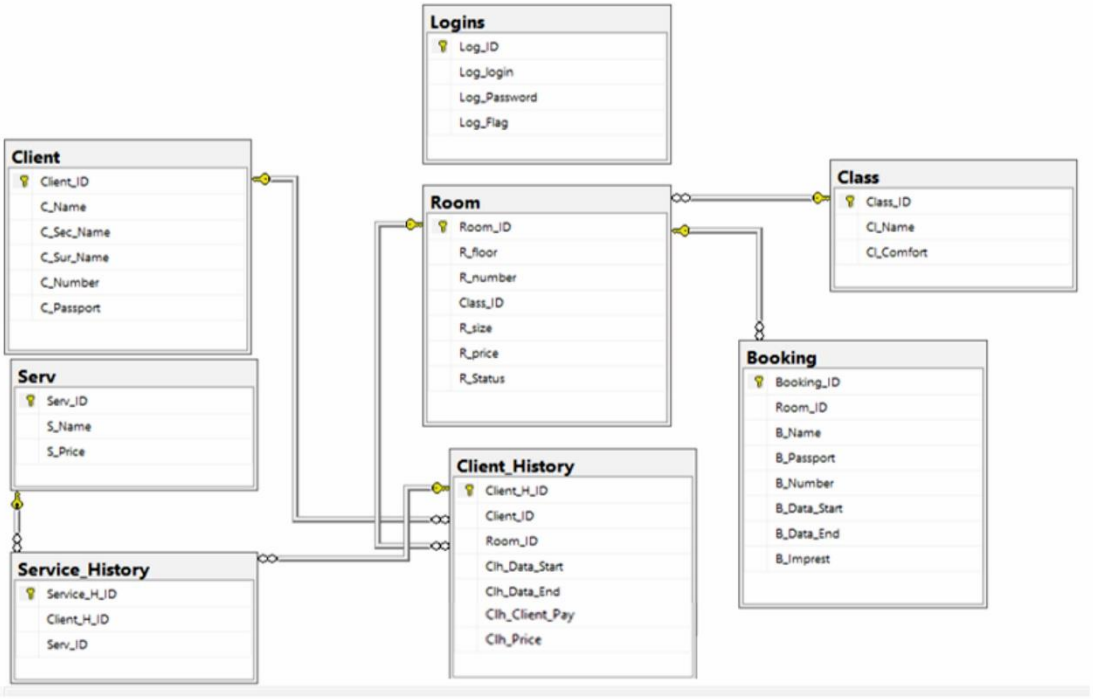
						КРКБ.189130.19.01.07 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Жуков Р.О.				Система контролю доступу готельного комплексу "Coliseum" Функціональна схема мережі та системи контролю доступу	Літера / Маса / Масштаб
Перевір.		Орлов В.С.					
Н.Контр.							Аркуш / Аркушів
Т.Контр.		Мостовий С.В.					ХНУ, КІ2 19 2
Затв.		Клець Ю.П.					

КРКБ.189130.19.01.07 Е8



						КРКБ.189130.19.01.07 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Жуков Р.О.				Система контролю доступу готельного комплексу "Coliseum" Система відеоспостереження	Літера / Маса / Масштаб
Перевір.		Орлов В.С.					
Н.Контр.							Аркуш / Аркушів
Т.Контр.		Мостовий С.В.					ХНУ, КІ2 19 2
Затв.		Клець Ю.П.					





						КРКБ.189130.19.01.07 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Система контролю доступу готельного комплексу "Coliseum" Модель бази даних	Літера	Маса	Масштаб
Розроб.		Жаліс Р.Л.						
Перевір.		Одинко В.С.				Аркуш	Аркушів	
Н.Контр.								
Т.Контр.		Мостовой С.В.				ХНУ, КБ–19–1		
Затв.		Кльоц Ю.П.						

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система контролю доступу готельного комплексу "Coliseum"

Автор: Житнік Роман Леонідович

Спеціальність: 125 – Кібербезпека

Освітня програма: Освітньо-професійна

Науковий керівник: Орленко В.С.

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих методів та технологій, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 6.77% і адресується до 363 першоджерел, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ В.С. Орленко

Завідувач кафедри КБ, гарант ОП _____ Ю.П. Кльоц

Дата: 07.06.2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Житнік Роман Леонідович

Тема Система контролю доступу готельного комплексу "Coliseum"

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 5; кількість сторінок записки 64.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі проведено аналіз фізичної та інформаційної структури готельного комплексу "Колізей". Результати аналізу були використані для розробки індивідуальної системи захисту інформації, яка забезпечує безпечне функціонування готелю відповідно до його комерційного призначення.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі висвітлюється актуальність теми роботи, дається аналіз досліджуваної проблеми і обґрунтовується застосовуваний підхід до її вирішення, формулюються цілі і завдання. У першому розділі розглядаються аналізуються підходи до побудов систем контролю доступу. Наступні розділи присвячені розробці моделей порушника, загроз. Враховуючи їх запропоновано структуру ситеми контролю доступу, розроблене програмне забезпечення, та розраховано собівартість

4. Позитивні сторони роботи Кваліфікаційна робота містить ряд інноваційних рішень, зокрема, запропоновано підхід до захисту інформації, який забезпечує безпечне функціонування готелю відповідно до його комерційного призначення

5. Негативні сторони роботи роботи Не розроблено веб-додаток для інформаційної системи готелю

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження Окремі описи в пояснювальній записці подано занадто деталізовано, що ускладнює сприйняття матеріалу фахівцями в обраній предметній галузі.

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
д.т.н., професор Лисенко С.М.

« 07 » 06 2023. (підпис)

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

Дата перевірки:
06.06.2023 22:22:36 EEST

Дата звіту:
06.06.2023 22:33:30 EEST

ID перевірки:
1015471184

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100008300

Назва документа: Житнік

Кількість сторінок: 63 Кількість слів: 12148 Кількість символів: 92096 Розмір файлу: 1.94 MB ID файлу: 1015129509

6.77%
Схожість

Найбільша схожість: 1.07% з джерелом з Бібліотеки (ID файлу: 1011358693)

5.95% Джерела з Інтернету	390	Сторінка 65
3.08% Джерела з Бібліотеки	73	Сторінка 68

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

6.33%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 8 слів та 0%)

5.56% Вилучення з Інтернету	3	Сторінка 69
6.33% Вилученого тексту з Бібліотеки	164	Сторінка 69

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 2.0%

Словники перевірки: en_US. ru_RU. ua_UA. Помилок в документах: 6%

	Документ		Сумарний збіг по Базі Даних	
ID: 115003 Назва: Система контролю доступу готельного комплексу "Coliseum" Додано в БД: 2023-06-06 Автора: Житнік Р.Л. Керівники: Орленко В.С. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	69851	1064	3401 (5%)	50 (5%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми