Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Хоптинця Богдана Олександровича

на здобуття ступеня вищої освіти Бакалавра

Система контролю доступу для готельного комплексу

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

КРБКБ.220131.22.01.20 ПЗ

Виконав студент 4 курсу, група КБ-22-1 _____ Богдан ХОПТИНЕЦЬ
Підпис, дата — Ініціали, прізвище

Керівник доктор тех. наук, професор _____ Михайло КАСЯНЧУК
Науковий ступінь, вчене звання — Підпис, дата — Ініціали, прізвище

Нормоконтролер д-р філософії _____ Наталія ПЕТЛЯК
Науковий ступінь, вчене звання — Підпис, дата — Ініціали, прізвище

До захисту допускаю:

Зав. кафедри кібербезпеки _____ Юрій КЛЬОЦ
Підпис, дата — Ініціали, прізвище

16 06 2026р.

Хмельницький, 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ
20 січня 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Хоптинця Богдана Олександровича

1 Тема роботи Система контролю доступу готельного комплексу «Optima Collection Khmelnytskyi»
Керівник роботи к.т.н, доц. зав. кафедри кібербезпеки Юрій Павлович Кльоц
Затверджено наказом ректора університету від 20 січня 2026 № 7
2 Строк подання студентом кваліфікаційної роботи на кафедру _____
3 Вихідні дані до роботи розробити комплексну систему контролю доступу для готельного комплексу на основі аналізу його інфраструктури, побудови моделі загроз та вимог щодо розмежування прав доступу до фізичних приміщень і критичних інформаційних ресурсів.
4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Аналіз предметної області та інформаційної структури готельного комплексу. Визначення об'єктів захисту, розробка моделі загроз та моделі порушника. Проєктування системи фізичного захисту внутрішніх приміщень і контролю периметру. Розробка захищеної корпоративної мережевої інфраструктури та проєктування реляційної бази даних системи доступу. Оцінка функціональних характеристик, економічної доцільності впровадження та розробка рекомендацій для реалізації.
5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Структурна схема об'єкта та рівнів доступу. Модель загроз та реагування на інциденти. Архітектура захищеної корпоративної мережевої системи. ER-модель (структура) бази даних системи контролю доступу.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Петляк Н.С., д-р філософії, доцент кафедри кібербезпеки		

7 Дата видачі завдання 20 січня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	лютий	
Ознайомлення з предметною областю	лютий	
Дослідження існуючих рішень	лютий	
Постановка задачі	березень	
Визначення загальних принципів рішення задачі	березень	
Деталізація принципів рішення задачі	квітень	
Розробка проєктних рішень	квітень	
Апробація проєктних рішень	травень	
Оформлення пояснювальної записки згідно вимог	травень	
Оформлення графічної частини	червень	
Захист КР	червень	

Студент _____ Богдан ХОПТИНЕЦЬ

Керівник кваліфікаційної роботи _____ Михайло КАСЯНЧУК

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система контролю доступу для готельного комплексу».

Авторка роботи: Хоптинець Богдан Олександрович

Керівник роботи: Кльоц Юрій Павлович

Пояснювальна записка: 65 с., 2 додатки, 10 рис., 4 табл., 40 джерела.

Графічна частина: 3 плакати.

Ключові слова: система контролю доступу, СКУД, готельний комплекс, фізична безпека, інформаційна безпека, відеоспостереження, модель загроз, база даних, корпоративна мережа.

У кваліфікаційній роботі розроблено комплексну систему контролю доступу для готельного комплексу «Optima Collection Khmelnytskyi», яка забезпечує інтегрований фізичний та інформаційний захист об'єкта. Проведено аналіз сучасного стану безпеки готельних комплексів, визначено вразливості інформаційної структури та критичні активи. Сформовано модель загроз і модель потенційного порушника. Запропоновано багаторівневу архітектуру захисту, що поєднує периметровий контроль, електронні засоби ідентифікації (на базі RFID/NFC технологій) та систему відеоспостереження. Спроєктовано захищену корпоративну мережеву інфраструктуру з використанням VLAN-сегментації та розроблено структуру реляційної бази даних для централізованого управління доступом і журналювання подій. Виконано оцінку собівартості впровадження та надано практичні рекомендації щодо монтажу й експлуатації комплексу. Доведено економічну та функціональну доцільність інтеграції всіх підсистем безпеки в єдине середовище управління.

17.06.2026

ABSTRACT

Theme of the qualification work: Access Control System of the Hotel Complex.

Author of the work: Khoptynets Bohdan Oleksandrovych.

Supervisor: Klots Yurii Pavlovych.

Explanatory note: 65 p., 2 appendices, 10 figures, 4 tables, 40 references.

Graphic part: 3 posters

Keywords: access control system, ACS, hotel complex, physical security, information security, video surveillance, threat model, database, corporate network.

The qualification thesis develops a comprehensive access control system for the hotel complex "Optima Collection Khmelnytskyi", providing integrated physical and information security of the facility. An analysis of the current state of hotel security was conducted, identifying vulnerabilities in the information structure and critical assets. A threat model and a potential intruder model were formed. A multi-level security architecture combining perimeter control, electronic identification means (based on RFID/NFC technologies), and video surveillance is proposed. A secure corporate network infrastructure using VLAN segmentation was designed, and a relational database structure for centralized access management and event logging was developed. The cost of implementation was evaluated, and practical recommendations for the installation and operation of the complex were provided. The economic and functional feasibility of integrating all security subsystems into a single management environment has been proven.

17.06.2026

ЗМІСТ

ВСТУП

Стрімка цифровізація бізнес-процесів у сфері гостинності зумовлює підвищені вимоги до забезпечення фізичної та інформаційної безпеки готельних комплексів. Сучасний готель функціонує не лише як об’єкт розміщення клієнтів, але й як інтегрована інформаційна система, що обробляє значні обсяги персональних, фінансових та службових даних. У таких умовах питання контролю доступу набуває стратегічного значення.

Готельний комплекс «Optima Collection Khmelnytskyi» є комерційним об’єктом із розвиненою інфраструктурою, який щоденно забезпечує обслуговування великої кількості клієнтів. У процесі діяльності здійснюється реєстрація гостей, ведення бухгалтерського обліку, обробка персональних даних, функціонування внутрішньої мережі, систем відеоспостереження та автоматизованих сервісів. Наявність таких процесів формує комплекс потенційних загроз як фізичного, так і кібернетичного характеру.

Недостатній рівень контролю доступу в готельному комплексі створює низку критичних загроз, найпершою з яких є ризик несанкціонованого проникнення сторонніх осіб до службових та технічних приміщень. Це стає підґрунтям для витоку конфіденційної інформації, зокрема персональних даних клієнтів, що зберігаються в базах даних готелю. Окрім цього, вразливість системи може призвести до прямої компрометації фінансової інформації, включаючи дані про транзакції та банківські реквізити, що ставить під удар економічну безпеку закладу.

Збій у системі розмежування прав доступу також здатен спричинити порушення безперервності роботи готелю, оскільки несанкціоноване втручання в інженерні або ІТ-системи може паралізувати операційну діяльність. У підсумку, сукупність цих факторів неминуче призводить до значних репутаційних та матеріальних втрат, що ставить під загрозу конкурентоспроможність готельного комплексу на ринку.

Особливої актуальності проблема набуває в умовах зростання кількості

кібератак, внутрішніх інцидентів безпеки та необхідності дотримання вимог законодавства щодо захисту персональних даних.

Таким чином, створення комплексної системи контролю доступу, що інтегрує фізичні, технічні та програмні засоби захисту, є необхідною умовою стабільного функціонування готельного комплексу.

Метою бакалаврської кваліфікаційної роботи є розробка комплексної системи контролю доступу для готельного комплексу «Optima Collection Khmelnytskyi», яка забезпечує захист фізичних приміщень та інформаційних ресурсів від внутрішніх і зовнішніх загроз.

Для досягнення поставленої мети необхідно:

– провести аналіз предметної області та дослідити особливості функціонування готельного комплексу;

– виконати первинне обстеження об’єкта та оцінити існуючий рівень безпеки;

– проаналізувати інформаційні потоки та визначити критичні ресурси;

– розробити модель загроз та модель порушника;

– спроєктувати систему фізичного захисту та контролю периметру;

– розробити архітектуру програмно-апаратної системи контролю доступу;

– спроєктувати структуру бази даних системи;

– оцінити економічну доцільність впровадження.

Об’єктом дослідження є процес забезпечення фізичної та інформаційної безпеки готельного комплексу. Предметом дослідження є методи, засоби та технології побудови системи контролю доступу в умовах функціонування сучасного готельного комплексу.

Розроблена система може бути використана як модель впровадження для готельних закладів середнього класу та адаптована до конкретних умов експлуатації.

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз предметної області і виявлення наявних проблем і завдань

Сфера готельного бізнесу належить до об’єктів з підвищеним рівнем відповідальності щодо захисту інформації та фізичної безпеки. Сучасний готель функціонує як складна організаційно-технічна система, що поєднує, сучасний готель функціонує як складна організаційно-технічна система, що базується на тісній інтеграції різнорідних підсистем та сервісів. Фундаментом операційної діяльності є автоматизована система розміщення гостей, яка синхронізована з фінансово-бухгалтерськими процесами для забезпечення прозорості розрахунків та звітності. Паралельно з цим функціонує кадрова система, що відповідає за управління персоналом та розмежування посадових обов'язків.

Інформаційна стійкість закладу забезпечується через чіткий поділ мережевої інфраструктури на внутрішню корпоративну мережу для службового користування та окрему гостьову мережу Wi-Fi, що дозволяє мінімізувати ризики кіберзагроз. Фізична безпека об'єкта підтримується завдяки комплексному використанню систем відеоспостереження та автоматизованих інженерних систем. До останніх належать система контролю та управління доступом, пожежна сигналізація та модулі контролю клімату, які в сукупності створюють захищене та комфортне середовище для перебування клієнтів і роботи персоналу.

Об’єктом дослідження у даній роботі є готельний комплекс Optima Collection Khmelnytskyi, який відноситься до закладів середнього класу з розвиненою інфраструктурою обслуговування.

Особливістю готельних комплексів є постійна ротація клієнтів, наявність відкритих громадських зон та одночасне функціонування службових приміщень з обмеженим доступом. Це створює специфічне середовище, в якому необхідно забезпечити: у межах функціонування готельного комплексу особлива увага повинна приділятися створенню специфічного безпекового середовища, яке б гарантувало надійне розмежування прав доступу між обслуговуючим

персоналом та гостями закладу. Це передбачає впровадження механізмів суворого контролю переміщення осіб у внутрішніх та службових приміщеннях, куди доступ клієнтам має бути обмежений. Окрім фізичної безпеки, пріоритетним завданням є комплексний захист персональних даних клієнтів від будь-яких форм компрометації чи несанкціонованого копіювання. Усі ці заходи в сукупності мають бути спрямовані на підтримку безперервності роботи ключових інформаційних систем готелю, оскільки будь-який технічний збій або втручання в їхню роботу може паралізувати надання послуг та завдати значних репутаційних збитків.

Аналіз сучасних готельних комплексів дозволяє виділити типові проблеми безпеки [27, с. 45]: аналіз сучасного стану безпеки готельних комплексів дозволяє виділити низку типових проблем, серед яких найбільш критичною є відсутність чіткого розмежування рівнів доступу для різних категорій осіб. Ситуація ускладнюється тривалим використанням застарілих механічних замків, які не дозволяють гнучко керувати правами доступу та відстежувати історію відкриттів. З боку IT-інфраструктури спостерігається недостатня сегментація внутрішньої мережі, що в поєднанні з низьким рівнем журналювання подій робить систему вразливою до прихованих атак. Відсутність централізованого моніторингу не дозволяє службі безпеки оперативно реагувати на загрози, а вагомий вплив людського фактора підвищує ймовірність виникнення внутрішніх інцидентів.

Такі недоліки створюють умови для реалізації потенційних ризиків, що притаманні готельному бізнесу. Зокрема, стає можливим безперешкодне проникнення сторонніх осіб у службові зони, а також використання відкритої гостьової мережі як плацдарму для атак на внутрішню IT-інфраструктуру об'єкта. Наслідком таких дій може стати масштабний витік персональних даних клієнтів або компрометація фінансової інформації, що завдає прямої економічної шкоди. Крім того, не можна виключати ризик фізичного пошкодження дороговартісного обладнання через недостатній контроль за критичними зонами готелю.

Система контролю доступу повинна бути інтегрованою та включати, реалізація комплексного підходу до безпеки готельного комплексу передбачає впровадження багатошарової системи захисту, що охоплює як фізичні, так і цифрові аспекти. Першочерговим завданням є організація надійного фізичного контролю периметру об'єкта, що доповнюється сучасною електронною системою доступу до приміщень на базі технологій RFID та NFC. Ефективність такої системи забезпечується через створення централізованої бази даних користувачів, яка дозволяє гнучко керувати правами доступу в режимі реального часу. Для візуального контролю та верифікації інцидентів інтегрується інтелектуальне відеоспостереження з обов’язковим архівуванням даних, що працює в єдиному комплексі із системою логування та безперервного моніторингу всіх подій безпеки.

Окрім технічних засобів фізичної безпеки, особлива увага приділяється захисту інформаційного простору шляхом впровадження мережевої сегментації. Це дозволяє ізолювати критичні вузли системи від загального доступу та мінімізувати площу потенційних атак. Для гарантування стабільної роботи в екстремальних умовах передбачається обов'язкове резервування критичних компонентів системи. Таке поєднання інструментів дозволяє розробити комплексну архітектуру, яка є максимально адаптованою до специфічних умов функціонування конкретного готельного комплексу.

Таким чином, виникає необхідність розробки комплексної архітектури СКУД, адаптованої до умов функціонування конкретного готельного комплексу.

1.2 Первинне дослідження об’єкта

Optima Collection Khmelnytskyi

Первинне дослідження об’єкта передбачає аналіз фізичних характеристик готельного комплексу, його територіального розташування, інженерної інфраструктури та існуючих засобів безпеки.

Готельний комплекс розташований у межах міської забудови та має зручний доступ до транспортної інфраструктури. Такий фактор, з одного боку, забезпечує високу доступність для клієнтів, а з іншого — створює додаткові ризики несанкціонованого проникнення та спостереження за об’єктом (див. рис. 1.1 та 1.2).

Рисунок 1.1 - Об’єкт дослідження

Рисунок 1.2 - Об’єкт дослідження з середини

Територія готелю включає:

- основну будівлю;
- зону центрального входу;
- технічні входи для персоналу;
- паркувальний майданчик;
- господарську зону.

На основі аналізу території встановлено, що периметр об’єкта контролюється лише частково, а відкритий характер фасадної частини будівлі створює додаткові безпекові виклики. Це зумовлює гостру потребу у впровадженні розширеної мережі засобів відеоспостереження та безперервного моніторингу ключових зон ризику. Особливої уваги в цьому контексті потребують службові входи, через які здійснюється рух персоналу та підрядників, а також завантажувальна зона, де постійна ротація транспортних засобів та вантажів підвищує ймовірність несанкціонованого проникнення. Крім того, критичними точками є місця можливого доступу до інженерних комунікацій, оскільки будь-яке втручання в роботу систем життєзабезпечення готелю може призвести до зупинки його функціонування.

Будівля готелю має декілька поверхів та включає:

- рецепцію та адміністративну зону;
- номерний фонд;
- конференц-зали;
- ресторанну зону;
- службові приміщення;
- серверну та технічні кімнати.

Наявність громадських зон (вестибюль, ресторан, конференц-зал) ускладнює реалізацію повного фізичного контролю без створення дискомфорту для гостей. Тому система контролю доступу повинна бути максимально інтегрованою та непомітною для клієнтів.

Об’єкт підключений до міських систем:

- електропостачання;

- водопостачання;
- каналізації;
- телекомунікаційних мереж;
- інтернет-провайдерів.

У готелі функціонують:

- система пожежної сигналізації;
- система відеоспостереження;
- гостьова Wi-Fi мережа;
- внутрішня корпоративна мережа.

Проведений аналіз показав, що існуючі системи безпеки працюють автономно та не інтегровані в єдину систему управління, що знижує ефективність реагування на інциденти.

За результатами первинного дослідження визначено такі потенційні слабкі місця, як відсутність централізованого контролю доступу до службових приміщень.

Обмежене журналювання подій входу/виходу; недостатня сегментація мережевої інфраструктури; відсутність інтеграції відеоспостереження з системою контролю доступу; ризик використання гостьової мережі для спроб несанкціонованого доступу до внутрішніх ресурсів.

Первинне обстеження показало, що готельний комплекс потребує впровадження комплексної системи контролю доступу, яка повинна: забезпечувати багаторівневе розмежування доступу; інтегрувати фізичні та інформаційні механізми захисту; передбачати централізований моніторинг; мінімізувати людський фактор.

1.3 Аналіз інформаційної структури об’єкта захисту Optima Collection Khmelnytskyi

Функціонування сучасного готельного комплексу супроводжується постійною генерацією, обробкою, зберіганням та передачею значних обсягів

інформації. Інформаційна структура готелю являє собою сукупність апаратних, програмних, мережевих та організаційних компонентів, які забезпечують виконання основних бізнес-процесів.

На відміну від підприємств закритого типу, готельний комплекс характеризується високим рівнем відкритості для зовнішніх осіб, що суттєво ускладнює побудову ефективної системи захисту. Саме тому аналіз інформаційної структури є ключовим етапом у процесі розробки системи контролю доступу.

Загальна характеристика інформаційного середовища готельного комплексу охоплює широкий спектр технологічних рішень, що забезпечують автоматизацію ключових бізнес-процесів. Основу структури складають автоматизовані робочі місця адміністрації, на яких розгорнуто спеціалізоване бухгалтерське програмне забезпечення та систему управління бронюванням номерів. Ефективність внутрішньої взаємодії підтримується за допомогою електронного документообігу та корпоративної локальної мережі, яка функціонує паралельно з гостьовою бездротовою мережею Wi-Fi. Надійність фізичного захисту та збереження даних забезпечується інтегрованою системою відеоспостереження, потужним серверним обладнанням, а також спеціалізованими системами зберігання резервних копій, що гарантують відновлення інформації у критичних ситуаціях.

Всі інформаційні процеси в готелі відбуваються безперервно, тому будь-яке їх порушення або збій у роботі IT-інфраструктури може мати критичні наслідки. Найперше, це призводить до значних фінансових втрат через неможливість обробки платежів та бронювань. Крім того, технічні помилки спричиняють суттєве зниження довіри клієнтів та можуть стати причиною виникнення юридичної відповідальності за порушення умов обслуговування чи захисту даних. У найгіршому випадку вихід з ладу інформаційних систем призводить до повної зупинки операційної діяльності закладу, що ставить під загрозу існування готельного комплексу в цілому.

Персонал готельного комплексу за рівнем доступу до інформаційних та

фізичних ресурсів доцільно розділити на дві основні категорії. До першої групи належить адміністративний персонал, що включає директора, адміністраторів рецепції, менеджерів різних ланок та працівників бухгалтерії. Ця категорія користувачів наділяється розширеними правами, оскільки їхня професійна діяльність потребує постійного доступу до персональних даних клієнтів, фінансової звітності та внутрішньої документації підприємства. Окрім того, адміністративний склад має повноваження для роботи з централізованою системою бронювання та доступ до серверних ресурсів, що необхідно для оперативного управління закладом.

Другу групу складає технічний та обслуговуючий персонал, зокрема покоївки, технічні працівники, служба охорони та інші співробітники допоміжних підрозділів. Для цієї категорії передбачається впровадження моделі обмеженого доступу, який надається виключно в межах, необхідних для виконання конкретних службових обов'язків. Такий підхід дозволяє мінімізувати ризики внутрішніх загроз та забезпечити суворе розмежування прав, де кожен працівник має доступ лише до тих зон чи інформаційних масивів, що безпосередньо стосуються його поточної роботи.

Окрему категорію користувачів складають клієнти готелю, для яких права доступу обмежуються виключно зонами загального користування та забронюваними житловими приміщеннями. Гості мають санкціонований доступ до власних номерів, громадських зон закладу та гостьової бездротової мережі Wi-Fi, що забезпечує необхідний рівень комфорту під час перебування. Разом з тим, архітектура системи безпеки повинна бути побудована таким чином, щоб будь-яка можливість доступу клієнтів до внутрішніх інформаційних ресурсів, баз даних або службових мереж готелю була повністю виключена. Такий підхід гарантує цілісність конфіденційної корпоративної інформації та запобігає випадковому або навмисному втручанню сторонніх осіб у роботу критичної інфраструктури.

Інформаційні потоки можна поділити на три основні категорії:

1. Внутрішні інформаційні потоки:

- обмін даними між відділами;
- обробка бронювань;
- фінансові операції;
- передача управлінських рішень.

2. Зовнішні інформаційні потоки:

- взаємодія з клієнтами;
- онлайн-бронювання через зовнішні платформи;
- електронна пошта;
- взаємодія з банківськими системами.

3. Гостьові інформаційні потоки:

- підключення до Wi-Fi;
- використання IPTV та цифрових сервісів;
- мобільні додатки.

Особливу небезпеку становить перетин гостьових та корпоративних потоків у разі відсутності належної мережевої сегментації.

У процесі аналізу визначено наступні критичні активи: База даних клієнтів; фінансова інформація; серверна інфраструктура; система відеоспостереження; логи доступу та журналювання подій; облікові записи персоналу.

Порушення конфіденційності, цілісності або доступності цих активів може мати критичні наслідки.

Проведений аналіз інформаційної інфраструктури готелю дозволив виокремити низку критичних ризиків, що можуть суттєво вплинути на загальний рівень безпеки закладу. Найбільш розповсюдженою технічною загрозою є використання слабких паролів та повна відсутність механізмів багатофакторної автентифікації, що робить облікові записи персоналу легко вразливими до зламу. Ситуація погіршується постійною загрозою проведення фішингових атак, спрямованих на співробітників готелю з метою викрадення їхніх облікових даних. Крім зовнішніх загроз, існують значні внутрішні ризики, зокрема зловживання повноваженнями з боку персоналу, що має доступ до

конфіденційних масивів інформації.

Додатковим фактором небезпеки є можливість несанкціонованого фізичного доступу до серверного обладнання, що може призвести до прямого втручання в роботу критичних вузлів системи або викрадення фізичних носіїв даних. Ризики ускладнюються відсутністю інтегрованої централізованої системи логування, через що виявлення та розслідування інцидентів безпеки стає вкрай складним або неможливим завданням. Усі ці фактори підкреслюють необхідність впровадження комплексних заходів захисту, які б охоплювали як цифрові, так і фізичні аспекти безпеки готельного комплексу.

Система контролю доступу в межах сучасного готельного комплексу повинна базуватися на комплексному підході та охоплювати всі критичні рівні безпеки об'єкта. Це передбачає суворий контроль фізичного доступу до приміщень різного призначення, що працює в єдиній зв'язці з механізмами логічного доступу до інформаційних ресурсів готелю. Фундаментом такої архітектури є чітке розмежування прав доступу, що дозволяє надавати повноваження користувачам згідно з їхньою роллю в системі. Для оперативного реагування на загрози необхідно забезпечити постійний моніторинг усіх подій безпеки в режимі реального часу. Крім того, важливою складовою є функціонал для проведення аудиту та глибокого аналізу інцидентів, що дозволяє не лише виявляти порушення, а й запобігати їх виникненню в майбутньому через усунення виявлених вразливостей.

Завдяки детальному аналізу інформаційної архітектури готельного комплексу було успішно проведено класифікацію співробітників за відповідними рівнями доступу до ресурсів закладу. Це дозволило чітко окреслити основні інформаційні потоки всередині організації та ідентифікувати найбільш вразливі й критично важливі активи, що потребують посиленого захисту. Крім того, у ході дослідження було виявлено та систематизовано потенційні загрози, які можуть дестабілізувати роботу об'єкта. Сформовані таким чином висновки створюють необхідне підґрунтя для чіткого формулювання постановки задачі та подальшого проектування ефективної

системи контролю та управління доступом.

На основі проведеного аналізу предметної області, первинного дослідження об’єкта та оцінки інформаційної структури готельного комплексу Optima Collection Khmelnytskyi встановлено необхідність розробки комплексної системи контролю доступу, яка забезпечить належний рівень фізичної та інформаційної безпеки.

Сучасні умови функціонування готельного бізнесу характеризуються високою динамікою змін, постійною ротацією клієнтів, значним обсягом обробки персональних даних та необхідністю забезпечення безперервності бізнес-процесів. У таких умовах система безпеки повинна бути не лише ефективною, а й адаптивною, масштабованою та інтегрованою.

Основною задачею кваліфікаційної роботи є:

Проєктування комплексної системи контролю доступу готельного комплексу, яка забезпечить розмежування прав доступу до фізичних приміщень та інформаційних ресурсів, мінімізує ризики несанкціонованого проникнення та забезпечить централізований моніторинг подій безпеки.

Для реалізації поставленої задачі необхідно вирішити такі підзадачі: Визначити перелік об’єктів захисту; провести класифікацію приміщень за рівнем доступу; сформувати модель загроз; розробити модель потенційного порушника; спроєктувати фізичну систему контролю доступу (СКУД); забезпечити інтеграцію з відеоспостереженням; розробити архітектуру захищеної корпоративної мережі; спроєктувати структуру бази даних системи; оцінити економічну доцільність впровадження.

Вимоги до системи

1. Система повинна забезпечувати:

- ідентифікацію та автентифікацію користувачів;
- розмежування прав доступу за ролями;
- журналювання подій входу/виходу;
- можливість блокування облікових записів;
- інтеграцію з відеоспостереженням;

- централізоване адміністрування;
- формування звітів про події.

2. Система повинна відповідати таким характеристикам:
   - масштабованість;
   - відмовостійкість;
   - резервування критичних компонентів;
   - захист від несанкціонованого доступу;
   - простота адміністрування;
   - мінімальний вплив на комфорт гостей.

Під час розробки системи необхідно врахувати такі обмеження: Архітектурні особливості будівлі. Обмеження бюджету; необхідність безперервної роботи готелю під час впровадження; відповідність чинному законодавству щодо захисту персональних даних; сумісність із наявними інженерними системами.

Ефективність розробленої системи оцінюватиметься за такими критеріями:

- зниження ймовірності несанкціонованого доступу;
- скорочення часу реагування на інциденти;
- підвищення рівня контролю над переміщенням персоналу;
- забезпечення захисту критичних інформаційних активів;
- економічна доцільність впровадження.

Результатом виконання бакалаврської роботи повинна стати:

- проєктна модель системи контролю доступу;
- архітектурна схема інтеграції компонентів;
- структурна схема мережевої інфраструктури;
- модель бази даних;
- економічне обґрунтування;
- рекомендації щодо практичної реалізації.

Висновок до розділу 1

У першому розділі бакалаврської роботи було здійснено комплексне дослідження предметної області та виконано постановку задачі розробки системи контролю доступу для готельного комплексу Optima Collection Khmelnytskyi.

У процесі аналізу предметної області встановлено, що сучасний готельний комплекс є багатофункціональним об’єктом із підвищеним рівнем динамічності інформаційних та людських потоків. Одночасна присутність гостей, адміністративного персоналу, технічних працівників та сторонніх відвідувачів створює складну систему взаємодії, яка потребує чіткого розмежування доступу до фізичних приміщень та інформаційних ресурсів. Виявлено, що відсутність інтегрованої системи контролю доступу або використання застарілих рішень значно підвищує ризик несанкціонованого проникнення, витоку інформації та матеріальних втрат.

У межах первинного дослідження об’єкта було визначено його структурну організацію, функціональні зони та категорії приміщень. Проведено класифікацію зон за рівнем критичності: публічні приміщення, службові приміщення, зони обмеженого доступу та приміщення з підвищеними вимогами до безпеки (серверні, архіви, технічні кімнати). Встановлено, що ефективна система контролю доступу повинна забезпечувати багаторівневе розмежування прав відповідно до ролей користувачів.

Аналіз інформаційної структури об’єкта дозволив ідентифікувати основні інформаційні активи, серед яких персональні дані клієнтів, внутрішня документація, фінансова інформація, журнали подій безпеки та дані відеоспостереження. Досліджено канали передачі інформації, визначено точки потенційної вразливості та сформовано перелік критичних ресурсів, що потребують пріоритетного захисту. Особливу увагу приділено взаємодії фізичної інфраструктури з корпоративною мережею, оскільки сучасні системи контролю доступу інтегруються з IT-середовищем підприємства.

У результаті проведеного аналізу було виявлено комплекс системних проблем, ключовою з яких є відсутність механізмів централізованого управління доступом та недостатній рівень сегментації внутрішніх приміщень. Ситуація ускладнюється через відсутність автоматизованого журналювання подій, що суттєво обмежує можливості служби безпеки щодо оперативного реагування на інциденти. Окремим фактором ризику залишається значний вплив людського фактору, зумовлений використанням застарілих механічних засобів контролю.

На основі отриманих результатів було сформульовано постановку задачі, яка полягає у проектуванні та впровадженні інтегрованої системи контролю доступу. Майбутнє рішення має забезпечувати суворе розмежування прав доступу до фізичних зон об'єкта та впровадження єдиної платформи для централізованого управління користувачами. Крім того, система повинна реалізовувати повне журналювання подій із можливістю подальшого аудиту, а також підтримувати безшовну інтеграцію із засобами відеоспостереження. Реалізація цих заходів дозволить суттєво підвищити загальний рівень інформаційної та фізичної безпеки готельного комплексу.

Визначено функціональні вимоги до системи, зокрема підтримку електронної ідентифікації, гнучке налаштування ролей, масштабованість, резервування та відмовостійкість. Також сформовано нефункціональні вимоги, що включають надійність, продуктивність, зручність адміністрування та відповідність чинному законодавству щодо захисту персональних даних.

Таким чином, у першому розділі було створено теоретичне та аналітичне підґрунтя для подальшої розробки системи контролю доступу. Проведене дослідження дозволило чітко визначити структуру об’єкта захисту, ідентифікувати основні загрози та сформулювати технічну задачу проєктування. Отримані результати стали основою для розробки моделі загроз, архітектури системи та технічних рішень, що розглядаються у наступних розділах роботи.

2 РОЗРОБКА КОМПОНЕНТІВ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

2.1 Обґрунтування об’єктів захисту

Розробка системи контролю доступу передбачає попередню ідентифікацію та класифікацію об’єктів, що підлягають захисту. Визначення таких об’єктів є ключовим етапом проєктування, оскільки саме від правильності їх виділення залежить ефективність усієї системи безпеки.

У межах даної роботи об’єктом впровадження системи є готельний комплекс Optima Collection Khmelnytskyi, який поєднує житлову, адміністративну, господарську та технічну інфраструктуру (рис. 2.1).

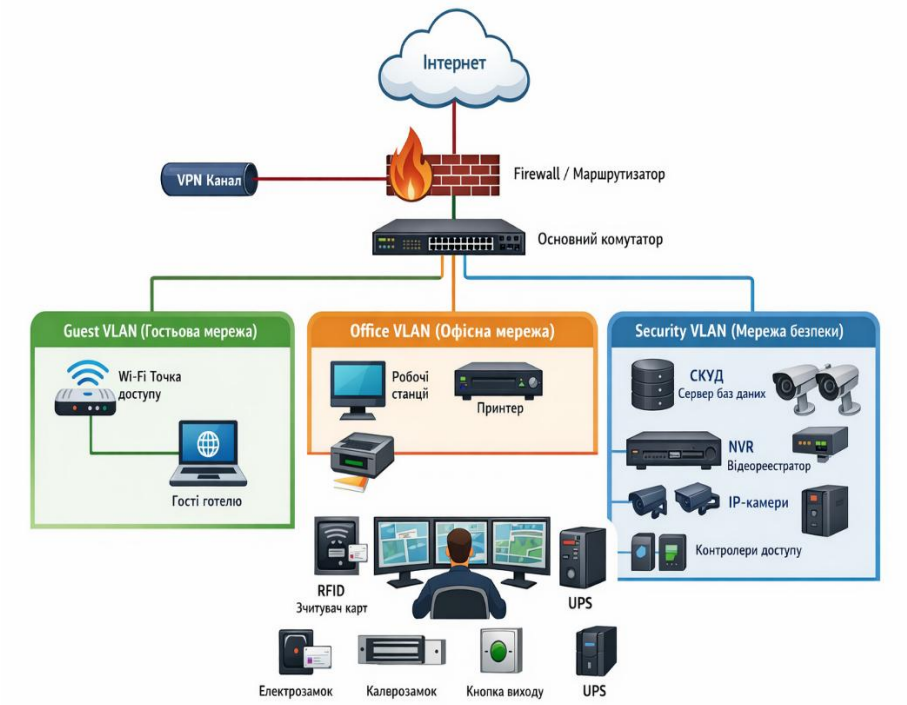


Рисунок 2.1 - Схема об’єкту

Об’єкти захисту доцільно розподілити на такі категорії: Фізичні об’єкти; інформаційні ресурси; технічні засоби; персонал та користувачі системи.

Такий підхід дозволяє забезпечити комплексність проєктування та врахувати як матеріальні, так і нематеріальні активи.

До фізичних об’єктів належать приміщення та зони готельного комплексу,

доступ до яких повинен бути регламентований.

Приміщення готельного комплексу за рівнем режимності доцільно розділити на кілька функціональних зон, першою з яких є зона загального доступу. Вона охоплює вестибюль, зону рецепції, ресторан, конференц-зали та коридори загального користування. Хоча ці локації характеризуються відкритістю для всіх відвідувачів, вони потребують безперервного відеомоніторингу, а в неробочий час - встановлення особливого режиму контролю для запобігання нештатним ситуаціям.

Другу категорію складають зони обмеженого доступу, куди належать адміністративні кабінети, приміщення бухгалтерії, архіви, а також службові кімнати персоналу та складські площі. Вхід до таких приміщень суворо регламентується і має надаватися виключно авторизованим співробітникам відповідно до їхніх безпосередніх посадових обов’язків. Це дозволяє забезпечити конфіденційність робочих процесів та збереження матеріальних цінностей готелю.

Найвищий пріоритет захисту мають зони критичної інфраструктури, що включають серверну кімнату, вузли мережевого обладнання, приміщення з відеореєстраторами, електрощитову та технічні комунікаційні вузли. Будь-яке несанкціоноване проникнення до цих об'єктів несе критичну загрозу, оскільки може спричинити повну зупинку роботи готелю, незворотну втрату даних або масштабну компрометацію інформаційних систем. Як наслідок, порушення безпеки в цій зоні неминуче призводить до значних фінансових та репутаційних збитків для підприємства.

Тому для даної категорії необхідно передбачити багаторівневий контроль доступу з використанням електронних засобів ідентифікації та журналювання подій. До інформаційних об’єктів захисту належать:

- база даних клієнтів;
- фінансова звітність;
- внутрішня документація;
- облікові записи користувачів;

– журнали подій системи безпеки.

Особливої уваги потребують персональні дані клієнтів, що обробляються у процесі бронювання та проживання. Порушення конфіденційності такої інформації може спричинити юридичну відповідальність та репутаційні втрати.

Перелік технічних засобів, що потребують захисту, охоплює ключові вузли інформаційно-комунікаційної мережі готелю. Особлива увага приділяється серверному обладнанню та системам зберігання даних, які є основними сховищами конфіденційної інформації та забезпечують роботу бізнес-додатків. Цілісність мережевої інфраструктури підтримується через захист активного обладнання, зокрема комутаторів та маршрутизаторів, що відповідають за стабільний обмін даними. Безпосередній вплив на безпеку об'єкта мають контролери системи доступу та IP-камери відеоспостереження, оскільки вони формують контур фізичного захисту готелю. Крім того, важливими елементами є робочі станції персоналу, які виступають точками взаємодії співробітників з інформаційним середовищем закладу. Фізична компрометація або логічне втручання в роботу будь-якого з цих компонентів неминуче призводить до порушення цілісності та доступності критично важливої інформації.

Окрему категорію загроз становить персонал готелю, оскільки практичний досвід демонструє, що значна частина інцидентів у сфері безпеки пов’язана саме з діями внутрішніх користувачів. До основних ризиків, що виникають у цьому контексті, належать навмисне або випадкове перевищення службових повноважень, а також використання сторонніх носіїв інформації, що може призвести до зараження систем шкідливим програмним забезпеченням. Крім того, критичними факторами є розголошення службових відомостей третім особам та виникнення помилок у роботі через людський фактор, які можуть мати як випадковий, так і навмисний характер. З огляду на це, проектована система контролю доступу має базуватися на принципі надання мінімально необхідних привілеїв для кожного співробітника, забезпечуючи при цьому безперервне та повне журналювання всіх дій користувачів для можливості подальшого аудиту.

Аналіз об’єктів захисту свідчить про доцільність впровадження

багаторівневої моделі безпеки, що включає: Периметровий контроль; контроль доступу до внутрішніх приміщень; логічний контроль доступу до інформаційних ресурсів; централізований моніторинг подій; систему аудиту та звітності.

Комплексність підходу дозволяє мінімізувати ймовірність реалізації загроз та забезпечити стійкість системи до внутрішніх і зовнішніх впливів.

У результаті обґрунтування об’єктів захисту:

- визначено фізичні, інформаційні та технічні активи;
- класифіковано приміщення за рівнем доступу;
- встановлено критичні зони;
- обґрунтовано необхідність багаторівневого контролю.

Отримані результати є підґрунтям для формування моделі загроз та моделі потенційного порушника.

2.2 Створення моделі загроз та моделі порушника на основі проаналізованих даних

Розробка системи контролю доступу неможлива без формування обґрунтованої моделі загроз та моделі потенційного порушника. Саме ці моделі визначають перелік заходів захисту, рівень складності технічних рішень та архітектуру системи безпеки.

Об’єктом аналізу виступає готельний комплекс Optima Collection Khmelnytskyi, який функціонує як відкрита система з постійною взаємодією із зовнішнім середовищем.

Процес формування моделі загроз базується на комплексному дослідженні архітектури готельного комплексу, що передбачає детальне вивчення фізичної структури об’єкта та аналіз наявних інформаційних потоків. Важливим етапом побудови моделі є класифікація ключових об’єктів захисту, що дозволяє провести об’єктивну оцінку потенційних каналів несанкціонованого доступу та врахувати ризики, зумовлені впливом людського фактору.

При розробці такої моделі ключовим орієнтиром виступають три базові властивості інформації, а саме її конфіденційність, цілісність та постійна доступність для авторизованих користувачів. Варто враховувати, що порушення хоча б однієї з цих характеристик неминуче призводить до виникнення інциденту безпеки, що може мати критичні наслідки для функціонування всього закладу (схема реагування наведена на рис. 2.2).

Рисунок 2.2 Опис реагування на інциденти

Класифікація загроз безпеці готельного комплексу дозволяє виділити групу зовнішніх чинників, що пов’язані з діями осіб, які не мають внутрішніх привілеїв, проте здатні використовувати відкритий характер громадських зон об'єкта. До таких загроз належать спроби несанкціонованого фізичного проникнення до будівлі або безпосередньо до службових приміщень, а також ризики крадіжки дороговартісного обладнання. Окремий пласт складають цифрові загрози, зокрема кібератаки через глобальну мережу, втручання в роботу гостьового сегменту Wi-Fi та застосування методів соціальної інженерії щодо співробітників з метою отримання конфіденційних відомостей.

Більш критичний характер мають внутрішні загрози, оскільки вони

безпосередньо пов’язані з наявністю у правопорушників легітимного авторизованого доступу до систем. У цьому контексті найбільш небезпечними є випадки перевищення службових повноважень або використання робочого доступу в особистих цілях. Це створює умови для несанкціонованого копіювання і передачі конфіденційної інформації третім особам, отримання прямого доступу до серверної інфраструктури, а також створює ризики навмисного виведення з ладу технічних засобів захисту.

Окрім антропогенних чинників, на стабільність функціонування закладу впливають технічні загрози, що мають переважно експлуатаційний характер. До них відносять раптові відмови апаратного забезпечення, критичні перебої в системі електропостачання та програмні збої в роботі спеціалізованого софту. Надійність системи також ставиться під удар через можливі помилки в конфігурації мережевого обладнання або ігнорування процедур регулярного резервного копіювання даних, що в сукупності може призвести до тривалого простою бізнес-процесів.

Ідентифікація каналів реалізації загроз. Можливі канали реалізації загроз: Фізичний доступ через службові входи; використання втрачених або викрадених карт доступу; несанкціоноване підключення до мережевих портів; підбір паролів до облікових записів; використання шкідливого програмного забезпечення; доступ до серверної без належної ідентифікації.

Для проєктування ефективної системи контролю доступу розробляється узагальнена модель порушника, яка дозволяє класифікувати потенційних суб'єктів загроз за їхніми можливостями та намірами.

Перша категорія охоплює зовнішніх порушників, які не володіють легітимними правами доступу до об'єкта, проте характеризуються середнім або високим рівнем підготовки. Такі особи можуть діяти одноразово, застосовуючи різноманітні фізичні або технічні методи для несанкціонованого проникнення в систему. Основним рушійним фактором для них виступає матеріальна вигода, прагнення до викрадення конфіденційної інформації або навмисний саботаж роботи готельного комплексу.

Значно більшу небезпеку становить внутрішній порушник, оскільки він має законний доступ до певних зон та детально обізнаний із внутрішньою структурою та розпорядком роботи закладу. Наявність службових повноважень дозволяє такому суб'єкту діяти приховано протягом тривалого часу. Його мотивація зазвичай ґрунтується на отриманні особистої вигоди, наслідках конфлікту з керівництвом або є результатом елементарної недбалості при виконанні обов'язків.

Окрему групу формує випадковий порушник, дії якого не мають попереднього злого умислу, проте створюють суттєві вразливості в контурі безпеки. Сюди належать ненавмисні помилки персоналу, ігнорування встановлених процедур безпеки та використання слабких паролів, що легко піддаються зламу. Також критичним фактором ризику в цій категорії є передача персональних карт доступу стороннім особам, що нівелює персональну відповідальність та порушує цілісність системи контролю.

Оцінка ризиків

Оцінка ризику здійснюється за формулою:

Ризик = Ймовірність × Наслідки [21]

Результати оцінки для готельного комплексу наведено у таблиці 2.1

Таблиця 2.1 - Основні ризики для готельного комплексу

Загроза	Ймовірність	Наслідки	Рівень ризику
Проникнення до серверної	Середня	Критичні	Високий
Використання гостьової мережі для атак	Висока	Значні	Високий
Втрата картки доступу	Висока	Помірні	Середній
Відмова обладнання	Середня	Значні	Середній
Внутрішнє копіювання даних	Низька	Критичні	Середній

Результати оцінки свідчать про необхідність впровадження системи

багаторівневого контролю.

Вимоги до системи на основі моделі загроз

На основі сформованої моделі загроз система контролю доступу повинна:

- забезпечувати персоніфіковану ідентифікацію;
- підтримувати гнучке розмежування прав;
- забезпечувати журналювання всіх подій;
- інтегруватися із системою відеоспостереження;
- мати механізми блокування доступу в режимі реального часу;
- підтримувати резервування критичних компонентів.

У результаті побудови моделі загроз та моделі порушника:

- визначено основні джерела небезпеки;
- класифіковано типи порушників;
- проведено оцінку ризиків;
- сформовано вимоги до архітектури системи контролю доступу.

Отримані результати є підґрунтям для переходу до проєктування системи фізичного захисту та контролю периметру.

2.3 Розробка системи фізичного захисту внутрішніх приміщень та контролю периметру

Проєктування системи фізичного захисту є ключовим етапом створення комплексної системи контролю доступу. Основною метою даного підрозділу є розробка багаторівневої системи захисту, що забезпечить ефективне розмежування доступу до приміщень готельного комплексу Optima Collection Khmelnytskyi, а також контроль периметру та критичних зон.

Система фізичного захисту будується за принципом багаторівневої оборони, що передбачає послідовне проходження кількох рубежів контролю.

Передбачається реалізація таких рівнів захисту: Периметровий контроль; контроль входу до будівлі; контроль доступу до службових приміщень; контроль

доступу до критичних технічних зон; централізований моніторинг та фіксація подій.

Такий підхід дозволяє локалізувати інцидент на ранньому етапі та мінімізувати наслідки.

Організація ефективного периметрового контролю готельного комплексу передбачає впровадження комплексу технічних заходів, спрямованих на раннє виявлення та запобігання спробам несанкціонованого проникнення. Основу цієї підсистеми складає розгалужена мережа IP-камер відеоспостереження, встановлених по всьому периметру будівлі, що забезпечує безперервний візуальний моніторинг прилеглої території та паркувальної зони. Особлива увага приділяється суворому контролю службових входів, де поряд із засобами відеофіксації застосовуються датчики відкриття дверей для миттєвого сповіщення про порушення цілісності контуру. Для забезпечення високої якості роботи оптичних засобів у будь-яку пору доби передбачається належне освітлення всієї території, що в сукупності з іншими елементами створює надійний перший рівень фізичного захисту об'єкта.

Для ефективного моніторингу периметру готельного комплексу доцільно використовувати сучасні IP-камери, технічні характеристики яких забезпечують високу якість зображення та надійність спостереження за будь-яких умов. Зокрема, пристрої повинні мати роздільну здатність не менше 4 Мп, що дозволяє досягти необхідної деталізації кадрів для ідентифікації осіб чи об'єктів. Обов'язковим є наявність інфрачервоного підсвічування та підтримка повноцінного нічного режиму, що гарантує стабільну роботу системи у темну пору доби або при недостатньому освітленні.

Функціональні можливості камер мають включати підтримку віддаленого перегляду, що дозволяє службі безпеки здійснювати оперативний візуальний контроль із будь-якої точки мережі. Весь генерований відеопотік спрямовується для зберігання на централізований сервер. Згідно з вимогами до безпеки об'єкта, система забезпечує архівацію та збереження відеоданих протягом періоду не менше 30 діб, що створює необхідну базу для ретроспективного аналізу подій та

розслідування можливих інцидентів.

Використання RFID-карт стандарту MIFARE або NFC-міток є оптимальним технологічним рішенням для сучасного готельного комплексу [20, с. 112], оскільки ці засоби забезпечують максимально швидку та надійну ідентифікацію користувачів. Ключовою перевагою обраного підходу є гнучкість у програмуванні рівнів доступу, що дозволяє легко інтегрувати карти з централізованою системою бронювання готелю. Це значно підвищує рівень зручності для гостей, забезпечуючи їм безперешкодний прохід до заброньованих номерів та зон загального користування. Окрім сервісних переваг, технологія суттєво посилює безпеку об'єкта завдяки можливості миттєвого блокування втрачених або викрадених ідентифікаторів у режимі реального часу.

Для співробітників закладу передбачається впровадження персоніфікованих електронних карт, які мають обов’язкову прив’язку до індивідуального облікового запису в системі управління. Такий підхід дозволяє не лише розмежувати права доступу згідно з посадовими обов'язками, а й здійснювати чіткий контроль за діями персоналу, що є критично важливим для забезпечення внутрішньої безпеки готелю.

Проєктована система передбачає використання комплексу апаратних засобів, що забезпечують фізичне блокування та керування точками доступу. Основними виконавчими механізмами виступають електромагнітні та електромеханічні замки, вибір яких залежить від типу дверей та вимог до рівня безпеки конкретного приміщення. Керування цими механізмами здійснюється за допомогою зчитувачів RFID-карт, які забезпечують безконтактну ідентифікацію користувачів. Координацію роботи всієї периферії виконують контролери доступу, що приймають рішення про відкриття згідно з налаштованими правилами. Крім того, для дотримання норм пожежної безпеки та можливості швидкої евакуації в екстрених ситуаціях обов'язковим є встановлення кнопок аварійного виходу в кожній точці проходу.

Приміщення поділяються на рівні доступу:

Рівень 0 — загальний доступ (вестибюль, ресторан)

Рівень 1 — обмежений доступ (адміністративні кабінети)

Рівень 2 — службовий доступ (склади, архіви)

Рівень 3 — критична інфраструктура (серверна, електрощитова)

Кожному користувачу призначається індивідуальний профіль доступу.

Оскільки серверна кімната є найбільш критичним об’єктом у структурі готельного комплексу, для забезпечення її безпеки впроваджується посилений комплекс заходів захисту. Зокрема, доступ до приміщення реалізується через систему подвійної ідентифікації, яка поєднує використання безконтактної RFID-карти та обов’язкове введення персонального PIN-коду. Кожна спроба входу підлягає автоматичному журналюванню, що дозволяє відстежувати активність у режимі реального часу.

Для візуального контролю безпосередньо у серверній встановлюється окрема IP-камера, а фізичний стан входу контролюється за допомогою датчиків відкриття дверей. Окрім захисту від несанкціонованого доступу, передбачено встановлення системи моніторингу температури для запобігання перегріву критичного обладнання. З огляду на високу важливість об'єкта, право доступу до нього надається виключно обмеженому колу осіб зі складу технічного персоналу.

Кожна операція в системі контролю доступу супроводжується автоматичною фіксацією точного часу події та повною ідентифікацією користувача, що здійснює вхід. Важливою технічною особливістю є синхронізація цих даних із системою відеоспостереження, що забезпечує прив’язку кожної дії до відповідного відеофрагмента. Такий комплексний підхід створює умови для проведення детального аудиту безпеки та дозволяє ефективно розслідувати будь-які інциденти. Окрім того, наявність відеоверифікації дає змогу беззаперечно підтверджувати факт присутності конкретної особи у приміщенні в певний момент часу, що значно підвищує рівень відповідальності персоналу.

Логіка роботи системи. Алгоритм функціонування: Користувач прикладає картку до зчитувача; контролер перевіряє права доступу; у разі авторизації

активується замок; подія записується в журнал; відеосистема фіксує момент входу.

У ситуації, коли система ідентифікує відмову в доступі, спрацьовує автоматичний протокол безпеки, що передбачає негайне блокування входу до приміщення або ресурсу. Кожен такий інцидент автоматично класифікується та фіксується в системі як спроба несанкціонованого проникнення. Одночасно з цим адміністратор системи або відповідальний співробітник служби безпеки отримує миттєве сповіщення про подію, що дозволяє оперативно проаналізувати причини відмови та вжити необхідних заходів реагування.

Для забезпечення стабільної та безперервної роботи інфраструктури готелю впроваджується комплекс заходів технічної відмовостійкості. Зокрема, передбачається обов'язкове використання джерел безперебійного живлення, що дозволяє захистити систему від раптових перепадів або зникнення напруги в електромережі. Надійність збереження інформації гарантується завдяки регулярному резервному копіюванню баз даних, а висока доступність сервісів досягається шляхом апаратного дублювання серверів. Додатковим рівнем безпеки є використання локальної пам’яті безпосередньо в контролерах доступу, що дозволяє системі продовжувати автономну роботу та приймати рішення щодо допуску осіб навіть у разі тимчасової втрати зв'язку з центральним сервером.

Навіть при відсутності зв’язку з центральним сервером контролери повинні працювати автономно.

Успішна практична реалізація запропонованої системи контролю доступу дозволить суттєво мінімізувати ризики несанкціонованого проникнення до критичних зон готельного комплексу. Впровадження індивідуальних засобів ідентифікації забезпечить точний персоніфікований облік доступу до ресурсів, що, у свою чергу, сприятиме помітному підвищенню виконавчої дисципліни серед персоналу закладу. Крім того, автоматизація процесів моніторингу допоможе значно скоротити час реагування служби безпеки на потенційні інциденти. Завдяки створенню єдиного інформаційного контуру буде забезпечено повний централізований контроль усіх подій у режимі реального

часу, що зробить систему захисту прозорою та ефективною.

Розроблена система фізичного захисту внутрішніх приміщень та контролю периметру ґрунтується на принципі багаторівневої безпеки та інтеграції електронних засобів ідентифікації з системою відеоспостереження. Запропоноване рішення враховує специфіку функціонування готельного комплексу та забезпечує баланс між безпекою та комфортом гостей.

Висновок до розділу 2

У другому розділі бакалаврської роботи було здійснено комплексну розробку компонентів системи контролю доступу для готельного комплексу Optima Collection Khmelnytskyi з урахуванням результатів аналізу предметної області, моделі загроз та особливостей функціонування об’єкта.

На початковому етапі було проведено обґрунтування об’єктів захисту, у межах якого визначено фізичні, інформаційні та технічні активи готелю. Приміщення об’єкта класифіковано за рівнем доступу на зони загального, обмеженого, службового та критичного доступу. Такий підхід дозволив сформувати структуровану основу для подальшого проєктування системи безпеки.

У процесі створення моделі загроз було ідентифіковано зовнішні, внутрішні та технічні джерела небезпеки.

Проведено класифікацію потенційних порушників за рівнем повноважень, мотивацією та можливостями реалізації загроз.

На основі якісної оцінки ризиків встановлено найбільш критичні сценарії, що потребують першочергового врахування при розробці системи контролю доступу.

Особливу увагу приділено формуванню моделі внутрішнього порушника, оскільки саме цей тип загроз характеризується найбільшим потенціалом завдання шкоди через наявність легітимного доступу до ресурсів. Це зумовило необхідність реалізації принципу мінімально необхідних привілеїв та повного журналювання дій користувачів.

У межах підрозділу 2.3 було розроблено архітектуру системи фізичного

захисту, концепція якої базується на фундаментальному принципі багаторівневої оборони. Запропонована структура передбачає впровадження суцільного периметрового контролю із залученням сучасних засобів IP-відеоспостереження для моніторингу прилеглої території. Основний контур безпеки реалізується через електронну систему контролю доступу, що працює на базі безконтактних RFID/NFC-технологій та забезпечує чітке зонування внутрішніх приміщень відповідно до встановлених рівнів доступу.

Особливістю архітектури є глибока технічна інтеграція системи контролю доступу з підсистемою відеомоніторингу, що дозволяє верифікувати кожну подію в режимі реального часу. Для забезпечення прозорості та можливості проведення розслідувань впроваджено механізм централізованого журналювання всіх дій у системі. Крім того, для гарантування високої відмовостійкості та стабільності захисту в екстремальних ситуаціях передбачено обов'язкове апаратне резервування всіх критичних компонентів комплексу.

Визначено технічні рішення щодо встановлення електромагнітних та електромеханічних замків, контролерів доступу, зчитувачів ідентифікаційних карт та системи безперебійного живлення. Окремо розроблено підхід до захисту серверної кімнати як зони критичної інфраструктури із застосуванням подвійної автентифікації та посиленого моніторингу.

Запропонована система передбачає централізоване адміністрування, автоматизоване ведення журналів подій, можливість оперативного блокування облікових записів та формування аналітичних звітів. Такий підхід дозволяє підвищити керованість процесами безпеки та скоротити час реагування на інциденти.

Отже, у другому розділі було сформовано цілісну концепцію системи фізичного захисту готельного комплексу, яка враховує специфіку його діяльності, структуру приміщень та потенційні ризики. Розроблені рішення створюють основу для подальшого проєктування захищеної корпоративної мережевої інфраструктури та інтеграції всіх компонентів в єдину систему управління безпекою, що буде розглянуто у третьому розділі роботи.

3 ОЦІНКА ФУНКЦІОНАЛЬНИХ ХАРАКТЕРИСТИК СИСТЕМИ

3.1 Проєктування захищеної корпоративної мережевої системи готельного комплексу

Ефективність системи контролю доступу значною мірою залежить від надійності корпоративної мережевої інфраструктури, у межах якої здійснюється передача службових даних, журналювання подій, інтеграція із відеоспостереженням та централізоване адміністрування (рис. 3.1).

Рисунок 3.1 - Оцінка собівартості

Проєктування захищеної мережевої інфраструктури для готельного комплексу Optima Collection Khmelnytskyi базується на системному підході до інформаційної безпеки та операційної стабільності. Першочерговим завданням у межах цієї розробки є реалізація чіткого розмежування гостьового та службового сегментів трафіку, що дозволяє надійно ізолювати критичні бізнес-процеси від публічних мереж. Такий розподіл ресурсів у поєднанні з використанням передових методів захисту від зовнішніх кібератак виступає фундаментом для гарантування повної конфіденційності корпоративної інформації та персональних даних клієнтів.

Особлива увага при розробці архітектури приділяється показникам відмовостійкості системи для запобігання будь-яким перебоям у наданні послуг, а також забезпеченню високого потенціалу для масштабування при майбутньому розширенні сервісів готелю. Ключовим елементом інтегрованого підходу є безшовна синхронізація мережевих ресурсів із загальною системою контролю доступу. Це дозволяє сформувати єдиний, легко керований контур безпеки, який забезпечує централізований моніторинг та оперативне реагування на будь-які загрози в межах усього комплексу.

Мережева інфраструктура будується за ієрархічною моделлю та включає: Рівень доступу (Access Layer); Рівень розподілу (Distribution Layer); Ядро мережі (Core Layer).

Апаратний каркас мережі готельного комплексу формується на основі передового мережевого обладнання, що гарантує високу швидкість обробки даних та багаторівневий захист інформаційних ресурсів. Головним елементом вхідної групи є високопродуктивний маршрутизатор із підтримкою VPN-технологій, який працює в тісній інтеграції з міжмережевим екраном (Firewall) для забезпечення безпечного віддаленого з’єднання та ретельної фільтрації вхідного трафіку. Для організації внутрішньої топології застосовуються керовані комутатори, що завдяки підтримці технології VLAN дозволяють ефективно розділити мережу на логічно ізольовані сегменти. Це забезпечує стабільне та захищене функціонування серверів системи контролю доступу, відеоспостереження та файлових сховищ, виключаючи ризик несанкціонованого втручання з боку гостьових підмереж.

Цілісність та постійна доступність корпоративних даних підтримується за допомогою виділеної системи резервного копіювання, яка виступає гарантом швидкого відновлення працездатності інфраструктури у разі технічних збоїв. Крім того, мережева архітектура включає розгалужену систему сучасних точок доступу Wi-Fi, що забезпечують стабільне бездротове покриття на всій території об'єкта. Таке поєднання апаратних засобів дозволяє створити цілісне, відмовостійке середовище, що повністю відповідає вимогам масштабованості та

сучасним стандартам безпеки.

Одним із ключових елементів захисту є сегментація мережі шляхом створення окремих віртуальних локальних мереж (VLAN) [14].

Передбачається створення таких сегментів:

VLAN 10 — Адміністрація (бухгалтерія, керівництво)

VLAN 20 — Службовий персонал

VLAN 30 — Серверна інфраструктура

VLAN 40 — Система відеоспостереження

VLAN 50 — СКУД

VLAN 60 — Гостьова Wi-Fi мережа

Гостьова мережа ізолюється від внутрішніх ресурсів та має доступ лише до мережі Інтернет.

Функціональне призначення міжмережевого екрана в архітектурі мережі полягає у забезпеченні комплексного моніторингу та фільтрації трафіку для запобігання різнорівневим цифровим загрозам. Завдяки реалізації алгоритмів блокування несанкціонованих з’єднань, пристрій створює надійний бар'єр, що унеможливлює встановлення нелегітимних сесій із внутрішніми ресурсами готелю. Окрім захисту вхідного каналу, брандмауер здійснює ретельний контроль вихідного трафіку, що дозволяє запобігти витоку конфіденційної інформації та виявити активність прихованого шкідливого програмного забезпечення.

Особливу роль у забезпеченні цілісності мережевого середовища відіграють вбудовані підсистеми виявлення та запобігання вторгненням (IDS/IPS), які в режимі реального часу аналізують мережеву активність на предмет аномалій. У поєднанні зі спеціалізованими модулями захисту від DDoS-атак, ці інструменти гарантують високу доступність сервісів та стабільність інфраструктури навіть в умовах інтенсивних кібернападів

Налаштовуються правила доступу між VLAN, що дозволяє обмежити обмін трафіком лише необхідними сервісами.

Серверна інфраструктура готельного комплексу виділена в окремий

логічний сегмент мережі — VLAN 30, що дозволяє ізолювати критичні ресурси та забезпечити жорсткий контроль трафіку на рівні комутації. Доступ до обладнання в цьому сегменті суворо обмежений і надається виключно системним адміністраторам, що мінімізує коло осіб, здатних впливати на роботу ядра мережі. Вся технічна взаємодія із серверами реалізується виключно через захищені протоколи передачі даних, зокрема SSH для адміністрування та HTTPS для керування веб-інтерфейсами додатків, що гарантує цілісність та конфіденційність команд управління.

Безпека адміністрування додатково посилюється шляхом обов’язкового впровадження багатофакторної автентифікації, яка виключає можливість несанкціонованого входу навіть у разі компрометації основного пароля. При цьому в основу управління правами покладено концепцію мінімально необхідних привілеїв. Згідно з цією моделлю, кожному користувачу або системному процесу надається лише той обсяг прав, який є технологічно необхідним для виконання його функцій, що дозволяє ефективно локалізувати потенційні загрози та значно підвищити загальний рівень стійкості інформаційної системи закладу.

Гостьова мережа готельного комплексу визначається як один із найбільш вразливих сегментів інфраструктури, що зумовлює необхідність впровадження посилених механізмів захисту. Для гарантування безпеки корпоративного контуру передбачається повна логічна ізоляція гостьового сегмента від внутрішніх VLAN, що унеможливлює несанкціонований доступ до службових ресурсів та конфіденційних даних. Стабільність роботи всієї системи забезпечується шляхом обмеження швидкості трафіку для відвідувачів, а високий рівень шифрування бездротового з’єднання досягається завдяки використанню сучасних стандартів WPA3 або WPA2-Enterprise. Додатковим рівнем контролю виступає обов'язкова авторизація користувачів через спеціалізований веб-портал, що у поєднанні з безперервним журналюванням підключень дозволяє ідентифікувати суб'єктів мережевої активності. Такий комплексний підхід дозволяє ефективно мінімізувати ризики використання

публічного Wi-Fi як вектора для проведення атак на внутрішню цифрову мережу закладу.

Функціонування системи контролю та управління доступом реалізовано в межах окремого логічного сегмента мережі VLAN 50, що забезпечує необхідний рівень ізоляції керуючого трафіку від інших підсистем готелю. Архітектурна модель СКУД включає центральний сервер, який виконує роль ядра системи, мережу інтелектуальних контролерів доступу, а також спеціалізовані робочі станції адміністратора для налаштування прав і моніторингу подій у реальному часі. Усі ідентифікаційні відомості та налаштування політик безпеки зберігаються в захищеній базі даних користувачів.

Процес обміну інформацією між усіма компонентами системи базується на використанні зашифрованих протоколів передачі даних, що гарантує цілісність команд управління та захист від перехоплення. Крім того, технічна реалізація передбачає обов’язкове передавання відомостей про кожну спробу доступу до централізованого електронного журналу. Такий підхід забезпечує формування прозорої звітності та створює надійну базу для проведення аудиту безпеки або детального розслідування інцидентів.

Забезпечення стабільного та безперервного функціонування інформаційної інфраструктури готелю ґрунтується на впровадженні комплексної стратегії відмовостійкості. Вона передбачає обов’язкове підключення резервного каналу Інтернет-зв’язку для нівелювання ризиків збоїв на стороні провайдера та апаратне дублювання критично важливих серверів. На рівні збереження даних застосовуються RAID-масиви, що гарантують апаратну відмовостійкість накопичувачів, а регулярне резервне копіювання забезпечує можливість повного відновлення систем у разі логічних помилок. Енергетична незалежність вузлів підтримується джерелами безперебійного живлення (UPS), які захищають обладнання від перепадів напруги. У ситуації критичної аварії основного серверного обладнання архітектурою передбачено автоматичний перехід системи в режим обмеженої автономної роботи, що дозволяє підтримувати базові функції безпеки об'єкта до повного відновлення основних потужностей.

Впровадження мережевої архітектури готельного комплексу базується на сучасній концепції Zero Trust [6, с. 120], фундаментальним принципом якої є повна відсутність довіри до будь-якого суб'єкта чи пристрою за замовчуванням, незалежно від його розташування відносно периметра мережі. У межах цієї моделі реалізується механізм постійної перевірки автентичності та безперервного контролю кожного окремого запиту на доступ до ресурсів. Це гарантує, що жодна сесія не вважається легітимною без динамічного підтвердження прав користувача.

Для забезпечення прозорості та підзвітності в системі здійснюється тотальне журналювання всіх дій користувачів, що дозволяє відстежувати активність у режимі реального часу та проводити ретроспективний аналіз. Важливим елементом захисту є суворе обмеження прав доступу відповідно до визначеної ролі співробітника, що мінімізує обсяг доступних даних до рівня, необхідного для виконання посадових обов'язків. Такий комплексний підхід дозволяє суттєво зменшити ризики, пов’язані з внутрішніми загрозами, та запобігти горизонтальному переміщенню зловмисників усередині мережевої інфраструктури.

Запропонована мережева структура забезпечує ефективне розмежування трафіку, що дозволяє ізолювати критичні сегменти мережі та гарантувати надійний захист внутрішніх ресурсів готелю. Завдяки впровадженню багаторівневих механізмів фільтрації та моніторингу досягається висока стійкість інфраструктури до зовнішніх атак, а інтегровані засоби журналювання створюють умови для централізованого контролю всіх мережевих подій у режимі реального часу. Ключовою перевагою такої конфігурації є повна інтеграція засобів фізичної та інформаційної безпеки, що формує єдиний захищений контур управління об'єктом. Розроблена архітектура корпоративної мережі створює надійну технічну основу для безперебійного функціонування системи контролю доступу та забезпечує всебічний захист інформаційних активів готельного комплексу.

3.2 Інтеграція спроєктованих компонентів в єдину систему

Ефективність системи контролю доступу визначається не лише якістю окремих технічних рішень, а й рівнем їх інтеграції в єдине інформаційно-кероване середовище. Розрізнене функціонування систем безпеки значно знижує можливості оперативного реагування на інциденти, тому сучасні підходи передбачають створення централізованої інтегрованої системи управління.

У межах даної роботи інтеграція виконується для готельного комплексу Optima Collection Khmelnytskyi, де об’єднуються фізичні та інформаційні компоненти безпеки в єдину архітектуру.

Інтегрована система безпеки готельного комплексу є складним багатофункціональним комплексом, що поєднує в собі декілька ключових підсистем для забезпечення всебічного захисту об'єкта. Технічний фундамент системи складають підсистема контролю та управління доступом (СКУД) і система відеоспостереження, які працюють у тісній взаємодії на базі єдиної корпоративної мережевої інфраструктури. Надійність обробки та зберігання інформації забезпечується потужною серверною підсистемою та структурованою базою даних користувачів, що дозволяє централізовано керувати правами доступу та персоналізацією сервісів. Для оперативного управління всім комплексом передбачена підсистема адміністрування та моніторингу, яка дозволяє технічному персоналу контролювати стан безпеки в режимі реального часу.

Центральним елементом архітектури виступає сервер управління безпекою, який виконує роль інтелектуального ядра системи. Він забезпечує ефективну координацію роботи всіх перелічених компонентів, синхронізуючи потоки даних між відеокамерами, контролерами доступу та мережевим обладнанням. Завдяки такій централізації вдається досягти високого рівня автоматизації процесів безпеки та мінімізувати вплив людського фактора на прийняття критичних рішень.

Архітектура взаємодії компонентів. Взаємодія реалізується за клієнт-

серверною моделлю.

Основні зв’язки:

- Зчитувач доступу → контролер СКУД
- Контролер → сервер системи доступу
- Сервер → база даних
- Сервер → система відеоспостереження
- Сервер → робоче місце адміністратора

Усі передані дані шифруються з використанням захищених мережевих протоколів.

Інтеграція СКУД із відеоспостереженням

Одним із ключових елементів інтеграції є синхронізація подій доступу з відеофіксацією.

Алгоритм роботи: Користувач проходить ідентифікацію; система перевіряє права доступу; подія передається на сервер; сервер надсилає сигнал системі відеоспостереження; камера позначає фрагмент відео відповідною подією.

Це дозволяє:

- підтвердити особу користувача;
- швидко знаходити записи інцидентів;
- виконувати аудит доступу.

Для забезпечення цілісності та прозорості моніторингу безпеки всі задіяні підсистеми автоматично формують записи у єдиному журналі подій. Це включає детальну фіксацію кожної спроби входу, випадків відмови у доступі, фактів відкриття дверей, а також усіх мережевих підключень та маніпуляцій, що здійснюються адміністратором системи. Такий комплексний підхід до збору даних дозволяє отримати вичерпну картину стану безпеки об'єкта в будь-який момент часу.

Електронний журнал зберігається на виділеному сервері безпеки та характеризується суворими технічними вимогами. Зокрема, у системі реалізована точна часова синхронізація між усіма джерелами подій, що є критично важливим для коректного відтворення хронології інцидентів. Захист

від несанкціонованого редагування або видалення записів гарантує достовірність доказової бази, а вбудована можливість експорту звітів дозволяє оперативно готувати аналітичну документацію для керівництва. Зрештою, впровадження централізованого логування значно спрощує аналіз потенційних загроз та підвищує ефективність розслідування безпекових інцидентів у готельному комплексі.

Функціональне призначення сервера в структурі системи полягає у виконанні ролі центрального вузла обробки даних та управління всіма компонентами безпеки. До основних завдань сервера належить оперативна обробка запитів від периферійних контролерів, ведення та зберігання бази даних користувачів, а також динамічне управління політиками доступу згідно з визначеними ролями. Крім того, програмно-апаратний комплекс забезпечує автоматичну генерацію аналітичних звітів та виконання регулярного резервного копіювання для гарантування цілісності інформації.

Для суттєвого підвищення загальної надійності інфраструктури передбачено впровадження технології віртуалізації серверів. Таке архітектурне рішення дозволяє абстрагувати програмне середовище від фізичного обладнання, що забезпечує високу гнучкість в управлінні ресурсами та можливість максимально швидкого відновлення працездатності системи у разі виникнення технічних збоїв. Використання віртуальних машин у поєднанні з централізованим керуванням створює відмовостійке середовище, здатне підтримувати безперервне функціонування критично важливих сервісів готелю.

СКУД функціонує як окремий сегмент мережі, але взаємодіє з:

- сервером авторизації;
- системою адміністрування;
- системою резервного копіювання.

Доступ між сегментами контролюється міжмережевим екраном відповідно до політик безпеки.

Для ефективної експлуатації системи адміністратор отримує єдиний централізований інтерфейс управління, який дозволяє здійснювати повний цикл

адміністрування безпеки в межах одного програмного вікна. Функціональні можливості інтерфейсу охоплюють створення та редагування облікових записів користувачів, гнучке призначення індивідуальних прав доступу та оперативне блокування втрачених чи неактуальних карт ідентифікації. Окрім налаштувань, система забезпечує безперервний перегляд подій у режимі реального часу, що дає змогу миттєво реагувати на нештатні ситуації, а вбудовані інструменти формування звітів автоматизують підготовку аналітичної документації про роботу СКУД.

Важливою архітектурною особливістю робочого місця адміністратора є реалізація механізму розмежування прав для різних рівнів доступу до самої системи управління. Це означає, що кожен фахівець технічної служби отримує доступ лише до тих функцій інтерфейсу, які відповідають його посадовим обов'язкам та рівню кваліфікації. Такий підхід запобігає випадковим або навмисним помилкам у конфігурації системи та гарантує, що критичні налаштування залишаться доступними лише для обмеженого кола старших адміністраторів.

Інтегрована система підтримує автоматичні сценарії реагування:

- багаторазова відмова доступу → повідомлення адміністратору;
- доступ у неробочий час → сигнал тривоги;
- відкриття серверної → автоматичне збереження відеофрагмента;
- втрачена картка → миттєве блокування.

Впровадження запропонованого підходу дозволяє забезпечити комплексне централізоване управління всіма контурами безпеки готельного комплексу, що значно скорочує час реагування на позаштатні ситуації. Завдяки автоматизації ключових процесів суттєво підвищується рівень контролю за діями персоналу та зводиться до мінімуму негативний вплив людського фактора на прийняття критичних рішень. Важливою перевагою обраної моделі є повна простежуваність кожної події в системі, що гарантує наявність достовірної бази для аудиту та аналізу.

Інтеграція всіх спроєктованих компонентів дозволила сформувати цілісну

систему безпеки, у якій фізичний та інформаційний захист функціонують як єдиний узгоджений механізм. Таке архітектурне поєднання створює надійну технічну основу для ефективної експлуатації системи контролю доступу та виступає базою для подальшого проєктування інформаційної бази даних, що відповідає сучасним стандартам готельної галузі.

3.3 Проєктування бази даних системи контролю доступу

Рисунок 3.2 - БД

Ефективне функціонування системи контролю доступу неможливе без надійної структури зберігання даних. База даних є центральним елементом інформаційної підсистеми безпеки готельного комплексу Optima Collection Khmelnytskyi, оскільки саме вона забезпечує збереження відомостей про користувачів, права доступу, події та конфігурацію обладнання.

Проєктування бази даних для системи контролю доступу здійснювалося з дотриманням комплексу вимог, спрямованих на забезпечення стабільності та безпеки інформаційного середовища. Першочергову увагу було приділено гарантуванню цілісності даних та підтримці повноцінного багатокористувацького режиму, що дозволяє системі коректно обробляти запити

від декількох адміністраторів одночасно. Окрім цього, архітектура сховища оптимізована для забезпечення швидкого доступу до журналів подій, що є критично важливим для моніторингу в реальному часі, а закладений потенціал масштабованості дозволяє розширювати систему без втрати продуктивності.

Для надійного функціонування бази даних впроваджено багаторівневий захист від несанкціонованого доступу та повну підтримку механізмів регулярного резервного копіювання. У контексті технічної реалізації системи найбільш доцільним є використання саме реляційної моделі даних [33, с. 85]. Такий вибір обґрунтований її здатністю забезпечувати чітку структурованість інформації та ефективно реалізовувати складні логічні зв’язки між об’єктами, що є необхідною умовою для координації роботи користувачів, прав доступу та ідентифікаторів у межах єдиного цифрового простору.

У результаті аналізу функціональних вимог виділено такі основні сутності: Користувачі (Users); Ролі (Roles); Рівні доступу (AccessLevels); Приміщення (Rooms); Пристрої доступу (Devices); Картки доступу (AccessCards); Події доступу (AccessEvents); Адміністратори системи (Admins).

Структура основних таблиць

1. Таблиця Users

Містить інформацію про осіб, які мають доступ до системи.

Основні поля:

- UserID (Primary Key)
- LastName
- FirstName
- Position
- PhoneNumber
- Email
- RoleID (Foreign Key)
- Status (Active/Blocked)

2. Таблиця Roles

Визначає ролі користувачів.

Поля:

- RoleID (Primary Key)
- RoleName
- Description

Приклад ролей:

- Адміністратор
- Бухгалтер
- Менеджер
- Технічний персонал
- Охорона

3. Таблиця Rooms

Містить перелік приміщень.

Поля:

- RoomID (Primary Key)
- RoomName
- AccessLevelID (Foreign Key)
- Location
- CriticalFlag (Boolean)

4. Таблиця AccessLevels

Визначає рівні доступу.

Поля:

- AccessLevelID (Primary Key)
- LevelName
- Description

5. Таблиця AccessCards

Містить інформацію про RFID/NFC-картки.

Поля:

- CardID (Primary Key)
- CardUID
- UserID (Foreign Key)

- IssueDate
- ExpirationDate
- CardStatus

6. Таблиця Devices

Містить інформацію про зчитувачі та контролери.

Поля:

- DeviceID (Primary Key)
- DeviceType
- Location
- IPAddress
- RoomID (Foreign Key)

7. Таблиця AccessEvents

Журнал подій доступу.

Поля:

- EventID (Primary Key)
- UserID (Foreign Key)
- DeviceID (Foreign Key)
- EventDateTime
- AccessResult (Granted/Denied)
- Reason

Ця таблиця є найбільш об’ємною та потребує індексації для швидкого пошуку.

Логічна модель зв’язків. Основні зв’язки:

- Один користувач → одна роль (1:N)
- Одна роль → багато користувачів
- Один користувач → одна або декілька карт
- Один пристрій → одне приміщення
- Один користувач → багато подій доступу

Реалізовано зовнішні ключі для забезпечення цілісності даних.

З метою підвищення надійності та відмовостійкості бази даних на етапі

проєктування було впроваджено низку технічних інструментів контролю цілісності. Зокрема, на рівні схеми даних активно використовуються обмеження NOT NULL, що запобігає появі неповних або некоректних записів у критично важливих полях. Зв’язність та логічна єдність інформаційної структури забезпечується через застосування зовнішніх ключів (FOREIGN KEY), які гарантують каскадну цілісність посилань між таблицями. Окрему увагу приділено продуктивності системи: для прискорення вибірки даних та оптимізації пошукових запитів реалізовано індексацію таблиці AccessEvents, що акумулює відомості про події доступу.

Безпека даних на рівні сховища підтримується шляхом суворого розмежування прав доступу до об’єктів бази даних, що виключає можливість несанкціонованих маніпуляцій. Уся взаємодія між прикладним програмним забезпеченням та сервером бази даних здійснюється через захищене шифроване з’єднання, що запобігає перехопленню інформації в мережі. Крім того, стратегія захисту передбачає регулярне виконання процедур резервного копіювання, що створює необхідні умови для швидкого відновлення бази даних у разі виникнення апаратних збоїв або логічних помилок.

Враховуючи потенційно великий обсяг даних у журналі подій, архітектура бази даних передбачає використання спеціалізованих методів оптимізації для підтримки високої швидкості роботи системи. Одним із ключових рішень є впровадження механізму партиціювання таблиці AccessEvents, що дозволяє розділити великий масив даних на менші, логічно відокремлені сегменти за часовими інтервалами. Це значно прискорює процес вибірки інформації та спрощує подальшу архівацію застарілих записів, які виходять за межі встановленого періоду зберігання.

Для забезпечення оперативності роботи інтерфейсу адміністратора реалізовано стратегію індексації за найбільш часто використовуваними критеріями пошуку, зокрема по полях EventDateTime та UserID. Такий підхід у поєднанні з цілеспрямованою оптимізацією SQL-запитів дозволяє мінімізувати навантаження на апаратні ресурси сервера навіть при опрацюванні значної

кількості звернень до журналу. У сукупності ці заходи гарантують стабільну продуктивність системи моніторингу та швидке формування аналітичних звітів без затримок для кінцевого користувача.

Проєктована структура бази даних характеризується високим ступенем гнучкості, що дозволяє безперешкодно додавати нові приміщення до загальної схеми об'єкта та підключати додаткові периферійні пристрої без необхідності докорінної зміни архітектури. Окрім апаратного розширення, система передбачає можливість легкої адаптації під нові бізнес-вимоги, зокрема через розширення ролей користувачів та можливість глибокої інтеграції з іншими корпоративними сервісами, такими як HR-відділ або бухгалтерські модулі. Такий функціональний потенціал робить систему універсальним інструментом управління в межах готельного комплексу.

Розроблена база даних забезпечує впорядковане та структуроване зберігання всієї необхідної інформації, підтримуючи при цьому багаторівневу систему доступу до даних та повне журналювання всіх значущих подій. Завдяки закладеним принципам масштабування та впровадженим механізмам захисту цілісності, база даних виступає надійною інформаційною основою інтегрованої системи контролю доступу. Вона не лише гарантує стабільне функціонування всіх компонентів захисту, а й створює передумови для подальшого технологічного розвитку цифрової інфраструктури закладу.

3.4 Оцінка собівартості системи контролю доступу

Економічне обґрунтування є важливим етапом проєктування системи контролю доступу, оскільки дозволяє оцінити доцільність впровадження запропонованих технічних рішень у готельному комплексі Optima Collection Khmelnytskyi.

Метою даного підрозділу є визначення орієнтовної вартості обладнання, монтажних робіт та супутніх витрат, пов’язаних із впровадженням системи.

Загальні витрати на впровадження системи складаються з: Витрат на обладнання; витрат на програмне забезпечення; монтажних та пусконалагоджувальних робіт; витрат на налаштування мережевої інфраструктури; резервних витрат (непередбачені витрати).

Розрахунок вартості обладнання розподілено за категоріями (табл. 3.1 – 3.3)

Таблиця 3.1 - Система контролю доступу

Найменування	Кількість	Орієнтовна ціна за одиницю (грн)	Загальна вартість (грн)
Контролер доступу	6	6 000	36 000
RFID-зчитувач	12	2 500	30 000
Електромагнітний замок	10	2 000	20 000
RFID-картки (100 шт.)	100	80	8 000
Кнопки аварійного виходу	10	500	5 000

Разом по СКУД: 99 000 грн

Таблиця 3.2 - Система відеоспостереження

Найменування	Кількість	Ціна (грн)	Загальна вартість (грн)
IP-камера 4 Мп	16	3 000	48 000
Відеореєстратор (NVR)	1	15 000	15 000
Жорсткі диски (архів)	2	5 000	10 000

Разом: 73 000 грн

Таблиця 3.3 - Серверна та мережева інфраструктура

Найменування	Кількість	Ціна (грн)	Загальна вартість (грн)
Сервер (СКУД + БД)	1	45 000	45 000
Керований комутатор	2	12 000	24 000
Маршрутизатор з Firewall	1	18 000	18 000
UPS	2	8 000	16 000

Разом: 103 000 грн

Процес практичної реалізації проєкту розподіляється на декілька етапів, що охоплюють як загальнобудівельні роботи, так і тонке налаштування інтелектуальних компонентів системи. На початковій стадії здійснюється прокладання кабельних трас, що формують фізичну основу для обміну даними та живлення периферійних пристроїв. Паралельно з цим проводиться монтаж виконавчих механізмів та пристроїв ідентифікації, зокрема встановлення електромагнітних або електромеханічних замків і зчитувачів на точках проходу. Роботи з розгортання візуального контуру безпеки включають професійне встановлення та позиціонування камер відеоспостереження для забезпечення максимального охоплення території без «сліпих зон».

Після завершення монтажу польового обладнання основна увага приділяється програмно-апаратній підготовці центру управління. Цей етап передбачає інсталяцію та налаштування серверів, а також прецизійну конфігурацію параметрів VLAN для забезпечення логічної ізоляції мережевих сегментів згідно з розробленою архітектурою. Фінальним етапом є комплексне тестування системи, що включає перевірку працездатності кожного компонента, верифікацію сценаріїв доступу та контроль коректності передачі даних у журнал подій. Такий системний підхід до монтажу гарантує повну відповідність розгорнутої інфраструктури вимогам надійності та безпеки готельного комплексу.

Орієнтовна вартість монтажних робіт становить 25–30% від вартості обладнання.

Загальна вартість обладнання: 99 000 + 73 000 + 103 000 = 275 000 грн

Монтаж (30%): ≈ 82 500 грн.

Зведені показники собівартості наведено у таблиці 3.4.

Таблиця 3.4 - Загальна собівартість системи

Стаття витрат	Сума (грн)
Обладнання	275 000
Монтаж та налаштування	82 500
Резерв (5%)	13 750

Загальна орієнтовна вартість впровадження: 371 250 грн

Успішне впровадження спроєктованої системи безпеки в готельному комплексі дозволяє досягти вагомих результатів як у технічній, так і в економічній площинах. Завдяки автоматизації контролю доступу та відеомоніторингу вдається ефективно запобігти фінансовим втратам, пов'язаним із крадіжками або несанкціонованим використанням майна закладу. Окрім прямого захисту матеріальних активів, інтеграція сучасних мережевих протоколів значно зменшує ризик витоку персональних даних гостей та персоналу, що є критично важливим для збереження репутації готелю.

Оптимізація процесів моніторингу та управління доступом дозволяє скоротити витрати на утримання великого штату фізичної охорони без втрати якості захисту об'єкта. Такий підхід не лише підвищує рівень довіри клієнтів, які цінують високий стандарт безпеки та конфіденційності, а й забезпечує повну відповідність закладу сучасним вимогам інформаційної безпеки та галузевим стандартам. У підсумку, система стає надійним інструментом підтримки стабільної та безпечної роботи готельного комплексу в довгостроковій перспективі.

Навіть один серйозний інцидент (наприклад, витік бази даних або проникнення до серверної) може спричинити втрати, що перевищують вартість впровадження системи.

За умови зменшення витрат на охорону та запобігання інцидентам, орієнтовний термін окупності системи становить 2–3 роки.

Проведений економічний розрахунок показав, що впровадження системи

контролю доступу є фінансово обґрунтованим рішенням. Незважаючи на початкові капіталовкладення, система забезпечує довгострокову економію та суттєве зниження ризиків.

3.5 Розробка рекомендацій для реалізації системи

Ефективність впровадження системи контролю доступу визначається не лише якістю технічного проєктування, а й правильністю організаційної реалізації, дотриманням регламентів та підготовкою персоналу. Для готельного комплексу Optima Collection Khmelnytskyi реалізація системи повинна здійснюватися поетапно з урахуванням безперервності функціонування закладу.

Процес реалізації доцільно поділити на декілька послідовних етапів.

Перший етап впровадження системи є підготовчим. У межах цієї стадії необхідно провести детальне технічне обстеження приміщень, уточнити схеми прокладання кабельних трас та погодити місця майбутнього встановлення обладнання. На основі отриманих даних формується остаточна специфікація технічних засобів і розробляється детальний план-графік робіт. Під час планування надзвичайно важливо передбачити заходи для мінімізації впливу монтажного процесу на комфорт гостей.

Наступним кроком є безпосередній монтаж обладнання. Цей процес охоплює встановлення зчитувачів, електронних замків, контролерів доступу та необхідного серверного обладнання. Разом із цим здійснюється налаштування мережевої інфраструктури та фізичне встановлення камер відеоспостереження. Для того щоб не створювати незручностей для відвідувачів, виконання всіх монтажних робіт доцільно проводити у неробочий або нічний час.

Завершальним етапом є програмне налаштування комплексу. На цій стадії виконується інсталяція спеціалізованого програмного забезпечення СКУД, після чого створюється структура користувачів із подальшим призначенням їм відповідних ролей та рівнів доступу. Також проводиться конфігурація системи

журналювання подій та здійснюється інтеграція контролю доступу з підсистемою відеоспостереження. Фінальним кроком є комплексне тестування всієї системи, яке дозволяє переконатися в коректності її функціонування перед здачею в експлуатацію.

Після завершення програмного налаштування розпочинається етап тестової експлуатації. У ході цієї стадії здійснюється комплексна перевірка коректності роботи зчитувачів та тестування різноманітних сценаріїв відмови обладнання. Особлива увага приділяється перевірці надійності резервного живлення, а також моделюванню можливих спроб несанкціонованого доступу до об'єктів. За результатами проведеного тестування проводиться ретельний аналіз роботи комплексу, що дозволяє оперативно виявити та усунути всі можливі недоліки чи вразливості системи.

Останнім кроком впровадження є введення комплексу в промислову експлуатацію. На цій стадії система остаточно переводиться у штатний режим роботи. Одночасно з цим відбувається повне оформлення відповідної технічної та супровідної документації, а також розробляються і офіційно затверджуються регламенти подальшої експлуатації та обслуговування обладнання.

Ефективне функціонування будь-яких технічних рішень неможливе без належного супроводу відповідними організаційними заходами. До ключових завдань у цьому напрямку належить розробка комплексної політики інформаційної безпеки та затвердження чітких правил користування електронними картками. Крім того, необхідно встановити суворий порядок своєчасного блокування втрачених ідентифікаторів, призначити конкретних посадових осіб, відповідальних за адміністрування комплексу, а також створити детальний регламент реагування на можливі інциденти. Слід враховувати, що без належної формалізації цих процедур навіть найсучасніша апаратно-програмна система може суттєво втратити свою ефективність та надійність.

Невід'ємним елементом успішного впровадження системи є проведення кваліфікованого навчання працівників. Цей процес повинен охоплювати базовий інструктаж щодо правильного використання карток доступу, а також

спеціалізоване та поглиблене навчання адміністраторів для роботи з відповідним програмним забезпеченням. Обов'язковою умовою є ознайомлення всього персоналу із загальними правилами безпеки та детальне роз'яснення міри відповідальності за будь-які порушення встановленої політики доступу. Систематичне підвищення рівня обізнаності працівників дозволяє суттєво мінімізувати ризики виникнення внутрішніх інцидентів та порушень режиму.

З метою підтримання стабільної та безперебійної роботи розгорнутої системи формується регламент її технічного обслуговування. Відповідно до нього вимагається регулярне проведення щоквартальної перевірки стану всього обладнання, своєчасне оновлення встановленого програмного забезпечення та систематичний аудит журналів подій. Поряд із цим, критично важливим є періодичне тестування механізмів створення резервних копій даних та ретельна перевірка справності джерел безперебійного живлення. Таке регулярне та комплексне обслуговування ефективно запобігає непередбачуваним відмовам обладнання і значно знижує загальні експлуатаційні ризики.

Обов'язковою умовою функціонування розгорнутої системи є забезпечення її повної відповідності чинному законодавству. Зокрема, це стосується суворих нормативних вимог щодо захисту персональних даних, дотримання правил обробки відеоінформації, забезпечення загальних стандартів інформаційної безпеки та належного зберігання електронних журналів. Зі свого боку, адміністрація готелю зобов'язана організувати своєчасне інформування клієнтів про ведення відеоспостереження на території закладу. Крім того, керівництво має гарантувати надійне обмеження доступу до конфіденційних персональних даних та чітко визначити регламентовані строки зберігання зібраної інформації.

З метою подальшого розвитку та підвищення загальної ефективності комплексу рекомендується реалізувати низку перспективних заходів. Доцільним кроком є впровадження технологій біометричної автентифікації для організації доступу до критично важливих зон, а також інтеграція контролю доступу з корпоративною HR-системою закладу. Значно розширити зручність користування дозволить використання сучасних мобільних додатків як

альтернативи традиційним перепусткам. Водночас для оптимізації процесів управління варто розгорнути інструменти аналітики на основі зібраних журналів подій та запровадити постійну практику проведення періодичного аудиту інформаційної безпеки.

Процес впровадження системи неминуче супроводжується певними ризиками, які необхідно завчасно враховувати. Серед найбільш імовірних загроз варто виділити тимчасове порушення звичного режиму роботи готелю, виникнення непередбачуваних помилок конфігурації, можливу апаратну несумісність обладнання, а також психологічний опір персоналу до запроваджуваних змін. Для ефективної мінімізації цих ризиків процес модернізації слід реалізовувати виключно поетапно, обов'язково здійснюючи ретельне попереднє тестування кожного нового компонента. Критично важливо також заздалегідь підготувати надійні резервні рішення на випадок позаштатних ситуацій та доручати виконання робіт тільки кваліфікованим фахівцям.

Розроблені рекомендації дозволяють забезпечити поетапну та контрольовану реалізацію системи контролю доступу з мінімальним впливом на поточну діяльність готельного комплексу. Комплексне поєднання технічних та організаційних заходів гарантує досягнення запланованого рівня безпеки та підвищує ефективність функціонування системи в довгостроковій перспективі.

Висновок до розділу 3

У третьому розділі бакалаврської роботи було здійснено комплексне проєктування та оцінку функціональних характеристик інтегрованої системи контролю доступу для готельного комплексу Optima Collection Khmelnytskyi.

На першому етапі було розроблено архітектуру захищеної корпоративної мережевої інфраструктури, що забезпечує розмежування трафіку, ізоляцію гостьового сегмента та захист критичних інформаційних ресурсів.

Запропонована модель мережі передбачає використання VLAN-сегментації, міжмережевого екрану, резервування каналів зв’язку та впровадження принципів Zero Trust. Такий підхід дозволяє мінімізувати ризики несанкціонованого доступу до внутрішніх ресурсів та забезпечити стабільне функціонування інформаційних сервісів готелю.

У межах підрозділу 3.2 було реалізовано інтеграцію всіх спроєктованих компонентів — системи контролю доступу, відеоспостереження, серверної інфраструктури та мережевих засобів — в єдину централізовану систему управління безпекою. Особливу увагу приділено синхронізації подій доступу з відеофіксацією, що підвищує рівень контролю та забезпечує можливість проведення детального аудиту у випадку інцидентів.

У підрозділі 3.3 розроблено структуру реляційної бази даних, яка забезпечує зберігання інформації про користувачів, ролі, приміщення, пристрої доступу та журнали подій.

Запропонована модель бази даних гарантує цілісність, масштабованість та можливість швидкого пошуку інформації. Реалізовані механізми індексації, розмежування прав доступу та резервного копіювання сприяють підвищенню надійності системи.

Проведена в підрозділі 3.4 економічна оцінка показала, що впровадження системи є фінансово доцільним. Незважаючи на початкові капіталовкладення, реалізація проєкту забезпечує довгострокове зниження ризиків, мінімізацію можливих збитків та підвищення рівня довіри клієнтів до готельного комплексу.

У підрозділі 3.5 розроблено практичні рекомендації щодо реалізації системи, які включають етапи впровадження, організаційні заходи, навчання персоналу та регламент технічного обслуговування. Встановлено, що лише поєднання технічних рішень із чітко визначеними управлінськими процедурами дозволяє досягти максимального рівня ефективності.

Таким чином, у третьому розділі було сформовано завершену концепцію функціонування інтегрованої системи контролю доступу, що поєднує фізичний та інформаційний захист у межах єдиної архітектури. Запропоновані рішення

відповідають сучасним вимогам безпеки, враховують специфіку діяльності готельного комплексу та забезпечують високий рівень захисту критичних ресурсів.

Отримані результати підтверджують доцільність впровадження розробленої системи та створюють підґрунтя для формування загальних висновків бакалаврської роботи.

ВИСНОВКИ

У кваліфікаційній роботі розроблено комплексну систему контролю доступу для готельного комплексу Optima Collection Khmelnytskyi, яка забезпечує інтегрований фізичний та інформаційний захист об’єкта з урахуванням специфіки його функціонування.

У першому розділі було здійснено дослідження предметної області, проведено первинний аналіз об’єкта та його інформаційної структури. Визначено основні фізичні та інформаційні активи, що підлягають захисту, класифіковано приміщення за рівнями доступу, проаналізовано інформаційні потоки та встановлено критичні ресурси. На основі проведеного аналізу сформульовано технічну задачу проєктування системи контролю доступу, визначено її функціональні та нефункціональні вимоги, а також критерії ефективності.

У другому розділі здійснено розробку основних компонентів системи контролю доступу. Проведено обґрунтування об’єктів захисту та сформовано модель загроз і модель потенційного порушника. Ідентифіковано зовнішні, внутрішні та технічні загрози, оцінено їх можливі наслідки та рівень ризику. На основі отриманих результатів розроблено систему фізичного захисту внутрішніх приміщень та контролю периметру з використанням електронних засобів ідентифікації, відеоспостереження та централізованого журналювання подій. Запропоновано багаторівневу архітектуру захисту, що реалізує принцип «глибокоешелонованої оборони».

У третьому розділі виконано проєктування захищеної корпоративної мережевої інфраструктури, що забезпечує сегментацію трафіку, ізоляцію гостьової мережі та захист серверних ресурсів. Реалізовано інтеграцію системи контролю доступу з відеоспостереженням та серверною підсистемою в єдину централізовану систему управління безпекою.

Розроблено структуру реляційної бази даних, яка забезпечує зберігання інформації про користувачів, права доступу, пристрої та журнали подій із дотриманням принципів цілісності та масштабованості.

Проведена економічна оцінка підтвердила доцільність впровадження запропонованої системи. Визначено орієнтовну вартість реалізації проєкту та обґрунтовано його окупність у середньостроковій перспективі. Розроблено практичні рекомендації щодо поетапного впровадження, організаційного супроводу та технічного обслуговування системи.

У результаті виконання роботи було успішно досягнуто поставленої мети - розроблено та спроєктовано комплексну систему контролю доступу, яка гарантує чітке розмежування прав доступу до фізичних приміщень готельного комплексу. Завдяки впровадженню сучасних протоколів та архітектурних рішень забезпечено високий рівень захисту інформаційних ресурсів та реалізовано механізм централізованого управління подіями безпеки. Спроєктована структура дозволила досягти безшовної інтеграції фізичного та мережевого захисту, що створює єдиний контур безпеки об'єкта.

Окрім технічних аспектів, реалізація проєкту сприяє суттєвому підвищенню рівня контролю за діями персоналу та забезпечує повну простежуваність операцій. Це дозволяє мінімізувати ризики несанкціонованого доступу та оперативно реагувати на потенційні загрози. Таким чином, розроблена система є завершеним технологічним рішенням, що відповідає сучасним стандартам безпеки, масштабованості та надійності, створюючи безпечне середовище для гостей та співробітників закладу.

Запропоновані технічні та організаційні рішення відповідають сучасним вимогам інформаційної безпеки та можуть бути адаптовані до інших готельних закладів аналогічного типу.

Отже, розроблена система контролю доступу є практично орієнтованим та технічно обґрунтованим рішенням, що сприяє підвищенню рівня безпеки готельного комплексу та забезпечує стабільність його функціонування в умовах зростання загроз фізичного та кібернетичного характеру.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР.

2. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI.

3. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.

4. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Практичні правила управління інформаційною безпекою.

5. ДСТУ EN 50133-1:2014. Системи контролю доступу для застосування в системах безпеки.

6. Stallings W. Network Security Essentials: Applications and Standards. – 6th ed. – Pearson Education, 2017. 624 p.

7. Tanenbaum A. S., Wetherall D. J. Computer Networks. – 5th ed. – Pearson, 2011. 960 p.

8. Whitman M., Mattord H. Principles of Information Security. – 6th ed. – Cengage Learning, 2017. 656 p.

9. Stallings W., Brown L. Computer Security: Principles and Practice. New York : Pearson, 2023. 820 p.

10. Grassi P., Garcia M., Fenton J. Digital Identity Guidelines. – NIST Special Publication 800-63-3. – National Institute of Standards and Technology, 2017.

11. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems. – NIST SP 800-94. – NIST, 2007.

12. Грайворонський М. В., Корченко О. Г. Технології мережевої безпеки. Київ : НАУ, 2023. 415 с.

13. Kim D., Solomon M. Fundamentals of Information Systems Security. – Jones & Bartlett Learning, 2016. 492 p.

14. Cisco Systems. VLAN Configuration Guide. – Cisco Documentation, 2022. – URL: https://www.cisco.com

15. Oppenheimer P. Top-Down Network Design. – 3rd ed. – Cisco Press, 2011. 624 p.

16. Bishop M. Computer Security: Art and Science. – Addison-Wesley, 2018. 1184 p.

17. Anderson R. Security Engineering. – 2nd ed. – Wiley, 2008. 1040 p.

18. Easttom C. Modern Cryptography: Applied Mathematics for Encryption and Information Security. Cham : Springer, 2022. 530 p.

19. Easttom C. Network Defense and Countermeasures. – Pearson IT Certification, 2013. 512 p.

20. Hernandez J. RFID Security. – McGraw-Hill, 2013. 320 p.

21. ISO/IEC 27005:2018. Information security risk management.

22 NIST SP 800-53 Rev.5. Security and Privacy Controls for Information Systems and Organizations. – NIST, 2020.

23. Cole E. Network Security Bible. – 2nd ed. – Wiley, 2011. 768 p.

24. Stewart J., Chapple M., Gibson D. CISSP Study Guide. – 8th ed. – Sybex, 2018. 1008 p.

25. Глущенко О. В. Інформаційна безпека підприємств: навчальний посібник. – Київ : КНУ, 2019. 312 с.

26. ДСТУ ISO/IEC 27033-1:2016. Інформаційні технології. Методи захисту. Безпека мереж. Частина 1. Огляд і концепції.

27. Корченко О. Г. Системи контролю доступу та відеоспостереження: інтегровані рішення. – Київ: НАУ, 2019. 240 с.

28. Lammle T. CCNA Routing and Switching Complete Study Guide. – 2nd ed. – Sybex, 2016. 1104 p.

29. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – Київ: Видавнича група BHV, 2018. 608 с.

30. Odom T. CCNA 200-301 Official Cert Guide. – Cisco Press, 2020. 832 p.

31. Майстренко В. В. Системи електронного контролю доступу: теорія і практика. – Одеса: ОНАС, 2021. 215 с.

32. NIST Special Publication 800-115. Technical Guide to Information Security

Testing and Assessment. – NIST, 2008.

33. Бойко А. А. Проектування локальних мереж: навчальний посібник. – Харків: ХНУРЕ, 2020. 185 с.

34. Остроухов В. В., Гайдур Г.І. Основи інформаційної безпеки. – Київ: ДУТ, 2018. 412 с.

35. Chapple M., Seidl D. CompTIA Security+ Study Guide. – 8th ed. – Sybex, 2021. 1056 p.

36. Frahim J., Santos O. Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services. – 3rd ed. – Cisco Press, 2014. 1072 p.

37. Богуш В. М., Юдін О. К. Інформаційна безпека держави. – Київ: МК-Прес, 2015. 432 с.

38. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. – 7th ed. – Pearson, 2017. 864 p.

39. Козловський В. В. Управління інформаційною безпекою в готельному та туристичному бізнесі. – Львів: ЛНУ, 2020. 180 с.

40. Engebretson D. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. – 2nd ed. – Syngress, 2013. 224 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= " ;
```

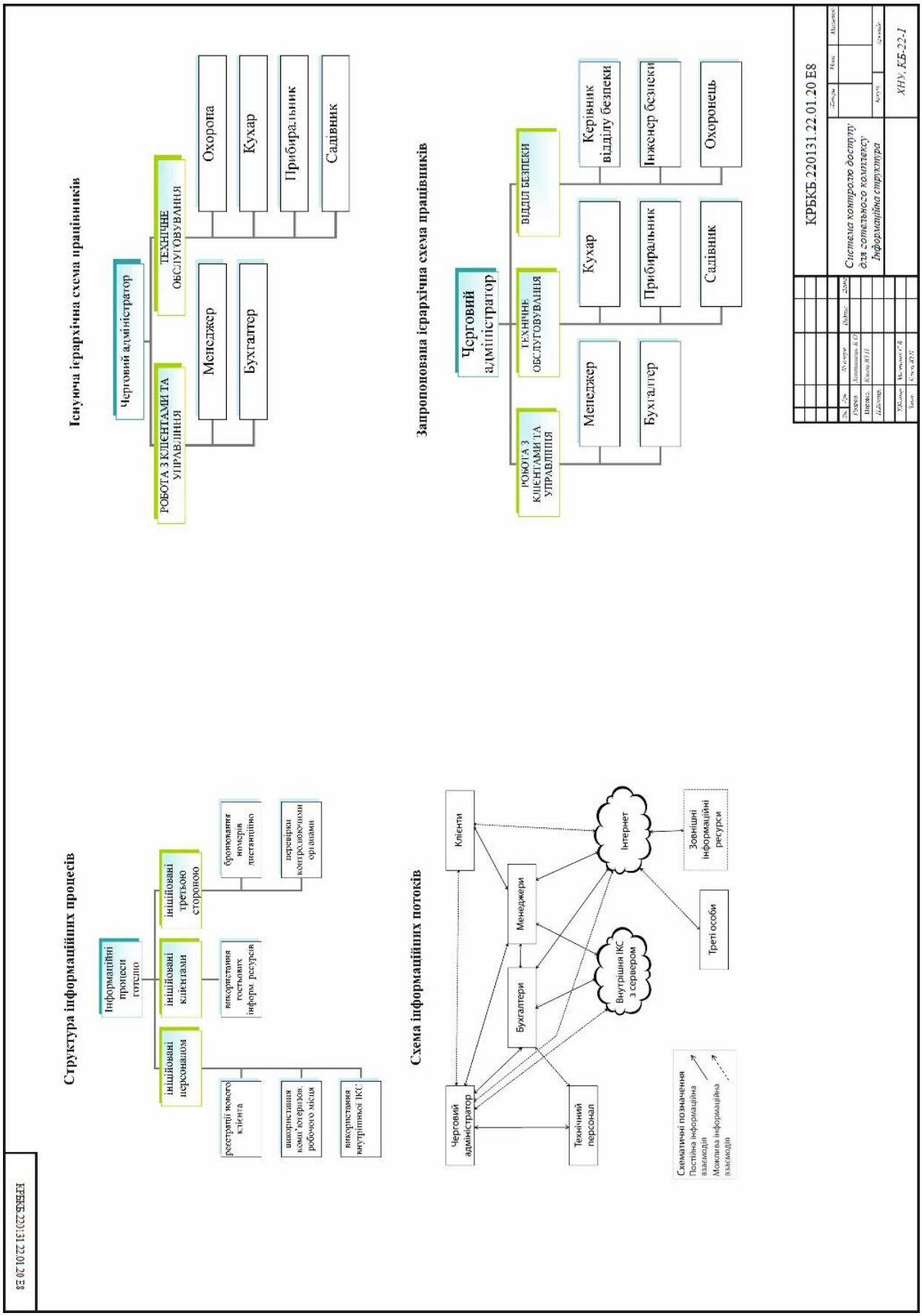
```
public Podrobutsi(int ID)
{
    this.UserID = ID;
    InitializeComponent();

}

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

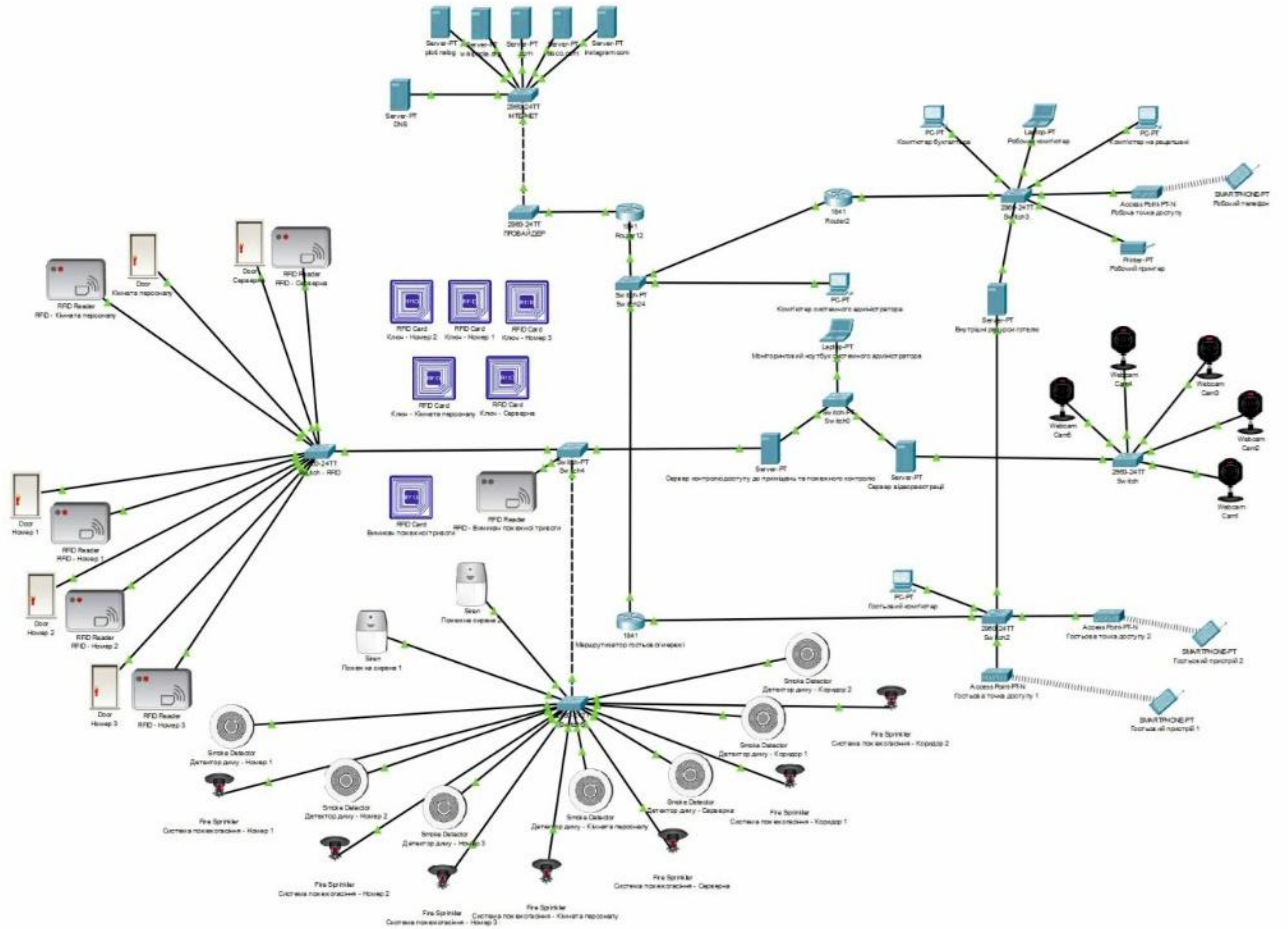
(обов’язковий)

Копія графічної частини

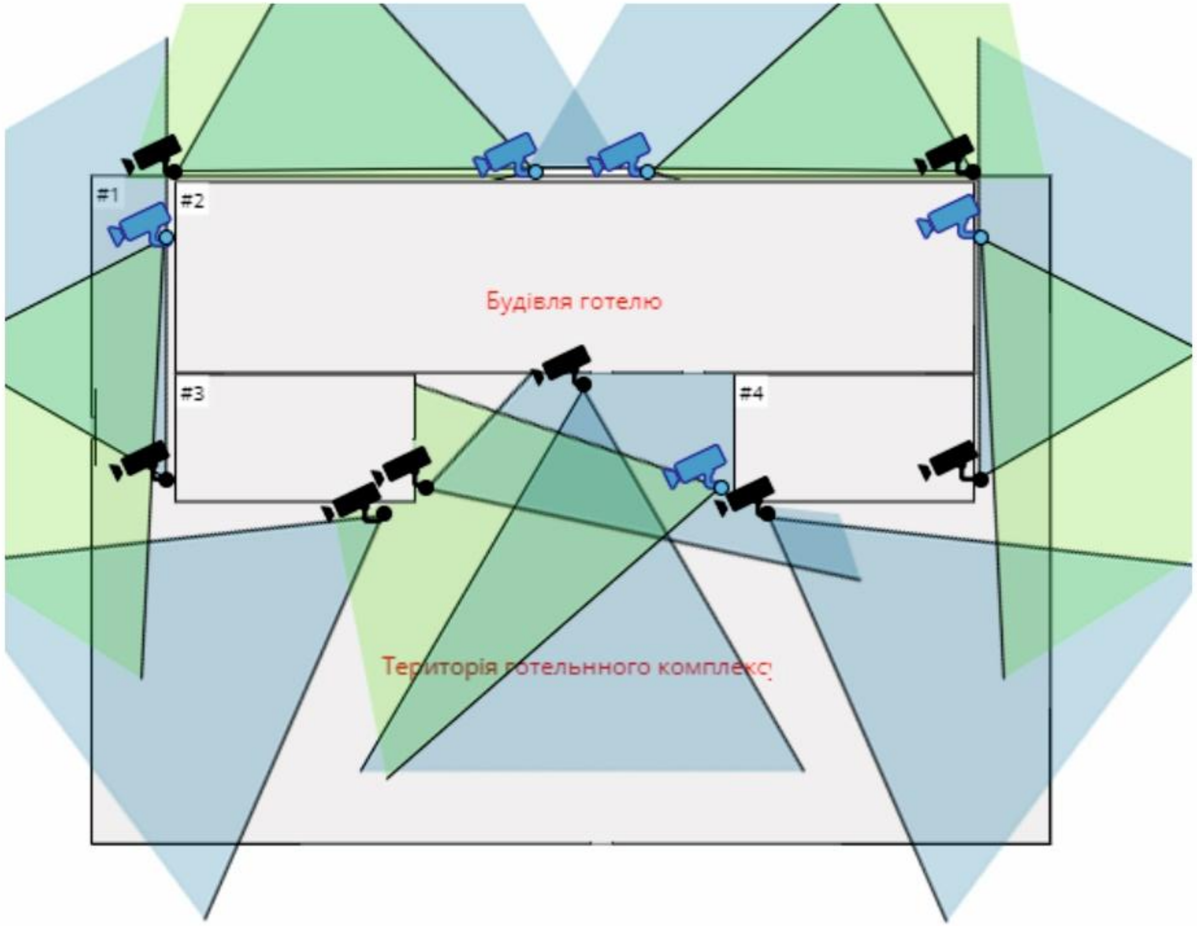


№	Потенційні загрози для інформації	Ризики для:		
		К	Ц	Д
	1 Загрози зі сторони персоналу			
1.1	Працівники можуть бути компрометовані третіми особами через підкуп або шантаж.	+	+	+
1.2	Нецільова діяльність, яка виходить за рамки повноважень	+	+	+
1.3	Надлишковість повноважень	+	+/-	+/-
1.4	Використання 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	+	+/-	+/-

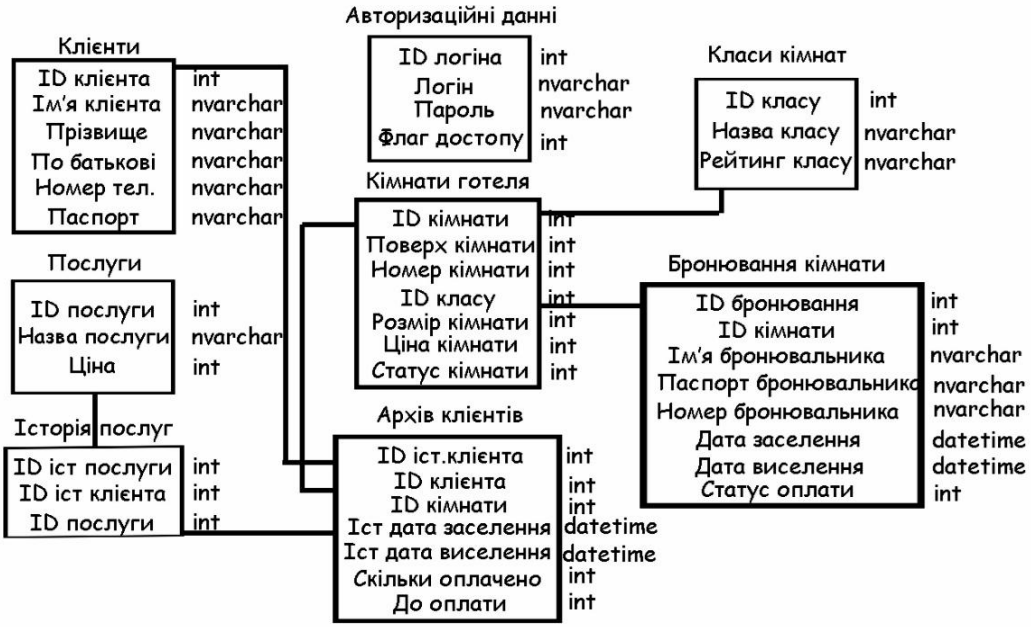
№	Порушник	Категорія порушника	Кваліфікація	Мотив	Можливості щодо пололання	Можливості за місцем дії	Можливості за часом дії	Сума загроз
1 Внутрішні порушники, по необережності								
1.1	Адміністратор	ПВ4	К2	М1	З2	Д4	Ч3	15
1.2	Бухгалтер	ПВ3	К2	М1	З2	Д2	Ч3	12
1.3	Менеджер	ПВ3	К2	М1	З2	Д2	Ч3	12
1.4	Технічний 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

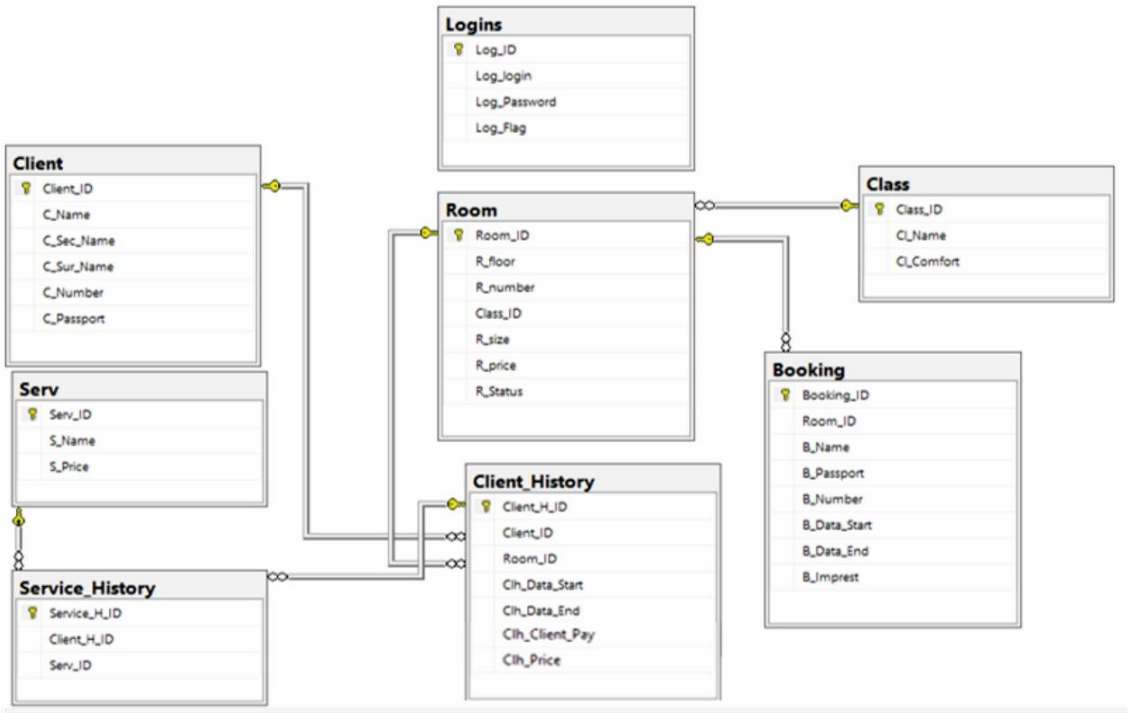


Зм.	Арк.	№ докум.	Підпис	Дата	КРБКБ.220131.22.01.20 Е8			
Розроб.		Хоптинець Б.О.			Система контролю доступу для готельного комплексу. Функціональна схемі мережі та система контролю доступу	Літера	Маса	Масштаб
Перевір.		Клєц Ю.Л.				Аркуш		Аркушів
Н.Контр.								
						ХНУ, КБ-22-1		
Т.Контр.		Мостовий С.В.						
Затв.		Клєц Ю.Л.						



Зм. Арк.	№ докум.	Підпис	Дата	КРБКБ.220131.22.01.20 Е8
Розроб.	Континець Б.О			Система контролю доступу для готельного комплексу Загальна функціональна схема мереж та системи контролю доступу
Перевір.	Клєць Ю.П.			Літера / Маса / Масштаб
Н.Контр.				Аркуш / Аркушів
Т.Контр.	Мостовий С.В.			ХНУ,КБ-22-1
Затв.	Клєць Ю.П.			





						КРБКБ.220131.22.01.20 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Антипець І.О.			Система контролю доступу для готельного комплексу Модель бази даних	Літера	Маса	Масштаб
Перевір.		Кльоц Ю.П.						
Н.Контр.						Аркуш	Аркушів	
Т.Контр.		Маслянай С.В.				ХНУ, КБ-22-1		
Затв.		Кльоц Ю.П.						