**УПРАВЛІННЯ БЕЗПЕКОЮ ГОТЕЛЮ**

### 1. Сутність і значення безпеки готелю

### 2. Характеристика можливих загроз, що можуть виникнути в готелі

### 3. Тактико-організаційні заходи забезпечення умов безпеки в готелі

### 4. Комплекс технічних засобів безпеки в готелі

### **1. Сутність і значення безпеки готелю**

Головне завдання безпеки готелю – реалізація умов, за яких клієнти готелю і його співробітники могли б почувати себе впевнено, спокійно і комфортно.

Поняття безпеки охоплює не лише захист від кримінальних посягань, але й ще створення запобіжних заходів щодо захисту від пожежі, вибуху й інших надзвичайних подій.

Ефективне вирішення цієї проблеми вимагає системного підходу, заснованого на аналізі функціонування об'єкта, виявленні найбільш вразливих зон і особливо небезпечних загроз, складанні всіх можливих сценаріїв кримінальних дій та вироблення адекватних заходів протидії.

Комплексний підхід передбачає оптимальне поєднання організаційних, технічних і фізичних заходів попередження та своєчасного реагування на будь-яку небезпечну ситуацію.

Ключового значення набуває правильний вибір технічних засобів і систем безпеки, їх правильне проектування, монтаж і обслуговування.

*Основними причинами, які виводять застосування технічних засобів на чільні позиції є:*

* несхильність (на відміну від людей) до втоми, неуважності, хвороб, миттєвих почуттів, впливу кліматичних умов;
	+ непідкупність, неможливість обману, шантажу і залякування;
		- миттєвість реакції, точність виконання закладених функцій.

Принципові відмінності готелів, як об'єктів впровадження комплексних систем безпеки, від промислових або військових (режимних) об'єктів полягають в такому:

* готель зацікавлений в створенні іміджу відкритого будинку з забезпеченням режиму найбільшого сприяння максимальному числу гостей. Тому будь-які пристрої безпеки повинні забезпечити у гостя почуття особистої безпеки і комфорту, а не лякати його;
* готелі розташовані в межах міста, в середовищі активного руху транспорту та пішоходів;
* система проходу в готель і номери повинна бути простою і не створювати для гостя великих труднощів.

Зазначені особливості вимагають побудови інтегрованого комплексу технічних засобів безпеки, сутність якого полягає в тому, що всі системи готелю взаємопов’язані, а процеси управління автоматизовані, що полегшує і прискорює в екстремальній ситуації процес прийняття рішень оператором служби безпеки, надаючи йому повну інформацію від усіх систем та автоматизуючи деякі дії. За рахунок передачі інформації іншим службам готелю полегшується робота покоївок, техніків, адміністраторів; підвищується рівень готельного обслуговування, споживачі почувають себе більш комфортно і спокійно.

### **2. Характеристика можливих загроз, що можуть виникнути в готелі**

На підставі статистичних даних і досвіду експлуатації готелів розглянемо найбільш небезпечні загрози:

* *пожежа*(причиною якої може бути недбалість гостей, несправність електрообладнання, недотримання або порушення правил протипожежної безпеки обслуговуючим персоналом, навмисний підпал);
* *вибух*викликаний пронесенням та встановленням вибухівки в кримінальних цілях, або вибух газу при його витоку (особливо ймовірно в місцях приготування їжі в ресторанах, барах при використанні газового обладнання);
* *несанкціонований прохід сторонніх осіб в номери*за відсутності гостей з метою крадіжки цінностей, документів, установлення вибухових пристроїв або підслуховувальної апара[**тур**](https://elearn.nubip.edu.ua/mod/glossary/showentry.php?eid=198909&displayformat=dictionary)и;
	+ *несанкціонований прохід в номери обслуговуючого персоналу*з кримінальними цілями чи обумовлений кримінальними мотивами або шантажем злочинців;
		- *напад на гостя в номері*, ліфті або в іншому місці готелю;
		- *напад на касу*в робочий час або спроба її відкриття у неробочий час;
		- *напад на адміністрацію*готелю з метою шантажу, вимоги відкрити касу або нейтралізувати систему безпеки;
			* *терористичний акт із взяттям заручників*клієнтів готелю або спроба підриву чи підпалу;
			* *збройний напад на номери*, орендовані у готелях комерційними фірмами під офіси.

*За ступенем підготовки і оснащення зловмисники можуть бути розділені на такі групи:*

* випадковий, необізнаний, як правило, не озброєний і без спеціального оснащення чоловік, що намагається проникнути в готель без певного плану дій. До цієї групи належать підлітки, алкоголіки, дрібні хулігани або психічно неврівноважені люди;
* поодинокий грабіжник чи терорист, обізнаний про режим роботи готелю, про місця зберігання значних цінностей або розміщення заможних гостей;
* озброєна група, яка проникає в готель з метою грабежу, теракту або взяття заручників;
* співробітник готелю, який вступив у змову з кримінальною групою з метою наживи або під впливом шантажу.

**Таблиця 39**– **Перелік можливих місць підвищеного інтересу кримінальних груп**

|  |  |
| --- | --- |
| Місця підвищеного інтересу | Можлива акція |
| Каса | Збройне пограбування |
| Приміщення тимчасового зберіганняцінностей | Збройне пограбування, крадіжка |
| Зал прийому / оформлення гостей тамісце зберігання ключів | Захоплення заручників, розкраданняключів |
| Адміністративні приміщення | Захоплення заручників, збройний напад, вбивство |
| Приміщення служби безпеки | Нейтралізація охорони та системисигналізації |
| Готельні номери і особливо[**апартаменти**](https://elearn.nubip.edu.ua/mod/glossary/showentry.php?eid=198825&displayformat=dictionary) люкс | Пограбування, крадіжка, напад нагостей |
| Приміщення для конфіденційнихпереговорів | Установлення підслуховувальноїапаратури |
| Ресторан | Збройне пограбування, захопленнязаручників |

Даний перелік може бути доповнений або змінений залежно від типу готелю і місцевих умов.

### **3. Тактико-організаційні заходи забезпечення умов безпеки в готелі**

Традиційний метод посилення безпеки шляхом збільшення чисельності співробітників не дає бажаного результату як через економічні міркування, так і через малу ефективність такого підходу. Єдине правильне рішення питання безпеки - використання системного, комплексного підходу, що поєднує в собі методи організаційного, технічного і фізичного характеру в їх правильному поєднанні і розумному визначенні частки кожної складової.

До організаційних заходів належать:

* розробка детальних інструкцій щодо дій в усіх можливих позаштатних ситуаціях і доведення їх до кожного співробітника;
* складання коротких, ілюстрованих, високоінформативних й інтуїтивно зрозумілих інструкцій з користування апара[**тур**](https://elearn.nubip.edu.ua/mod/glossary/showentry.php?eid=198909&displayformat=dictionary)ою безпеки для гостей, до яких повинні бути внесені короткі правила поведінки в екстремальній ситуації;
	+ регулярне проведення занять з підвищення кваліфікації персоналу служби безпеки, фізичної та бойової підготовки;
	+ проведення навчання всього персоналу готелю правилам користування апаратурою комплексу безпеки;
	+ організація періодичної (не менше одного разу на рік) перевірки знань в області безпеки для персоналу, проведення додаткових навчань по мірі зміни кадрів і модернізації комплексу;
	+ організація професійної інженерної служби (в рамках штату служби безпеки), до обов'язків якої має увійти проведення технічного обслуговування комплексу автоматизації будівлі, проведення навчання і консультування співробітників інших служб готелю.

### **4. Комплекс технічних засобів безпеки в готелі**

Пріоритетними напрямками забезпечення безпеки сучасного готелю є:

–   комплекс заходів з протипожежного захисту;

–   охоронна сигналізація та відеоспостереження;

–   контроль доступу на об'єкт.

Сформулюємо *загальні положення та вимоги до системи безпеки:*

–    зайва таємничість, жорсткий режим, постійна демонстрація збройної охорони і підозрілості може насторожити частину клієнтів і позбавити готель іміджу «відкритого будинку»;

–    система повинна бути збалансованою, тобто, засоби захисту повинні розподілятися рівномірно, відповідно до значимості зон, які захищаються;

–    всі застосовувані заходи й засоби не повинні створювати додаткової небезпеки здоров'ю, життю гостей та співробітників готелю.

Розглянемо основні підсистеми комплексу технічних засобів безпеки і засоби їх інтеграції в єдину систему.

***Система пожежної безпеки***

Призначення: ефективне і своєчасне виявлення загоряння з точним визначенням місця, оповіщення співробітників служби безпеки, міської служби пожежної охорони, ініціювання (подача сигналу на включення чи відключення) інших систем, документування інформації.

Побудова: для виявлення факту загоряння використовуються різні типи пожежних датчиків (оповіщувачів):

* димові (оптичні, іонізаційні, радіоізотопні, лінійні та ін.). Використовуються в найбільш важливих, пожежонебезпечних зонах, а при можливості в усіх приміщеннях;
* теплові (магнітні, із застосуванням легкоплавких матеріалів, термометричні тощо). Використовуються в менш відповідальних зонах і як допоміжні;
* ручні сигналізатори пожежі. Розташовуються, як правило, поблизу запасних пожежних виходів, у місцях паління тощо;
	+ комбіновані теплодимові датчики.

Інформація від датчиків збирається центральною станцією пожежної сигналізації, що виконує функції контролю стану і працездатності датчиків, шлейфів виконавчих пристроїв, оповіщення, передачі інформації, ініціювання та документування інформації.

*Система візуально звукового оповіщення*

Призначення: екстрене оповіщення гостей і співробітників готелю про виникнення пожежі або іншої екстремальної ситуації, вказання шляхів якнайшвидшої безпечної евакуації, видача іншої екстреної інформації.

Побудова: для оповіщення використовуються спеціалізовані гучномовці, світлові табло з фіксованими написами («Пожежа», «Вихід»), піктограми або світлодіодні табло. Сигнал на вмикання засобів оповіщення подається або автоматично центральною станцією пожежної сигналізації, або оператором системи безпеки. Аналогічно, передана через гучномовці аудіо інформація може або вимовлятися через мікрофон оператором або бути попередньо записана на магнітофон і передаватися автоматично.

*Система пожежогасіння*

Призначення: автоматичне гасіння вогнища загоряння, запобігання поширенню пожежі.

Побудова: можливі такі варіанти:

1)   за принципом пожежогасіння:

–          спрінклерне   пожежогасіння   (найдешевший    варіант    за   умови глобальної реконструкції будівлі);

–   аерозольне або порошкове пожежогасіння;

–       газове пожежогасіння (висока ефективність, не наносить шкоди інтер'єру);

2)   за принципом організації системи:

–        автономні   модулі   пожежогасіння   з   вбудованими   пожежними датчиками;

–    команда на вмикання модуля пожежогасіння подається центральною пожежною станцією або інтегрованою системою безпеки.

*Управління системою вентиляції і димовидалення*

Призначення: Запобігання поширенню диму і вогню від вогнища спалаху по ліфтових і вентиляційних шахтах і трубах, видалення диму з приміщень.

Побудова: вмикаються підсистеми:

–     димовидалення: центральна станція пожежної сигналізації формує сигнали, що запускають відповідні електродвигуни вентиляційної системи.

–         запобігання поширення диму: Центральна станція пожежної сигналізації формує сигнал, що керують приводами заслонок вентиляційної системи, запускає електродвигуни [**тур**](https://elearn.nubip.edu.ua/mod/glossary/showentry.php?eid=198909&displayformat=dictionary)бін, що створюють підвищений тиск у ліфтових шахтах.

*Система розблокування виходів*

Призначення: при виявленні системою пожежної сигналізації вогнища загоряння суворо необхідним є автоматичне розблокування всіх дверей, у тому числі готельних номерів, пожежних та інших виходів для забезпечення безперешкодної евакуації з будівлі. Також необхідним, з погляду пожежної безпеки, є вимога автоматичного спуску ліфтів донизу й повне їх блокування при виникненні пожежі.

Побудова: центральна станція пожежної сигналізації формує сигнали, що передаються головному контролеру (локальним контролерам) системи управління доступом, який забезпечує розблокування дверей*.*

***Система охоронної сигналізації та відеоспостереження***

Призначення: ефективне і своєчасне виявлення факту несанкціонованого проникнення в приміщення, що охороняються (майданчики, зони), з точним визначенням місця, оповіщення співробітників служби безпеки, міліції (позавідомчої охорони), документування інформації.

Захисту за допомогою засобів охоронної сигналізації підлягають:

-   зовнішній периметр готельного комплексу;

-   паркування автотранспорту;

-   зовнішній контур готелі;

-   відповідальні службові приміщення, такі як каса, камера тимчасового зберігання цінностей, комори, кабінети адміністрації готелю, різного роду апаратні і пультові;

-   готельні номери;

-   інші майданчики, зони, приміщення.

Для виявлення факту несанкціонованого проникнення використовуються різні типи сигналізаційних датчиків:

-  датчики (ємнісні, радіопроменеві, проводохвильові, активні інфрачервоні, вібраційні та ін.), що встановлюються на зовнішніх огородженнях та використовуються для охорони периметра (зовнішнього кордону) готельного комплексу та парковок автотранспорту;

-  датчики (мікрохвильові, інфрачервоні пасивні, комбіновані), що охороняють відкриті майданчики та застосовуються для охорони парковок автомобілів;

-  датчики (магнітоконтактні, вібраційні, інфрачервоні активні і пасивні), що сигналізують про відкриванні або руйнуванні дверей, вікон та застосовуються для охорони дверей будівлі, в тому числі ліфтів, надають інформацію для системи управління доступом;

-  датчики (акустичні, вібраційні), що реагують на розбиття скла;

-  датчики (інфрачервоні пасивні, мікрохвильові, ультразвукові, комбіновані, барометричні), що блокують внутрішні об’єми приміщень;

-  датчики (ємнісні, вібраційні та ін), що охороняють окремі предмети: сейфи, вітрини з цінностями, шафи зі зброєю.

Інформація від охоронних датчиків збирається центральною станцією охоронної сигналізації (системою збирання та обробки інформації), що виконує функції контролю стану і працездатності датчиків, шлейфів, виконавчих пристроїв, передачі інформації, документування.

*Система тривожної сигналізації*

Призначення: терміновий виклик (оповіщення про виникнення тривожної ситуації) служби безпеки.

Побудова: для подачі сигналу можуть бути використані різного роду пристрої:

-   механічні тривожні кнопки можуть бути ручними, ножними, прихованими;

-   радіокнопки (радіобрелки) можуть бути одно і багатокнопковими (для подачі різного роду сигналів), суміщеними з пластиковою карткою системи доступу, що дозволяє ідентифікувати особу, яка подала сигнал, її точне місце розташування.

Сигнал тривоги або виклику може бути поданий з інших пристроїв. Наприклад, кодонабірна панель системи управління доступом з набором

«коду тихої тривоги», коли клієнта або співробітника змушують відключити систему під загрозою зброї. За цих умов він може набрати особливий код і тоді система дійсно відключиться, але при цьому на пост служби безпеки надійде тривожне повідомлення про те, що відключення сталося під примусом.

*Система телевізійного спостереження*

Призначення: забезпечення візуального контролю за обстановкою на об'єкті, аналіз позаштатних ситуацій, верифікація (перевірка істинності) надходження сигналів тривоги, допомога в прийнятті оперативних рішень, протоколювання візуальної інформації.

Побудова: відеоінформація збирається телевізійними камерами (чорно- білими або кольоровими). Рекомендуються (стосовно оснащення готелю) такі принципи установки камер:

* відкрите (без маскування): по периметру будівлі, на парковках автотранспорту, в зоні центрального входу, залі реєстрації, у великих холах, приміщеннях особливої важливості, в службових приміщеннях;
* приховане (маскування в годинники, світильники, предмети інтер'єру, замуровування в стіну) в зонах розташування готельних номерів, у приміщеннях особливої важливості (дублюються відкрито встановлені камери).

Взагалі, при виборі типу встановлення потрібно враховувати таку обставину: відкрито встановлена камера, з одного боку, «відлякує» потенційного злочинця, з іншого боку, створює певний моральний дискомфорт для клієнтів.

Відеоінформація від камер надходить до центрального пульта, де за допомогою різного роду відеокомутаційних пристроїв здійснюється обробка відеосигналів (накладення дати, часу, імені або номера камери, поєднання зображень), виведення відеоінформації на монітори, запис на відеореєструвальні пристрої, розподіл інформації між постами, взаємодія з іншими системами комплексу безпеки.

***Система управління доступом***

Призначення: забезпечення безперешкодного санкціонованого доступу в приміщення і блокування несанкціонованого доступу.

Організація режиму доступу:

-  за тимчасовим розкладом;

-  за ієрархією;

-  залежно від оплачених клієнтом послуг тощо;

-  облік робочого часу співробітників;

-  документування інформації.

Побудова: найбільш поширеним у сучасній готельній практиці є використання автономних замків з пластиковою карткою системи VingCard.

Залежно від вимог готелю, можна побудувати систему контролю доступу різного рівня складності та функціональності, яка поєднує всі зони готелю: гостьові номери, зони загального доступу, службові приміщення та адміністративну частину.

*Електронна карткова бездротова он-лайн система - це:*

–     зручний доступ гостей до номерного фонду та дверей загального доступу за єдиною карткою;

–          розмежування доступу персоналу до службових приміщень, номерного фонду, розподільчих шаф тощо;

–    оперативна зміна схеми доступу у реальному часі з робочого місця адміністратора системи;

–   отримання даних про події у реальному часі;

–   дистанційне відмикання дверей (рис.1).

**Рисунок 1 – Електронна карткова бездротова он-лайн система контролю доступу**

*Електронна карткова віртуальна он-лайн система*являє собою:

–   зручний доступ гостей до номерного фонду та дверей загального доступу за єдиною карткою;

–      розмежування доступу персоналу до службових приміщень, номерного фонду, інших точок проходу;

–      оперативна зміна схеми доступу шляхом перенесення інформації ПК– модифікатор-картка-замок;

–      зчитування пам'яті подій замків на картку користувача та перенесення інформації до ПК через он-лайн модифікатор карток (рис.2).



**Рисунок 2 – Електронна карткова віртуальна он-лайн система контролю доступу**

*Електронна карткова оф-лайн система*являє собою (рис.3):

–      зручний доступ гостей до номерного фонду та дверей загального доступу за єдиною карткою;

–   розмежування доступу персоналу до службових приміщень, номерного фонду, розподільчих шаф тощо;

–   зміна схеми доступу шляхом перепрограмування замків;

–   зчитування пам'яті подій замків з використанням мобільних пристроїв перенесення інформації.



**Рисунок 3 – Електронна карткова оф-лайн система**

*Механічна система «Майстер-ключ»*(рис.4) представляє собою:

–   усунення необхідності використання громіздких зв'язок ключів;

–   розмежування доступу персоналу до службових приміщень, номерного фонду, розподільчих шаф тощо;

–   доступ гостей до дверей загального доступу з використанням ключа від номера.



**Рисунок 4 – Механічна система «Майстер-ключ»**

**Система захисту інформації**

Захисту підлягає нижченаведена інформація:

*1.   Інформація про клієнтів категорії VIP*:

–      про факт прибуття і вибуття, час проживання, розпорядок дня, відвідувачів і телефонних абонентів клієнта;

–       про зміст переговорів, що ведуться клієнтом (у номері або в спеціально виділених кімнатах);

–    інформація, що обробляється оргтехнікою (персональний комп'ютер, друкарська машинка, електронна записна книжка тощо).

*2.      Інформація, що обговорюється або оброблена із застосуванням технічних засобів під час нарад у спеціально виділених приміщеннях.*

*3.   Комерційна таємниця.*

Комерційну таємницю про діяльність готелю можуть складати відомості про окремі фінансові показники, про систему ділових зв'язків, відомості про клієнтів, дані з кадрів, відомості щодо організації охорони і протипожежної безпеки.

Технічні заходи мають на меті усунути витік захищуваних відомостей технічними каналами:

–   засобами прослуховування акустичними і віброакустичними каналами;

–   засобами побічних електромагнітних випромінювань і наведень технічних засобів зв'язку, електроживлення, радіотелевізійної приймальної апаратури, електропобутових приладів, оргтехніки тощо;

–   оптичними каналами;

–   засобами несанкціонованого знімання інформації.

*Технічні заходи захисту охоплюють:*

–   звукоізоляцію захисних конструкцій стін, підлог стель;

–   оснащення вікон приміщень, які захищаються, захисними жалюзями, шторами, плівкою;

–         використання сертифікованих засобів технічного захисту від побічних радіовипромінювань;

–      періодичну перевірку приміщень на предмет встановлення в них закладок.

Реалізовані заходи захисту від витоку інформації відображаються в атестаті приміщення, який, за необхідності, видається клієнтам категорії VIP, а також представникам організацій, відповідальних за проведення конфіденційних заходів у спеціально виділених приміщеннях.

*Технічне укріплення будівлі готелю*

Призначення: створення фізичних бар'єрів, що перешкоджають несанкціонованому проникненню в будівлі готельного комплексу шляхом руйнування (злому) інженерних конструкцій будівлі.

Побудова: дана задача може бути вирішена тільки при будівництві нового будинку або при генеральній реконструкції, що допускає її перепланування. В інших випадках можуть бути рекомендовані такі заходи підвищення технічної міцності будівлі:

–   встановлення металевих грат а вікнах першого і цокольного поверхів, обклеювання скла зазначених вікон, а також вікон готельних номерів (усіх або тільки категорії люкс) захисною плівкою;

–    встановлення металевих дверей на входах в найбільш відповідальні приміщення і блоки приміщень;

–      оснащення найбільш важливих дверей високоякісними замковими пристроями,

–   встановлення турнікетів, прохідних кабін, шлюзів.

Створення комплексної інтегрованої системи безпеки дозволяє не тільки значно підвищити рівень безпеки будівлі та її мешканців, а й суттєво полегшити роботу обслуговуючого персоналу та підняти імідж готелю.