Охорона об'єктів критичної інфраструктури

Лекція 6 · Тема 12

Поняття, класифікація, режимні заходи, патрулювання та взаємодія зі спеціальними службами при охороні об'єктів критичної інфраструктури України.

Зміст лекції

01

Поняття та класифікація ОКІ

Ознаки, нормативна база, категорії критичності та сектори інфраструктури.

02

Режимні заходи та виявлення загроз

Складові режиму охорони, класифікація загроз, методи та засоби виявлення.

03

Патрулювання та контроль доступу

КПР, види патрулів, зонування території об'єкта.

04

Взаємодія з адміністрацією та спецслужбами

Обов'язки адміністрації, компетенція служб, алгоритм передачі інформації.

Що таке об'єкти критичної інфраструктури?

Згідно із **Законом України «Про критичну інфраструктуру»**, до цієї категорії належать об'єкти, що надають життєво важливі послуги. Їхнє пошкодження або руйнування призводить до негативних наслідків для національної безпеки.

Незамінність

Відсутність альтернативних способів отримання послуги в короткостроковій перспективі.

Масштабність

Вплив на велику кількість населення або стратегічні галузі економіки.

Взаємозалежність

Збій на одному об'єкті (наприклад, електропідстанції) тягне зупинку інших: водоканалів, лікарень, зв'язку.

Нормативна база та критерії оцінки

Нормативна база

- Закон України «Про критичну інфраструктуру» – базовий закон.
- Постанова КМУ №1109 «Про затвердження Порядку віднесення об'єктів до критичної інфраструктури».

Критерії оцінки Комісії при КМУ

1. **Кількість жертв** – потенційні втрати серед населення у разі аварії.
2. **Економічні збитки** – прямі втрати та вплив на ВВП.
3. **Територіальне поширення** – скільки областей чи районів постраждає.
4. **Тривалість наслідків** – як швидко можна відновити функціонування системи.

Класифікація за категоріями критичності

1

IV — Необхідні об'єкти

Місцеве значення. Порушення відчутне, але не критичне для країни.

2

III — Важливі об'єкти

Вплив обмежений громадою або районом. Приклад: районні тепломережі, хлібозаводи.

3

II — Життєво важливі об'єкти

Криза регіонального рівня або окремої галузі. Приклад: обласні вузли зв'язку, хімічні підприємства.

4

I — Особливо важливі об'єкти

Загальнодержавне значення. Зупинка викликає кризу державного рівня. Приклад: Дніпровська ГЕС, мережі «Укренерго».

Класифікація об'єктів за секторами

Сектор	Приклади об'єктів
⚡ Енергетика	АЕС, ГЕС, ТЕС, нафто- та газопроводи, ЛЕП
✈️ Транспорт	Аеропорти, залізничні вузли, морські порти, мости
💧 Водопостачання	Очисні споруди, водозабори, насосні станції
🏥 Охорона здоров'я	Великі клінічні лікарні, центри медицини катастроф
🌾 Харчова промисловість	Елеватори, великі склади продовольства
💻 Цифрові технології	Дата-центри, вузли зв'язку, телевежі

РОЗДІЛ 2

Режимні заходи охорони

Режимні заходи – встановлений порядок, що забезпечується комплексом організаційних, правових та технічних засобів, спрямованих на захист об'єкта від будь-яких форм незаконного втручання.

Основні складові режиму охорони

Територіальний режим

Поділ об'єкта на зони: публічна, адміністративна, технологічна, режимна.

Пропускний режим

Порядок входу/виходу осіб, в'їзду/виїзду транспорту, внесення/винесення майна (ТМЦ).

Внутрішньооб'єктний режим

Правила поведінки персоналу: використання засобів зв'язку, заборона куріння, порядок зберігання ключів, дотримання графіку робіт.

Інформаційний режим

Захист конфіденційної інформації про системи охорони, схеми комунікацій та паролі.

Класифікація загроз ОКІ

Зовнішні фізичні загрози

- Терористичні акти та диверсії
- Збройний напад або проникнення розвідувальних груп
- Крадіжки обладнання та паливно-енергетичних ресурсів

Внутрішні загрози (Інсайдерство)

- Саботаж з боку персоналу
- Недбалість або порушення правил ТБ
- Передача конфіденційних даних стороннім особам

Кібернетичні загрози

- Атаки на АСУ ТП (автоматизовані системи керування)
- Злам систем відеоспостереження та контролю доступу

Методи та засоби виявлення загроз

🔧 Технічні системи

- **Периметральна сигналізація:** вібраційні кабелі, інфрачервоні бар'єри.
- **Інтелектуальне відеоспостереження:** розпізнавання облич, аналіз залишених предметів, виявлення скупчення людей.
- **Тепловізійний контроль:** виявлення порушників у темряві або задимленості.
- **Детектори дронів:** системи радіоелектронного моніторингу для виявлення БПЛА.

👁️ Оперативні заходи охорони

- **Спостереження:** візуальний контроль за підступами до об'єкта.
- **Профайлінг:** виявлення підозрілих осіб за невербальними ознаками – нервозність, нетиповий одяг, спостереження за постом.
- **Перевірка вразливостей:** регулярний огляд цілісності огорож, замків та пломб.

Алгоритм дій при виявленні загрози

- Згідно з Постановою КМУ №1109, кожен ОКІ повинен мати **План реагування на кризові ситуації** з алгоритмами дій для кожного виду загрози — від анонімного дзвінка про мінування до атаки дрона.

РОЗДІЛ 3

Контрольно-пропускний режим (КПР)

Контроль доступу – перший ешелон захисту. Мета – виключити можливість безконтрольного проходу осіб та проїзду транспорту на територію об'єкта.

Елементи КПР та алгоритм перевірки

Основні елементи КПР

- **КПП** – спеціально обладнані місця для перевірки документів та огляду транспорту.
- **Система перепусток:** постійні (персонал), тимчасові (відряджені), разові (відвідувачі).
- **СКУД:** турнікети, біометричні зчитувачі (відбиток пальця, сітківка, обличчя), магнітні картки.

Алгоритм перевірки на КПП

1. **Ідентифікація** – перевірка відповідності особи пред'явленому документу.
2. **Перевірка підстав** – чи має особа право доступу в цей сектор і в цей час.
3. **Огляд** – металодетектори, інтроскопи (рентген для сумок), газоаналізатори для виявлення вибухівки.

Організація патрулювання території

Піші патрулі

Огляд важкодоступних місць, внутрішніх приміщень та цехів.

Автотранспортні патрулі

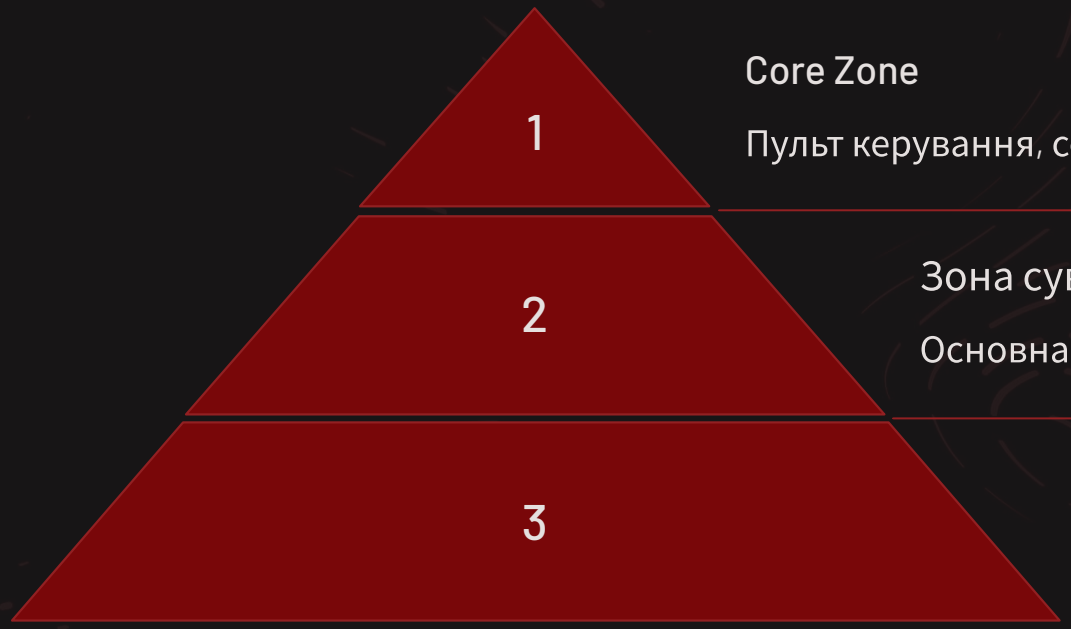
Оперативний об'їзд великих територій та зовнішнього периметру.

Повітряне патрулювання

БПЛА з тепловізорами для моніторингу вночі та у складних погодних умовах.

Тактика: маршрути та час виходу патруля постійно змінюються. На маршруті встановлюються RFID-мітки — патрульний фіксує присутність у конкретній точці у визначений час.

Зонування території ОКІ



Core Zone

Пульт керування, серверна, газорозподільний вузол. Принцип «двох осіб».

Зона суворого режиму

Основна територія з виробничими потужностями.

Вільна зона

Адміністративні будівлі, бюро перепусток, стоянка.

Кожна зона має власний рівень безпеки та обмежений перелік осіб, що мають право доступу. Особливо важлива зона (Core Zone) доступна лише обмеженому колу осіб за принципом «двох осіб» — вхід мінімум удвох.

РОЗДІЛ 4

Взаємодія з адміністрацією та спецслужбами

Адміністрація ОКІ несе повну відповідальність за створення умов безпеки. Охорона ніколи не діє ізольовано — при серйозній загрозі залучаються державні органи.

Ключові обов'язки адміністрації ОКІ

Фінансування

Забезпечення закупівлі технічних засобів: відеокамери, датчики, зброя для охорони.

Кадровий контроль

Надання списків працівників із доступом до зон та оперативне інформування про звільнення (анулювання перепусток).

Розробка документації

Створення Паспорта безпеки об'єкта та Інструкцій з режиму.

Технічна підтримка

Безперебійне освітлення, робота систем зв'язку та справність огорож.

Спеціальні служби та їхня компетенція

Служба	Сфера відповідальності щодо ОКІ
СБУ	Антитерористичний захист, протидія диверсіям та кіберзагрозам.
Національна поліція (НПУ)	Охорона громадського порядку навколо об'єкта, затримання злочинців.
ДСНС України	Ліквідація пожеж, наслідків аварій, розмінування підозрілих предметів.
Національна гвардія	Безпосередня фізична охорона об'єктів I та II категорій (наприклад, АЕС).

Організація каналів взаємодії

1

Єдиний черговий центр

Прямі канали зв'язку (виділені лінії, радіочастоти) з черговими частинами СБУ та поліції.

2

Плани взаємодії

Документи, погоджені з керівниками спецслужб: хто прибуває першим, порядок пропуску спецтранспорту, сигнали «свій-чужий».

3

Спільні навчання

Мінімум раз на півроку — тренування за сценаріями «Захоплення заручників», «Витік радіації» тощо.

Алгоритм передачі інформації про загрозу

Доповідь

Повідомити

Забезпечити доступ

Локалізація

📋 План охорони та оборони

Таємний документ – дії при надзвичайних ситуаціях.

📄 Інструкція з пропускного режиму

Основний документ для постів охорони.

📒 Журнал прийому-здачі чергування

Фіксація всіх подій за зміну.