Практична робота КР 3.2

Тема: Моделювання інтегрованої системи безпеки для об’єкта критичної інфраструктури (електропідстанція високої напруги)

Мета роботи:

Сформувати у студентів здатність моделювати інтегровану систему безпеки для об’єкта критичної інфраструктури – електропідстанції високої напруги, з урахуванням технічних, організаційних, інформаційних та нормативних компонентів. Ознайомити з принципами системного підходу до управління ризиками, сучасними технологіями безпеки та методами забезпечення стійкості об’єктів енергетичної інфраструктури до техногенних, природних та антропогенних загроз.

Теоретичні відомості:

Об’єкти критичної інфраструктури – це системи, ресурси та об’єкти, порушення функціонування яких може призвести до значних соціальних, економічних або екологічних наслідків. Електропідстанції високої напруги належать до таких об’єктів, оскільки забезпечують передачу та розподіл електроенергії, що є основою життєдіяльності промисловості, транспорту, медицини, зв’язку та інших галузей.

У сучасних умовах, коли зростає кількість загроз – від технічних несправностей до кібератак і диверсій – виникає потреба у створенні інтегрованих систем безпеки, які поєднують різні рівні захисту, забезпечують моніторинг, реагування та стійкість до надзвичайних ситуацій. Моделювання такої системи є важливим етапом у плануванні, проєктуванні та експлуатації об’єктів енергетичної інфраструктури.

Поняття інтегрованої системи безпеки. Інтегрована система безпеки – це сукупність технічних, програмних, організаційних та нормативних елементів, які функціонують узгоджено для забезпечення захисту об’єкта від внутрішніх і зовнішніх загроз. Така система має бути адаптивною, багаторівневою та здатною до самостійного реагування на зміну умов.

Для електропідстанції високої напруги інтегрована система безпеки охоплює:

- **Фізичну безпеку** – охорону периметра, контроль доступу, відеоспостереження.
- **Технічну безпеку** – моніторинг стану обладнання, аварійне відключення, захист від перенапруги.
- **Інформаційну безпеку** – захист цифрових систем управління, мережевих протоколів, баз даних.
- **Екологічну безпеку** – контроль викидів, захист від пожеж, реагування на аварії.

- **Організаційну безпеку** – підготовку персоналу, інструктажі, планування дій у надзвичайних ситуаціях.

Принципи побудови інтегрованої системи безпеки.
Моделювання інтегрованої системи безпеки має базуватися на таких принципах:

1. Системність.

Безпека не може бути забезпечена окремими елементами – вона потребує узгодженої роботи всіх компонентів. Важливо враховувати взаємозв'язки між технічними, людськими та інформаційними факторами.

2. Превентивність.

Система має бути орієнтована на запобігання загрозам, а не лише на реагування. Це передбачає прогнозування ризиків, аналіз сценаріїв, впровадження превентивних заходів.

3. Адаптивність.

Умови функціонування об'єкта можуть змінюватися – технічні параметри, зовнішні загрози, нормативні вимоги. Система має бути здатною до швидкої адаптації.

4. Надійність.

Усі елементи системи мають працювати стабільно, з мінімальним ризиком відмови. Особливо це стосується аварійних систем, резервного живлення, каналів зв'язку.

5. Інтеграція.

Система має об'єднувати різні технології – відеоспостереження, сенсори, програмне забезпечення, комунікаційні платформи – в єдину архітектуру.

6. Відповідність нормативам.

Модель має враховувати чинні стандарти, закони, галузеві регламенти, зокрема щодо охорони праці, цивільного захисту, енергетичної безпеки.

Основні компоненти моделі безпеки електропідстанції.

Фізичний захист.

Передбачає охорону периметра, контроль доступу до критичних зон, встановлення бар'єрів, датчиків руху, систем відеоспостереження. Важливо забезпечити захист від несанкціонованого проникнення, диверсій, крадіжок.

Технічний моніторинг.

Включає системи контролю параметрів обладнання – напруги, струму, температури, вібрацій. Застосовуються автоматизовані системи діагностики, аварійного відключення, резервного живлення.

Інформаційна безпека.

Цифрові системи управління підстанцією мають бути захищені від кібератак, несанкціонованого доступу, втрати даних. Використовуються шифрування, багаторівнева автентифікація, антивірусні платформи, системи резервного копіювання.

Екологічна безпека.

Передбачає контроль за впливом на довкілля – викиди, шум, електромагнітне поле. Важливо мати системи пожежогасіння, аварійного реагування, нейтралізації небезпечних речовин.

Організаційна структура.

Модель має включати розподіл відповідальності між підрозділами, процедури інформування, навчання персоналу, плани евакуації, сценарії реагування на надзвичайні ситуації.

Етапи моделювання системи безпеки

1. Ідентифікація загроз.

Аналізуються потенційні загрози – технічні, природні, антропогенні, кібернетичні. Визначаються джерела ризику, їх ймовірність та наслідки.

2. Визначення цілей безпеки.

Формулюються цілі – захист персоналу, збереження обладнання, безперервність енергопостачання, відповідність нормативам.

3. Вибір технологій.

Обираються технічні рішення – сенсори, камери, програмне забезпечення, системи зв’язку – які відповідають потребам об’єкта.

4. Побудова архітектури.

Створюється модель взаємодії компонентів – як фізичних, так і цифрових. Визначаються точки інтеграції, канали передачі даних, логіка реагування.

5. Тестування та адаптація.

Модель перевіряється в умовах симуляції, аналізуються її слабкі місця, вносяться корективи. Проводяться навчання, тренування, аудит.

Значення теми для України

У контексті постконфліктного відновлення, енергетичної трансформації та зростання кіберзагроз, моделювання інтегрованих систем безпеки для об’єктів критичної інфраструктури набуває особливої актуальності. Електропідстанції високої напруги є стратегічними об’єктами, від яких залежить стабільність регіонів, функціонування промисловості та безпека населення. Сучасні моделі безпеки мають враховувати не лише технічні аспекти, а й соціальні, екологічні та інформаційні виклики.

Моделювання інтегрованої системи безпеки – це складний, міждисциплінарний процес, що поєднує інженерію, управління ризиками, інформаційні технології та нормативне регулювання

Варіанти задач для самостійного опрацювання

1. Розробити модель інтегрованої системи безпеки для хімічного підприємства з урахуванням ризику витоку токсичних речовин.
2. Сформувати систему безпеки для логістичного хабу з використанням сенсорів руху, GPS-моніторингу та прогнозування перевантажень.
3. Моделювати цифрову систему безпеки для водоочисної станції з контролем якості води, доступу та кіберзахистом.
4. Розробити інтегровану систему безпеки для атомної електростанції з багаторівневим моніторингом та автоматичним реагуванням.
5. Створити модель безпеки для підприємства з ВДЕ (вітрова електростанція) з урахуванням погодних ризиків та технічних збоїв.
6. Моделювати систему безпеки для транспортного вузла (залізнична станція) з сенсорами навантаження, відеоаналітикою та прогнозуванням заторів.
7. Розробити систему безпеки для агропромислового комплексу з контролем температури, вологості та біологічних загроз.
8. Сформувати модель безпеки для підприємства, що працює в зоні бойових дій, з мобільними сенсорами, резервними каналами зв’язку та адаптивним реагуванням.
9. Моделювати систему безпеки для складу небезпечних речовин з багаторівневим контролем доступу та автоматичним гасінням.
10. Розробити інтегровану систему безпеки для міської електромережі з прогнозуванням перевантажень, кіберзахистом та аварійним реагуванням.

Роботу оформити окремим файлом та прикріпити до МУДЛ.