МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Захист інформації в спеціалізованих ІТС

Практичне заняття №6

Виконання завдань фреймворку управління ризиками для OT/ICS. Категоризація інформаційної системи

Перевірив:
Зубок В. Ю.

Виконав:
студент І курсу
групи ФБ-41мп
Сахній Н. Р.

Київ 2025

Завдання до виконання:

1. Оберіть три уявні промислові, виробничі чи подібні об’єкти з різних секторів економіки (*легка промисловість, харчова промисловість, важка промисловість, транспорт, енергетична галузь, водопостачання, комунальні послуги, видобуток природних ресурсів тощо*). Визначте масштаб їхньої діяльності та опишіть взаємодію з природним середовищем, населенням, державою де вони функціонують.

❖ **<u>Об’єкт №1</u>: Опалення, вентиляція і кондиціонування (ОВіК)**

- <u>Масштаб діяльності</u>: “Локальний” – система клімат-контролю, для прикладу в дата-центрах, функціонує в межах однієї будівлі.

- **Природне середовище**: система ОВіК споживає електроенергію, тому недосконалий обігрів або охолодження призводитиме до збільшення викидів (через більшу потребу в електроенергії).

- **Населення**: ОВіК забезпечує комфорт і здоров’я людей (контроль температури, вологості, якості повітря), але при незадовільному управлінні може створювати перешкоди (такі як: шум, нестача вентиляції) або ризики (наприклад, поширення алергенів).

- **Держава**: ОВіК-системи будівель регулюються будівельними нормами, а також стандартами енергоефективності (технічними регламентами, законами про енергоощадність), тому відповідно держава зацікавлена в зниженні енергоспоживання будівель та використанні екологічно безпечних технологій ОВіК.

❖ **<u>Об’єкт №2</u>: Нафтопереробний завод (НПЗ)**

- <u>Масштаб діяльності</u>: “Розподілений” – складається з кількох технологічних майданчиків об’єднаних єдиною SCADA/DCS.

- **Природне середовище**: НПЗ суттєво впливає на довкілля, адже викиди в повітря включають токсичні органічні сполуки, а також оксиди сірки та азоту, які спричиняють проблеми з диханням.

- **Населення**: НПЗ створює робочі місця і забезпечує економічну активність регіону, але й несе ризики для здоров’я та безпеки населення. У разі аварій (вибухів, пожеж) можуть постраждати працівники заводу та мешканці прилеглих територій.

- **Держава**: НПЗ є стратегічно важливим об’єктом для енергетичної безпеки країни, тому держава здійснює контроль видобутку, переробки та експорту нафтопродуктів, а також викидів в повітря.

❖ **<u>Об’єкт №3</u>: Газотранспортна система (ГТС)**

- <u>Масштаб діяльності</u>: “Транскордонний” – система магістральних газопроводів та компресорних станцій пролягає через різні країни.

- **Природне середовище**: Транспортування газу може викликати викиди метану при протіканнях. Аварії на газопроводах можуть спричинити масштабні забруднення (загоряння/вибух).

- **Населення**: ГТС забезпечує мільйони споживачів теплом і енергією, яка є критичною для населення та промисловості. Однак існує пряма небезпека для споживачів при вибухах чи загораннях.

- **Держава**: ГТС – стратегічна інфраструктура, що часто задіяна у міжнародних відносинах (договори про транзит між країнами). Держава регулює операторів, видає ліцензії і контролює безпеку (національні стандарти газопроводів, екологічні норми та т.п.).

2. Уявіть інформаційну систему кожного об'єкту (*чи якусь окрему частину цієї системи, наприклад, мережа збору первинної інформації датчиків диспетчерського контролю*). Категоризуйте цю інформаційну систему, враховуючи рівні небезпечних подій, які можуть трапитись на підприємстві, та рівні впливу на кожен «сенсор» інформаційної безпеки (цілісність, конфіденційність, доступність), на основі таблиць 1 та 2.

1) <u>Інформаційна система ОВіК</u>:

Об'єкт зазвичай використовує систему керування будівлею (Building Management System, SCADA/BMS), що відповідно призначена для здійснення контролю обігріву, кондиціонування та вентиляції. Типи інформації, яка обробляється в системі наступні:

- Показники температури, вологості, тиску та забрудненості повітря;
- Журнали споживання енергії й експлуатаційного стану обладнання.

Рівень впливу – "помірний" (забезпечення комфортних умов праці згідно нормативів).

Ціль безпеки	Рівень впливу	Аргументація
Цілісність	Помірний	Зміна даних датчиків може привести до невідповідного регулювання клімату
Конфіденційність	Низький	Фактично, "чутлива" інформація відсутня
Доступність	Високий	Відмова BMS може спричинити дискомфорт або перебої в експлуатації будівлі

2) Інформаційна система НПЗ:

На виробництві використовується централізована SCADA- або DCS-система для управління технологічними процесами НПЗ. Типи інформації, яка обробляється:

- Показники технологічних параметрів;
- Стан перекачувальних насосів і клапанів;
- Аварійні сигнали систем безпеки.

Рівень впливу – "високий" (критична інфраструктура, небезпечні матеріали, нафтохімія).

Ціль безпеки	Рівень впливу	Аргументація
Цілісність	Високий	Фальсифікація сенсорних даних чи команд може призвести до неконтрольованих процесів, аварій чи пожеж
Конфіденційність	Помірний	Технологічна інформація є менш критичною, але захищати комерційні дані потрібно
Доступність	Високий	Зупинка виробництва може спричинити екологічні ризики й завдати фінансових втрат

3) Інформаційна система ГТС:

Об'єкт зазвичай використовує розподілені SCADA-системи для керування ГТС з віддаленими RTU-станціями по лінії та центрами управління. Типи інформації наступні:

- Показники тиску і витрат газу на різних ділянках;
- Статус перемичок, клапанів та кранів подачі газу;
- Телеметрія систем зв'язку та стан датчиків.

Рівень впливу – "високий" (критична інфраструктура, забезпечення безперебійного постачання газу до споживачів, капітальні інвестиції, вибухонебезпечні матеріали).

Ціль безпеки	Рівень впливу	Аргументація
Цілісність	Високий	Зміна даних із датчиків чи команд може викликати некоректну роботу клапанів і призвести до аварійних ситуації
Конфіденційність	Помірний	Технологічна інформація є менш критичною, але захищати комерційні дані потрібно
Доступність	Високий	Відключення центру управління чи зв'язку з RTU може зупинити газопостачання

3. Результат по кожній системі представте у вигляді:

Вплив = {Цілісність:Рівень, Конфіденційність:Рівень, Доступність:Рівень}

1) **Інформаційна система ОВіК**

Вплив = {Цілісність:Помірний, Конфіденційність:Низький, Доступність:Високий}

2) **Інформаційна система НПЗ**

Вплив = {Цілісність:Високий, Конфіденційність:Помірний, Доступність:Високий}

3) **Інформаційна система ГТС**

Вплив = {Цілісність:Високий, Конфіденційність:Помірний, Доступність:Високий}

4. Запропонуйте контролі безпеки з відомих “CIS Controls” (The 18 Critical Information Security Controls) для пом’якшення ризику інцидентів інформаційної безпеки, враховуючи проведену категоризацію.

1) **Інформаційна система ОВіК**

* Control №1: Inventory and Control of Enterprise Assets – застосовувати до IoT-пристроїв для виявлення несанкціонованих компонентів у BMS-системі.

* Control №2: Inventory and Control of Software Assets – налаштувати контроль за використанням авторизованого ПЗ на системах керування ОВіК.

* Control №4: Secure Configuration of Enterprise Assets and Software – встановити безпечні налаштування мережевих пристроїв і вбудованих систем.

* Control №7: Continuous Vulnerability Management – забезпечити своєчасне виявлення та усунення вразливостей у прошивках, BMS-серверів і т.д.

2) **Інформаційна система НПЗ**

* Control №1: Inventory and Control of Enterprise Assets – налаштувати точне відстеження всіх SCADA-компонентів: PLC/RTU, HMI і т.п.

* Control №7: Continuous Vulnerability Management – здійснювати регулярний аналіз вразливостей у SCADA/DCS-платформах.

* Control №12: Network Infrastructure Management – налаштувати DMZ, сегментацію OT-мереж і контроль доступу до мережевого обладнання.

* Control №13: Network Monitoring and Defense – виявляти аномальну активність в OT-сегменті через IDS/IPS в SCADA-протоколах.

3) **Інформаційна система ГТС**

* Control №1: Inventory and Control of Enterprise Assets – контролювати усі пристрої на тисячах км газопроводу – RTU, маршрутизаторів, контролерів.

* Control №7: Continuous Vulnerability Management – здійснювати моніторинг вразливостей на всіх критичних вузлах компонентів OT/ICS.

* Control №12: Network Infrastructure Management – забезпечити надійне управління сегментами мережі, маршрутизаторами, VPN-шлюзами і т.д.

* Control №13: Network Monitoring and Defense – впровадити системи збору телеметрії з RTU та віддалених вузлів для виявлення атак/вторгнень.