Державна служба спеціального зв’язку та захисту інформації України
Державний центр кіберзахисту

ПЕРСПЕКТИВИ ПОБУДОВИ ДЕРЖАВНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Худинцев М.М. - начальник ДЦКЗ Держспецзв’язку
Давидюк А.В. – фахівець сфери захисту інформації

ТЕХНІЧНІ АСПЕКТИ ЗАХИСТУ ОКІІ. ТЕНДЕНЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ (далі – АСУ ТП)

Використання широко розповсюджених технологій

- Операційні системи – Windows, WinCE, Linux тощо.
- Застосунки – Системи управління базами даних, веб-сервери, тощо.
- Протоколи – HTTP, RPC, FTP, DCOM, XML, SNMP, тошо.

Підключення АСУ ТП до корпоративних мереж

- Підвищення ефективності управління організацією.
- Віддалений доступ.

Розповсюдження IP та Ethernet мереж

- Загально прийнятні на верхніх рівнях, і розповсюджуються нижче.
- Велика кількість протоколів може використовувати TCP та UDP як транспорт.
- Більшість сучасних промислових пристроїв мають Ethernet порти.

ТЕХНІЧНІ АСПЕКТИ ЗАХИСТУ ОКІІ. ТЕХНІЧНІ ПРОБЛЕМИ

- Захист від атак DoS та DDoS
- Незахищена реалізація мережевих протоколів у пристроях АСУ ТП
- Не встановлені оновлення операційної системи і застосунків
- Відсутність антивірусного програмного забезпечення
- Незахищена аутентифікація та авторизація
- Неякісний аудит і реєстрація подій
- Не цільове використання ресурсів АСУ ТП
- Вимоги до віддаленого доступу/інтеграції
- Людський фактор

ТЕХНІЧНІ АСПЕКТИ ЗАХИСТУ ОКІІ. ІНШІ ОБМЕЖЕННЯ

- Екстримальні умови експлуатації
- Нетипові фізичні топології
- Велика кількість пристроїв спеціального призначення з обмеженою функціональністю
- Статичні мережеві конфігурації
- Broadcast та багатоадресовий трафік
- Довготривалий строк експлуатації
- Велика кількість застарівшого обладнання

МЕТОДОЛОГІЧНІ ПРОБЛЕМИ ЗАХИСТУ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (далі - ОКІ)

Одним з основних недоліків при виявленні ключових ОКІ є широке використання методик на основі методу експертних оцінок, який потребує обов’язкової наявності інформації про можливі збитки «еталонного об’єкту» або розробки спеціальної шкали факторів ризику.

Наприклад: The Asset Prioritization Model.

МЕТОДОЛОГІЧНІ ПРОБЛЕМИ ЗАХИСТУ ОКІ

При застосуванні таких моделей не приділяється достатньої уваги зв’язності об’єктів, що вона містить.

Існують складноші у повному розумінні всіх взаємозв'язків і взаємозалежностей між її об‘єктами.

Водночас без врахування та аналізу мережевої складової кожного сектору (сегменту) критичної інфраструктури (економічного, фінансового, енергетичного тощо) дуже проблематично забезпечити достатню адекватність моделі об’єкту дослідження.

КЛАСИФІКАЦІЯ. ТИПИ ЗВ'ЯЗКІВ ОКІ

Фізичний - визначає інженерну взаємозалежність між об'єктами.

Інформаційний - залежність від інформаційного обміну (потоку інформації) між об'єктами.

Геопросторовий – взаємозалежність, що виникає в результаті спільного розташування компонентів інфраструктури на місцевості.

Процедурний (політичний) - подібна взаємозалежність, що виникає при будь-якій зміні (події) в одному з компонентів сектора інфраструктури і тягне за собою вплив на об'єкти інших секторів.

Соціальний - така взаємозалежність може виражатися через соціальні чинники: громадська думка, суспільна довіра, страх та ін.

Джерело:
S. Rinaldi, J. Peerenboom, and T. Kelly. «Idenlifying, Understanding, and Analyzing Critical Infrastructure Interdependencies». IEEE Control Systems Magazine, IEEE, December 2001, pp. 11-25.
D. D. Dudenhoeffer. M. R. Permann. and M Manic. «CIMS: A Framework For Infrastructure Interdependency Modeling And Analysis.» Submitted to Proceedings of the 2006 Winter Simulation Conference, L. F. Perrone, F. P. Wieland, J. Liu, B. G. Lawson, D. M. Nicol, and R. M. Fujimoto. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers. 2006.

КЛАСИФІКАЦІЯ. ТИПИ ВЕЛИКИХ СКЛАДНИХ СИСТЕМ

Комплексна система - це відкрита система (локального масштабу) тісно взаємопов'язаних об'єктів, яка з часом еволюціонує і змінює свою поведінку в залежності від протікаючих внутрішніх процесів і зовнішніх умов і впливів.

Метасистема - це форма інтеграції автономних комплексних систем.

Система корпоративного рівня - це комплексна система стратегічного масштабу.

Таким чином, критична інфраструктура будь-якої держави не що інше, як велика складна система стратегічного масштабу, що представляє собою сукупність значної кількості елементов різного типу, об'єднаних зв'язками різної природи, і що володіє загальною властивістю (призначенням, функцією), відмінним від властивостей окремих елементів всій сукупності, що і вимагає розробки спеціальних методів дослідження.

Джерело:

Introduction to functional dependency network analysis. Paul R. Garveyl, Ph.D. and C. Ariel Pinto2, Ph.D. The MITRE Corporation and Old Dominion University P 2009, The MITRE Corporation. All Rights Reserved. Published and Used by MIT ESD and CESUN With Permission Approved for Public Release; Distribution Unlimited; 08-0418.

ЗАСОБИ ВИРІШЕННЯ ЗАЗНАЧЕНИХ ПРОБЛЕМ. ТЕОРІЯ КЛАУЗЕВІЦА ДЛЯ МЕРЕЖЕВИХ АРХІТЕКТУР

Теорія центрів ваги Клаузевіца полягає в тому, що центром ваги є деяка «центральна точка» держави або збройних сил, навколо якої все обертається.

У доктрині НАТО центр ваги описується як потенціал або місце, де держави, альянси, бойові формування або інші типи угруповань концентрують свої можливості для досягнення свободи дій, фізичної потужності (сили) і готовності вести боротьбу.

Дана теорія дозволяє не тільки розробляти методи виявлення критично важливих об'єктів (центрів ваги) інфраструктури, але і визначати можливі заходи і способи впливу на них.

Джерело:
Clausewitz, C-V (1832). On War. Swedish translation by Mertensson. Buhme och Johansson (1991). Stockholm, Sweden: Bonnier Fakta Bokfurlag.
NATO (2003). Gudelines for operational planning.

ЗАСОБИ ВИРІШЕННЯ ЗАЗНАЧЕНИХ ПРОБЛЕМ. ТЕОРІЯ САМООРГАНІЗОВАНИХ СИСТЕМ АЛЬБЕРТО-БАРАБАШИ

Відповідно до його теорії будь-яка неструктурована (пуассонівська) мережа під впливом набору загальновідомих правил і законів, в першу чергу економічного і соціального характеру, через певний час (після деякого числа ітерацій) приймає відповідну структуру, без будь-якого зовнішнього впливу організуючись навколо найбільш цінних або важливих вузлів.

ЗАСОБИ ВИРІШЕННЯ ЗАЗНАЧЕНИХ ПРОБЛЕМ. АТРИБУТИ «ЦЕНТРУ ВАГИ» КЛАУЗЕВІЦА

- **критичні можливості** (Critical Capabilities) - здатності (-сть) об'єкта, які роблять його ключовим в контексті певного сценарію, ситуації або завдання;
- **критичні потреби** (Critical Requirements) - умови, засоби, ресурси, методи або способи дії, що дозволяють об'єкту досягати критичних можливостей;
-**критична вразливість** (Critical Vulnerabilities) - найбільш вразлива потреба або складовий елемент, виведення з ладу якого не дозволить об'єктам досягти критичних можливостей або виконати поставлене завдання.

ЗАСОБИ ВИРІШЕННЯ ЗАЗНАЧЕНИХ ПРОБЛЕМ. ТЕОРІЯ ГРАФІВ.

Використанням теорії графів для побудови імітаційних моделей, дозволяє наочно уявити комплексні взаємозв'язки між об'єктами і розробити математичні вирази для опису рівня взаємодії і взаємозалежності.

У зв'язку з цим критична інфраструктура, як велика складна система стратегічного масштабу, може бути представлена у вигляді зваженого орієнтованого графа, вершини якого - об'єкти, а ребра - зв'язки між ними.

ЗАСОБИ ВИРІШЕННЯ ЗАЗНАЧЕНИХ ПРОБЛЕМ. ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

В імітаційних моделях можуть застосовуватися різні методи (агентське моделювання, дискретно-подієве, динамічне), а вибір будь-якого з них залежить від специфіки досліджуваної інфраструктури і завдань дослідження.

Основні зусилля в цій області повинні бути спрямовані на створення моделей, точно імітуюючих поведінку критичної інфраструктури і дозволяють визначати взаємозв'язки між її об'єктами і виявляти найбільш вразливі з них.

ПРИКЛАДИ ІСНУЮЧИХ ІМІТАЦІЙНИХ МОДЕЛЕЙ

«Система моделювання критичних інфраструктур» (Critical Infrastructure Interdependency Modeling - CIMS)

Для ефективної взаємодії оператора з програмою є ряд можливостей:
- створення певного сценарію подій для ініціювання аварійних подій через заданий проміжок часу;
- вибору і безпосереднього управління станом окремих об'єктів і зв'язків між ними (одним кліком користувач може імітувати вихід з ладу моста, електростанції і ін.);
- введення додаткової події безпосередньо під час роботи моделі для відкриття і відображення каскадного ефекту.

ПРИКЛАДИ ІСНУЮЧИХ ІМІТАЦІЙНИХ МОДЕЛЕЙ МОДЕЛЕЙ

Модель «Афіна» - програмний інструмент, розроблений для аналізу великих складних систем стратегічного масштабу (включаючи політичний, військовий, економічний інформаційний сектори), а також для виявлення взаємозалежності і взаимозв’язності їх елементів. У ній передбачено графічний інтерфейс з можливістю відображення виявлених об'єктів, зв'язків між ними і визначення ступеня їх взаємозалежності. Крім того, модель інтегрована з геоінформаційними системами.

У цьому програмному забезпеченні використовуються метод Барлоу (Barlow) для визначення горизонтальної зв'язності елементів з ваговими коефіцієнтами та метод Вардена (Warden) - для розкриття вертикальної взаємозалежності і ін.

ЗАСОБИ ВИРІШЕННЯ ЗАЗНАЧЕНИХ ПРОБЛЕМ

Математичний опис ступеня зв'язності об'єктів критичної інфраструктури необхідний для здійснення пошуку ланцюжків відмов у всіх взаємопов'язаних секторах і **прогнозування** відмов N-го покоління.

Пошуком ключових об'єктів, вплив на які може надати найбільш негативний ефект, дослідження критичної інфраструктури не обмежується.

Після чого, як правило, проводиться оцінка уразливості розкритих «центрів тяжіння» за допомогою інженерного методу побудови дерева відмов, що трансформується в дерево подій, що дозволяє визначити можливі уразливості інфраструктури, а також їх варіації.

На наступному етапі розробляються алгоритми оцінки ризиків, сенс яких полягає у визначенні ресурсів, необхідних для забезпечення безпеки (впливу) найбільш важливих з виявлених об'єктів критичної інфраструктури. При цьому одним з головних умов залишається дотримання критерію «вартість - ефективність», а ключова проблема полягає в тому, щоб правильно вибрати способи і засоби для організації захисту або впливу.

ПРИНЦИПИ ЗАХИСТУ ОКІ

Забезпечення захисту ОКІ повинно враховувати наслідки закону Парето, основними з яких є наступні:

- значущих чинників трохи, а тривіальних безліч - лише поодинокі дії призводять до важливих результатів;
- більша частина зусиль не дає бажаних результатів;
- більшість вдалих подій обумовлено дією незначного числа високопродуктивних сил, а більшість неприємностей пов'язано з дією невеликого числа високодеструктивних сил.

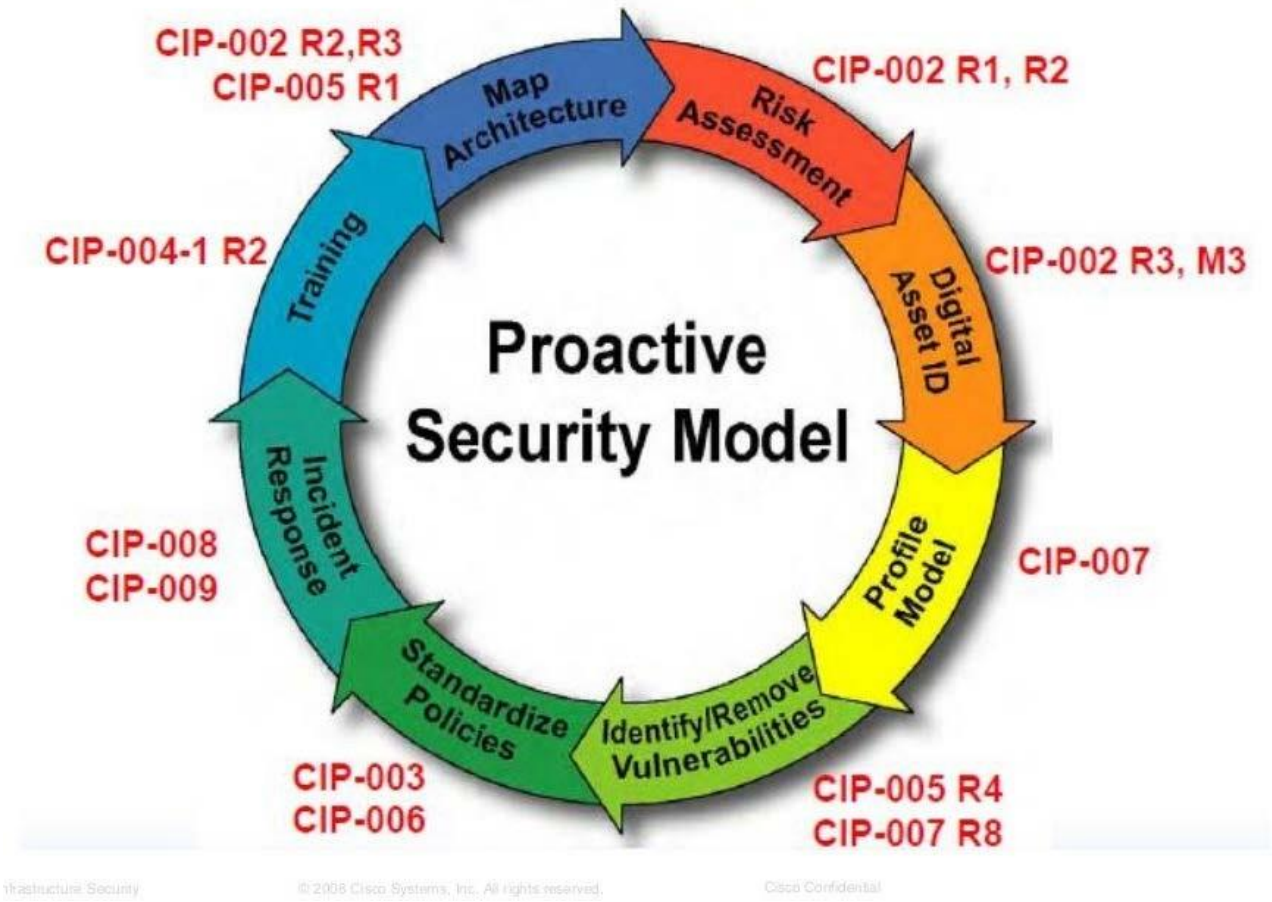
НАУКОВІ ГРАНІ ПРОБЛЕМИ ЗАХИСТУ ОКІІ ПРИКЛАДИ КОНКРЕТНИХ НАУКОВО-ДОСЛІДНИХ РОБІТ (далі - НДР)

- «Розвиток наукових засад теорії інформаційної безпеки великих розподілених АСУ ТП електроенергетичних систем», № ДР: 0113U002051;
- «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики», № ДР: 0114U002361;
- «Методичні та нормативно-правові основи забезпечення кібернетичної безпеки функціонування енергетики України з урахуванням європейських вимог», № ДР: 0116U002970;
- «Розвиток наукових засад забезпечення інформаційної безпеки об’єктів критичної інфраструктури електроенергетичної галузі на основі методології системних досліджень», № ДР: 0117U005467;
- «Розробка методів оцінювання чутливості Об’єднаної енергосистеми України до кібернетичних впливів», № ДР: 0118U005320.

КРАЩІ СВІТОВІ ПРАКТИКИ З ЗАХИСТУ АСУ ТП

- ISA SP99
  - ISA-TR99.00.01-2004 – Security Technologies of Manufacturing and Control Systems
  - ISA-TR99.00.01-2004 – Integrating Electronic Security into the Manufacturing and Control System Environment
- NERC
- Guidance for Addressing Cyber Security in the Chemical Indastry
- NIST PCSRF Security Capabilities Profile for Industrial Control Systems
- NIST SP800-82 “Guide to Industrial Control Systems (ICS) Security”
- IEC 61784-4 “Profiles for secure communication in industrial networks”

КРАЩІ СВІТОВІ ПРАКТИКИ З ЗАХИСТУ АСУ ТП. РЕКОМЕНДАЦІЇ NERC CIP



БАЗОВІ РЕКОМЕНДАЦІЇ ЩОДО ПОЛІПШЕННЯ СТАНУ ОРГАНІЗАЦІЙНО-МЕТОДОЛОГІЧНИХ ПРОБЛЕМ

LAN

Повна локалізація елементів критичної інфраструктури. Всі робочі станції диспетчерів, на яких функціонують засоби телемеханіки (SCADA), повинні бути відокремлені від будь-яких зовнішніх незахищених мереж, особливо, Інтернет (сегментація мережі). Доцільним є створення відокремлених доменів, термінальних серверів і т.п.

USB

Налаштування політик безпеки з обмеженням підключення зовнішніх носіїв даних та забороною запуску користувачем всіх виконуваних файлів (.exe, .bat, .scr, бібліотек .dll і т.д.) або використанням “білих листів” (Application White Listings).

AV

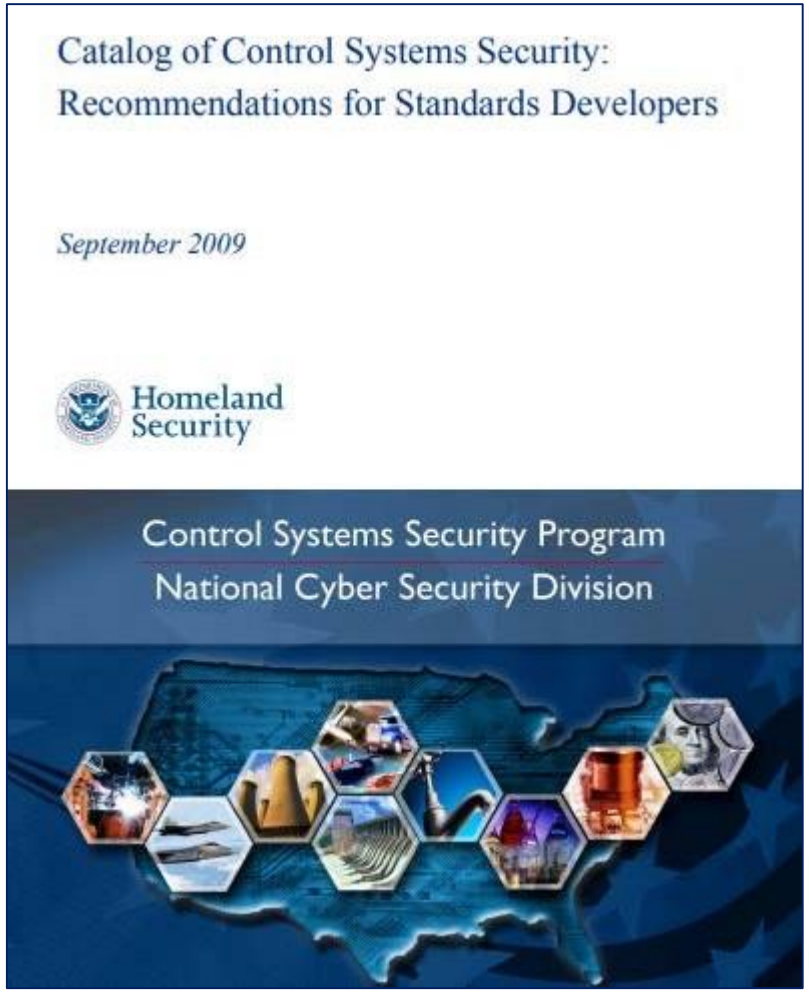
При виявленні будь-якої компрометуючої ознаки (після перевірки систем за yara-правилами, антивірусним скануванням і т.п.) – здійснювати перевстановлення операційної системи з перерозміткою дискового простору (напр., модуль Black Energy v3 дозволяє записувати зразки ШПЗ в загрузочний сектор диску, а в окремих випадках, “вшивати” в прошивку BIOS)

YARA

Завчасно оновлювати наявні в мережі yara-правила щодо основних загроз (напр., сайту з ics-cert.us-cert.gov або за посиланням github.com/Neo23x0/Loki/tree/master/signatures) та здійснювати відповідні сканування всіх елементів мережі.

МОДЕЛЬ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ АСУ ТП РОЗРОБКА ГАЛУЗЕВИХ СТАНДАРТІВ

- Спеціально для розробки галузевих стандартів існує набір рекомендацій, які повинні враховуватися при створенні власного переліку вимог з безпеки АСУ ТП .



НЕОБХІДНІ ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ ДОКУМЕНТИ

- Методика визначення актуальних загроз кіберзахисту в АСУ ТП
- Концепція розвитку організаційно-технічної моделі кіберзахисту
- Базова модель загроз кіберзахисту в АСУ ТП
- Рекомендації з забезпечення кіберзахисту в АСУ ТП
- Положення «Про аудит інформаційної безпеки на ОКІ»

ВИСНОВКИ

Незважаючи на всю різноманітність застосовуваних методів, в основі більшості імітаційних моделей лежить теорія графів. Крім того, широко використовуються знання теорії центрів тяжіння німецького військового теоретика і історика Клаузевіца і самоорганізованих мереж математика Альберто Барабаши, економіста міжгалузевого балансу Василя Леонтьєва, методи імітаційного моделювання, алгебри логіки, імовірнісної оцінки та ін. Подібний підхід дозволяє провести комплексний аналіз критичної інфраструктури з метою виявлення найбільш важливих її елементів, можливих вразливостей а також ризиків виведення цілих секторів з ладу.

ПЕРСПЕКТИВНІ НАПРЯМКИ ПОБУДОВИ ДЕРЖАВНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

- Організація та проведення регулярних семінарів обговорення з метою збільшення рівня освіченості та обміну досвідом.
- Створення лабораторії зі зразками АСУ ТП критичної інфраструктури для відпрацювання механізмів захисту.
- Організація та проведення навчань з кіберзахисту ОКІІ спеціалізованих підрозділів та співробвтників ОКІ.
- Організація НДР з захисту ОКІІ.
- Розробка галузевих стандартів з кіберзахисту АСУ ТП.
- Впровадження процедур обов’язкової оцінки ризиків на ОКІІ та звітування щодо результатів оцінки та плану впровадження заходів контролю.
- Розробка нових та модернізація існуючих нормативно-правових та нормативно-технічних документів.
- Впровадження кращих світових практик з кіберзахисту ОКІІ як в технічному так і організаційному напрямках.

ДЯКУЮ ЗА УВАГУ!

dckz_hmm@dsszzi.gov.ua
ckz_dav@dsszzi.gov.ua