Засідання МЕРГ на тему

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЗАБЕЗПЕЧЕННЯ ВЗАЄМОДІЇ НАЦІОНАЛЬНИХ/ДЕРЖАВНИХ СИСТЕМ БЕЗПЕКИ ТА КРИЗОВОГО РЕАГУВАННЯ

26 червня 2018 року

Захист КІ та проблеми взаємодії національних/державних систем безпеки та кризового реагування

Кондратов Сергій Іванович

kondratov@niss.gov.ua

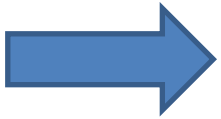
ЗРОСТАННЯ УРАЗЛИВОСТІ КІ

- Тенденції до загострення загроз:
  - Тероризму, екстремізму, сепаратизму
  - НС техногенного та природного характеру
  - Кіберзагроз на тлі
- Под-шого ускладнення і розгалуження взаємозв‘язків у сфері забезпечення життєдіяльності держави
- В результаті – зростання уразливості КІ

Важливість визначення терміну КІ

- Термін «КІ» обумовлює, зокрема:
  - Критерії віднесення до КІ (кількість ел-тів, масштаб. і часові рамки впливу);
  - Напрями захисту та розподіл відп-сті;
  - Усвідомлення: ЗКІ потребує зусиль усього сусп-ва, усієї держави:
  - Значення **КДВОІ,** особливо для компл. загроз і криз

Реакція розвинутих країн

- Системність:  **Створення** держ. систем ЗКІ (**ДСЗКІ**) для захисту від **фізичних** (прир., техн., зловм. дій) та **кіберзагроз + Уповн. орган**
- **КІ ≠ ∑** інфраструктурних об‘єктів,
- **КІ ≠ ∑** стратегічно важл., небезп., тих що підлягають охороні і т.д. об‘єктів
- США: тисячі; Польща: сотні елем-тів КІ

Ситуація в Україні

- Низка держ./національних систем
- > 10 переліків та списків (*особливо важливі, важливі, потенційно небезпечні, об'єкти держ. власності, що мають стратегічне значення для економіки і безпеки держави, що підлягають обов‘язковій охороні, ядерні об'єкти тощо)*
- Вплив на КДВОІ відомчих підходів

Вплив відомчих підходів

- КДВОІ **між системами** часто має лише формальний характер:
  - *кожна система має «власні» загрози та ризики, терміни, підходи, режими/умови функціонування*
  - *у рамках систем відсутня мотивація для міжсистемної взаємодії, якого потребує ЗКІ*
- Домінування відомчих підходів гальмує запровадження конц. ЗКІ

Опитування ключових відомств 1

- НІСД опитав ряд відомств щодо КДВОІ при реагуванні на комплексні загрози
  - ДІЯРУ: врегульовані чинними НПА
  - ДСНС: врегульовані Кодексом ЦЗ
  - АТЦ: вирішуються в залежності від встановлених рівнів тер. загроз; терміни «КІ», захист КІ відсутні у НПА, питаннями КІ займ. інш. підр.
  - ДЦКЗ: розроблено проект Протоколу (у процесі узгодження)

Опитування ключових відомств

- Серйозний прогрес за напрямом кіберзахисту
- Термін «КІ» визначений у ПКМУ за цим напрямом (ЗКІ «гальмує» КЗ)
- Інші відомства проявляють значну «обережність» до створення ДСЗКІ
- Неприпустимість необережного механічного переносу зарубіжного досвіду
- Ключове положення Концепції

Чи здатні існуючі системи ефективно взаємодіяти?

- У сфері нац. безпеки і оборони взагалі відсутній термін «***interoperability***»
- Розглянемо приклад 3-х систем
  - ЄДСЦЗ / ПКМУ від 09.01.2014 р. № 11.
  - ДСФЗ / ПКМУ від 21.12.2011 №1337.
  - ЄСЗРПТА ПКМУ від 18.02.2016 № 92

Чи здатні існуючі системи ефективно взаємодіяти?

У сфері нац. безпеки і оборони України взагалі відсутній термін «***interoperability***»

Таблиця. Параметри функціонування деяких систем безпеки та кризового реагування

ЄДСЦЗ ***режими*** функціонування	ДСФЗ ***умови*** функціонування	ЄСЗРПТА ***рівні*** терористичних загроз
режим повсякденного функціонування	нормальне функціонування	
		сірий (можлива загроза) за наявності факторів (умов), що сприяють вчиненню терористичного акту
підвищена готовність	підвищена готовність	
		синій (потенційна загроза) за наявності інформації, що потребує підтвердження, про підготовку до вчинення терористичного акту
надзвичайна ситуація	функціонування у кризовій ситуації	
		жовтий (імовірна загроза) за наявності достовірної (підтвердженої) інформації про підготовку до вчинення терористичного акту
надзвичайний стан		
		червоний (реальна загроза) у разі вчинення терористичного акту
	відновлення нормального функціонування	

Відмінності в параметрах функціонування систем

- Урегульованість КДВОІ = узгодженість осн. параметрів функціонування
- Повний збіг лише для перших 2-х режимів/умов СДСЦЗ та ДСФЗ
- ЄДСЦЗ: відсутн. ліквідації насл.; ДСФЗ: відновлення функц., ЄСЗРПТА – відсутн. рівень, що відповід. норм. функц. а червон. лише після т/акту

ПРИКЛАД 1

- Гіпотет-ний випадок: Надійшла підтвердж. інфо про загрозу т/акту на АЕС
- Відповідно до НПА:
  - ДСФЗ: функц-ня у кризовій ситуації
  - ЄДСЦЗ: режим повсякденного функц.
  - ЄСЗРПТА: жовтий рівень
- А як у реальній ситуації?

ПРИКЛАД 2. Державний план взаємодії1

- Державний план взаємодії…на випадок вчинення диверсії щодо ЯУ, ЯМ, ДІВ… а також р/а відходів…
  - Жодного разу не перевірявся
  - Термін-чна плутанина: «диверсія» при відсутності у НПА «ядерного» та «радіаційного» тероризму
  - Інформування вищого політ. кер-ва (формат, часові рамки, відп-сть)

ПРИКЛАД 2. Державний план взаємодії2

- Відсутні положення:
  - щодо кіберзагроз та інформаційних загроз
  - щодо ДПП, взаємодії з НУО (волонтери), ЗМІ, експертн. співтов.
  - інформування вищого політ. кер-ва (формат, часові рамки, відп-сть)
  - щодо залуч. сил і засобів МО у випадку тер. атак на ЯО
- Неконкретність в умовах обмеж. часу

2 ПРИКЛАДИ: Тренування ДСНС та хакерська атака на сайт Міненерговугілля

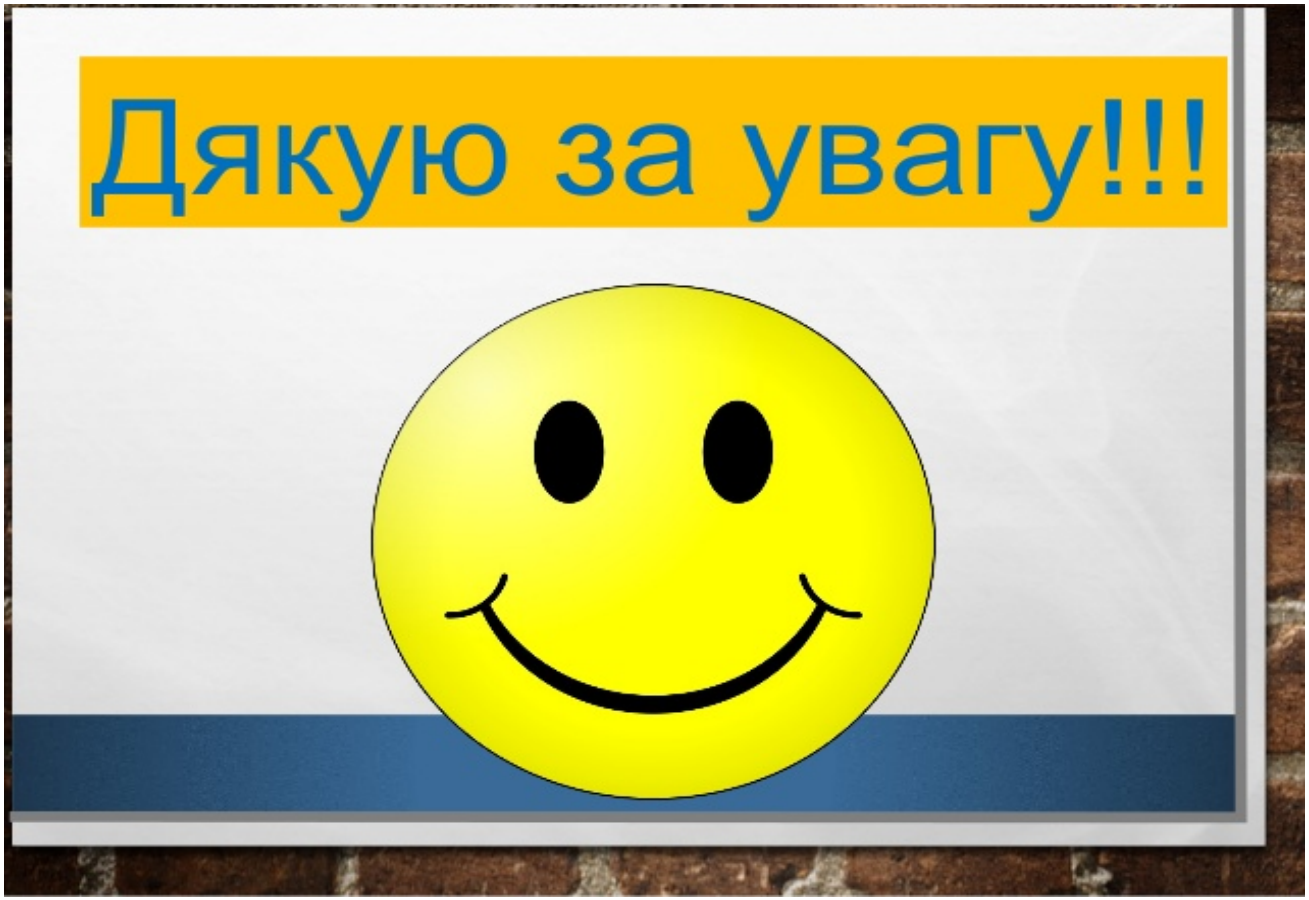
- Спрощена процедура реагування на комплексну загрозу («кейс з їдкою речовиною на площі» – ймовірна загроза т/акту)
- Атака на сайт Міненерговугілля, Кіберполіція обіцяє допомогу лише при офіційному запиті мін-ва

ВИСНОВКИ

- Необхідність створення ДСЗКІ зумовлена 3-ма основними прич-ми:
  - зростанням загроз КІ в суч. умовах та неефективністю заходів у рамках існуюч. систем
  - заявленим курсом України
  - прийнятим політичним рішенням.

РЕКОМЕНДАЦІЇ

- Максимально використовувати зарубіжний передовий досвід щодо
  - визначення терміну КІ
  - кола загроз, проти яких має діяти ДСЗКІ
  - організаційно-правових підходів до створення ДСЗКІ, забезпечення належного рівня КДВОІ


Дякую за увагу!!!