ОБСЄ Організація з безпеки та співробітництва в Європі

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

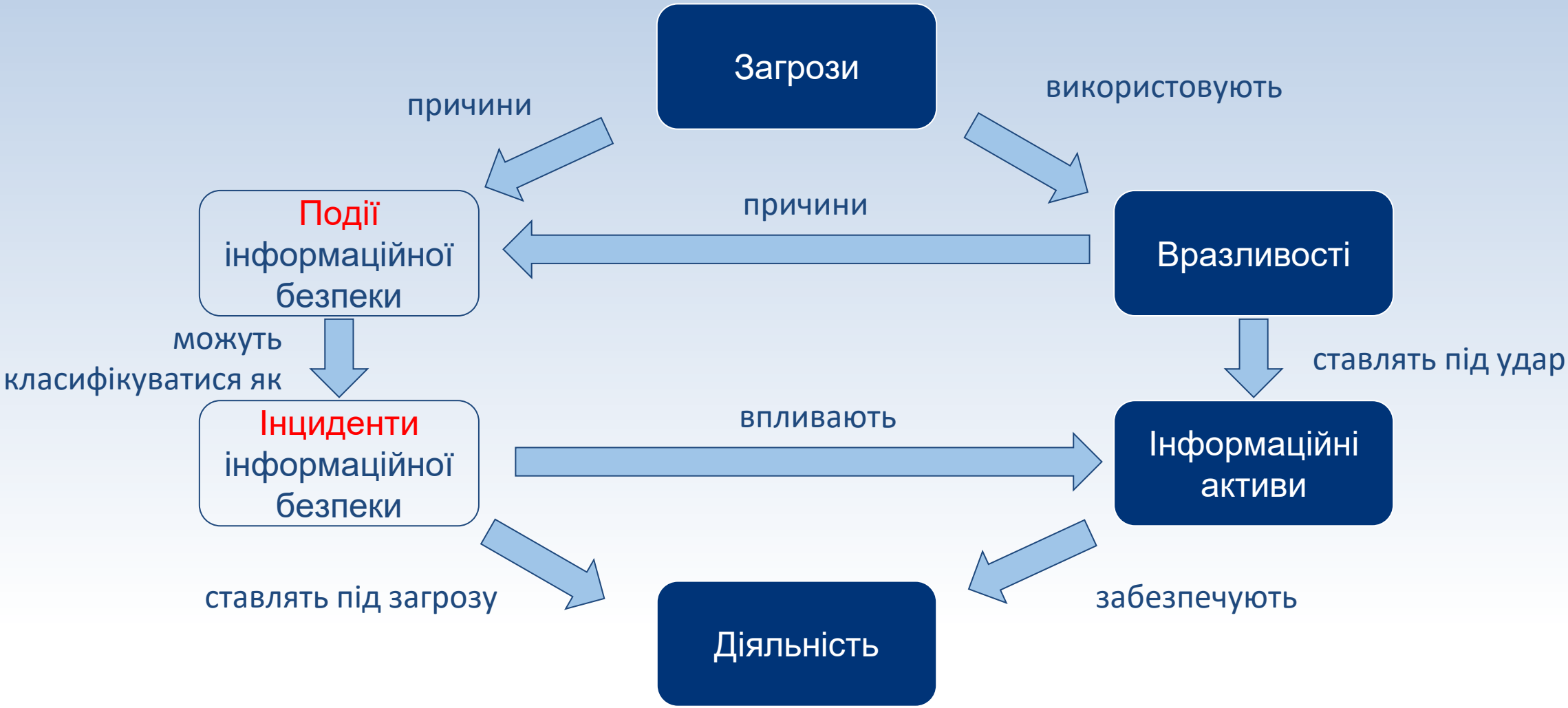
ОСНОВИ КІБЕРГІГІЄНИ

Реагування на інциденти безпеки інформації

Цілі

- визначення ролі користувача у реагуванні на інциденти інформаційної безпеки організації
- виявлення провісників інциденту інформаційної безпеки
- виявлення індикаторів інциденту інформаційної безпеки

Події та інциденти інформаційної безпеки



ОБСЄ Організація з безпеки та співробітництва в Європі

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Заходи управління інцидентами

визначення

відповідальності керівництва організації

процедур реагування на інциденти інформаційної безпеки

ОБСЄ Організація з безпеки та співробітництва в Європі

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Заходи управління інцидентами

звітування щодо

подій інформаційної безпеки

виявлених недоліків та вразливостей системи інформаційної безпеки

ОБСЄ Організація з безпеки та співробітництва в Європі

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Заходи управління інцидентами

оцінка подій інформаційної безпеки

прийняття рішень щодо віднесення їх до інцидентів інформаційної безпеки

ОБСЄ Організація з безпеки та співробітництва в Європі

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Заходи управління інцидентами

- реагування на інциденти інформаційної безпеки відповідно до встановлених процедур

Заходи управління інцидентами

- ідентифікація, збирання, отримання і зберігання доказів для притягнення винних до різних видів юридичної відповідальності

Заходи управління інцидентами

- аналіз і зіставлення інцидентів інформаційної безпеки для покращення безпеки СУІБ

ОБСЄ Організація з безпеки та співробітництва в Європі

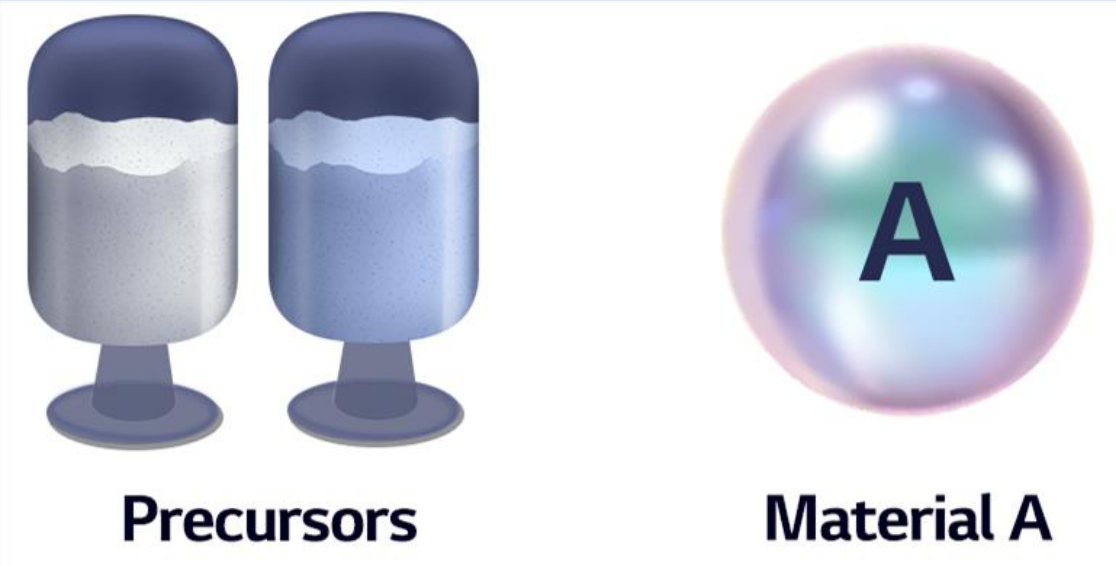
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Як виявляти події та інциденти?

- Автоматизовані засоби виявлення
  - системи виявлення вторгнень
  - антивірусне програмне забезпечення
  - аналізатори журналів подій
- Повідомлення користувачів за визначеною процедурою

Ознаки інциденту

- провісники (precursors)
- індикатори (indicators)



Організація з безпеки та співробітництва в Європі

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Провісники

- записи журналу вебсервера
- анонс на спеціалізованих ресурсах нового експлойту
- погрози здійснити атаку
- ….

Індикатори

- сповіщення IDS
- сповіщення антивірусу
- ім'я файлу з незвичними символами
- зареєстровано кілька невдалих спроб входу
- ……

Звіт про події інформаційної безпеки

ЗВІТ ПРО ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ			
1. Дата події		3. Ідентифікаційні номери відповідної події та/або інциденту (якщо застосовне)	
2. Номер події (надається фахівцем ISIRT)			
4. РЕКВІЗИТИ ОСОБИ, ЩО ЗВІТУЄ			
4.1 Ім'я та прізвище		4.2 Адреса	
4.3 Організація		4.4 Відділ	
4.5 Телефон		4.6 E-male	
5. ОПИС ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ			
5.1 Опис події: · Що сталося. · Яким чином сталося. · Чому так сталося. · Які компоненти/активи піддались впливу. · Оцінка впливу на діяльність організації. · Будь-які виявлені вразливості			
6. ДЕТАЛІ ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ			
6.1 Дата та час події			
6.2 Дата та час виявлення події			
6.3 Дата та час повідомлення про подію			
6.4 Чи відповідь на цю подію усунула небезпеку?		ТАК ☐ НІ ☐ (позначте відповідне)	
6.5 Якщо так. вкажіть, скільки часу тривала подія (у днях/годинах/хвилинах)			

ОБСЄ Організація з безпеки та співробітництва в Європі

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Виявлення провісників

- Налаштувати ведення та забезпечення доступу до журналу подій Windows Defender Firewall.
- Встановити Nmap Security Scanner та здійснити сканування системи, яке розглядається як підготовка до атаки.
- Виявити провісники атаки та заповнити звіт щодо події інформаційної безпеки.

Керівництво з виконання

Відео виконання

ОБСЄ Організація з безпеки та співробітництва в Європі

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Виявлення індикаторів

- Налаштувати аудит входу користувача в систему.
- Ввести декілька раз неправильний пароль при вході до ОС Windows.
- Виявити індикатори інциденту інформаційної безпеки та заповнити звіт щодо події інформаційної безпеки.

Керівництво з виконання

Відео виконання

ОБСЄ Організація з безпеки та співробітництва в Європі

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Підсумки

- визначили роль користувача у реагування на інциденти інформаційної безпеки
- у контексті реагування на інциденти інформаційної безпеки навчилися виявляти:
  - провісники
  - індикатори