ДЛЯ ЧОГО НАМ ПОТРІБНІ ЦЕНТРИ ОБМІНУ ТА АНАЛІЗУ ІНФОРМАЦІЇ (ISAC)

Підготував Іван Гокін, CISA
21 серпня 2023 року

СПИТАЙТЕ СЕБЕ…

Кобзар та зацікавлені споживачі інформації

- Вашій організації бракує ситуаційної обізнаності щодо загроз кібербезпеки?
- Постачальники CTI надають нерелевантну для Вашої організації інформацію?
- Не можете змоделювати кіберзагрози для вашої галузі?
- Хочете розуміти які вразливості пріоритетніші у виправленні?
- Винаймати розвідника кіберзагроз – занадто дорого і складно?
- Хочете отримувати максимум зі своїх інвестицій в розвідку кіберзагроз?

- Відповідь є: долучайтеся до ISAC!

ВСТУП

ISAC – це…	центри обміну та аналізу інформації (ISAC), що допомагають власникам і операторам критичної інфраструктури захищати свої об'єкти, персонал і клієнтів від кібер і фізичних загроз безпеки та інших небезпек. ISAC збирають, аналізують і поширюють дієву інформацію про загрози своїм членам і надають членам інструменти для зниження ризиків і підвищення стійкості.

(c) US National Council of ISACs

Послуги ISAC	Обмін інформацією про загрози та ризики
	Аналіз інформації про загрози та ризики
	Надання рекомендацій щодо захисту від загроз та ризиків
	Надання навчання з питань безпеки
	Організація спільних заходів реагування на інциденти

ПЕРЕВАГИ ISAC

Довірена спільнота

ISAC — це спільнота, яка об'єднує операторів галузі з однаковими цілями та інтересами, створюючи надійний простір.

Найкращі практики

ISAC є інструментами для обміну хорошими практиками, інформацією про загрози кібербезпеки та щодо протидії ним.

Обізнаність у сфері кібербезпеки

ISAC підвищує рівень ситуаційної обізнаності в критичних секторах.

Підтримка законодавства

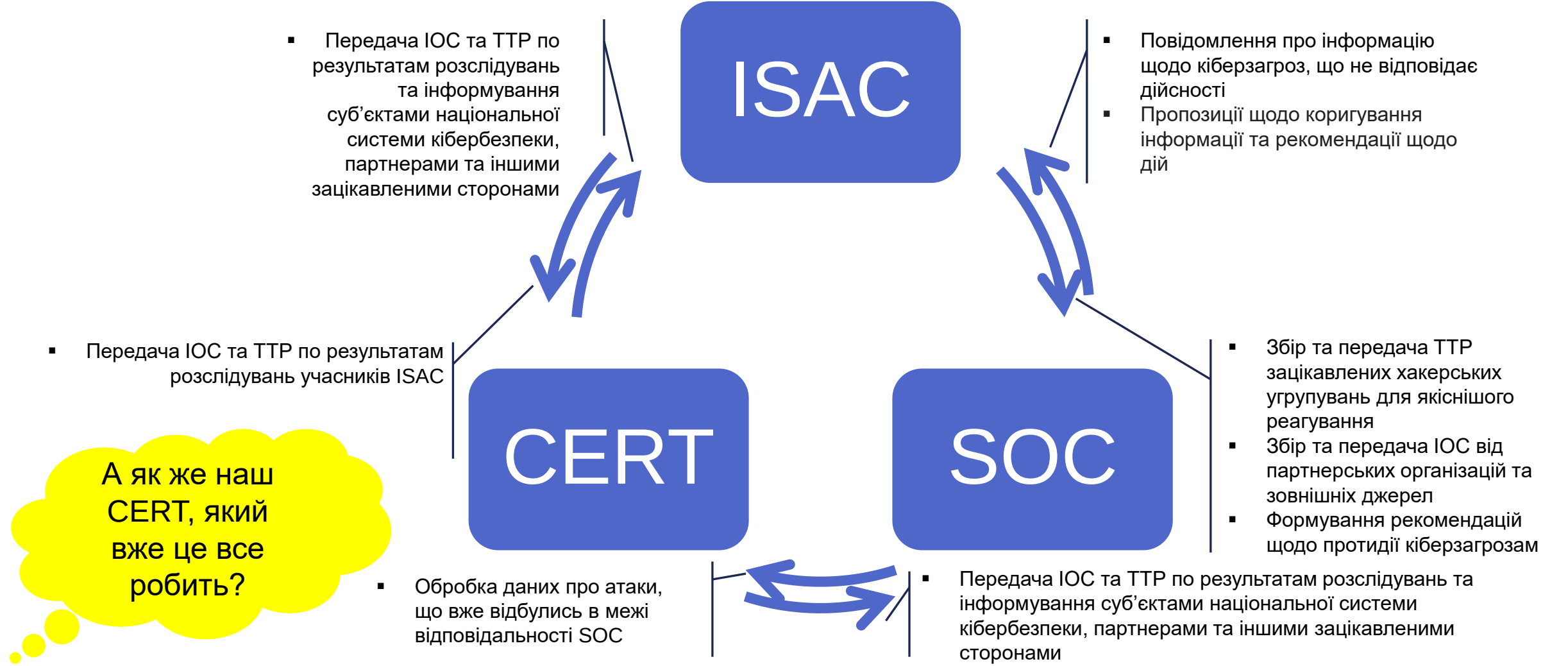
ISAC можуть підтримувати впровадження вимог законодавства.

Кризовий менеджмент

ISAC можна використовувати як механізми обміну інформацією у випадку кризи або інцидентів на рівні галузі.

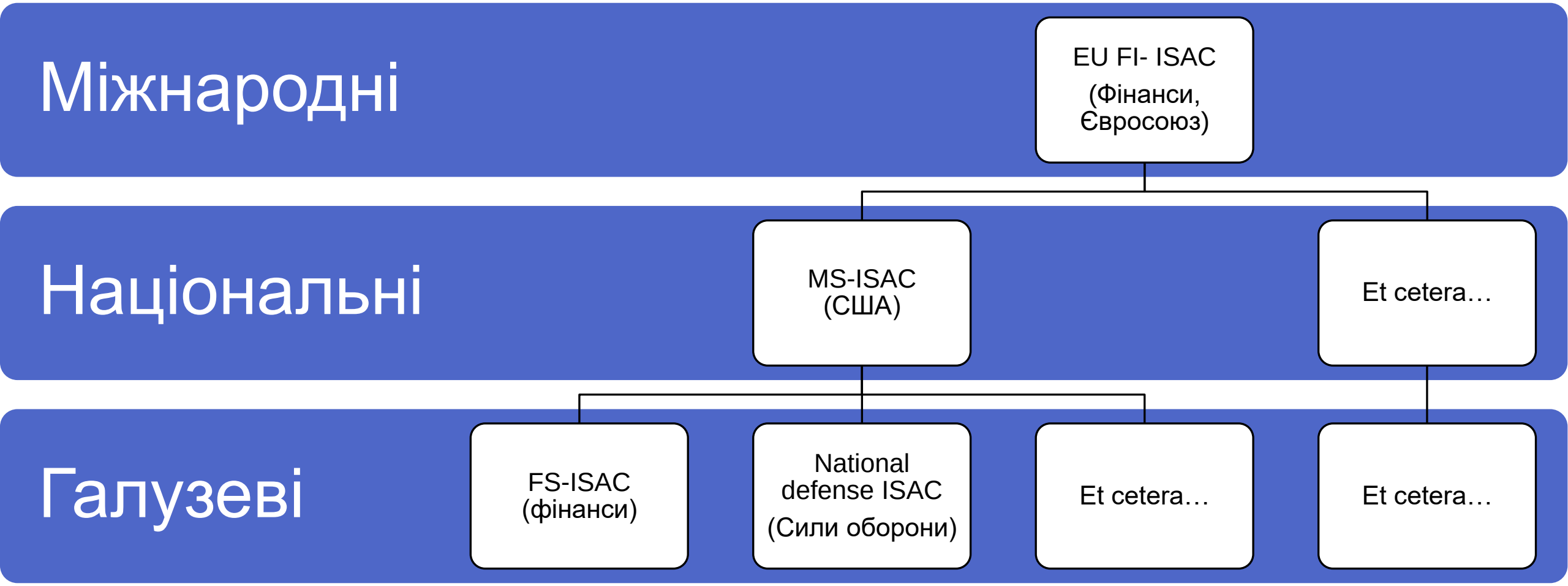
(c) ENISA

Приклади ISAC



«ЗАЛІЗНИЙ» ТРИКУТНИК КІБЕРБЕЗПЕКИ

Адаптовано з джерела: https://cms.aaasec.com.tw/index.php/2018/06/15/0010/

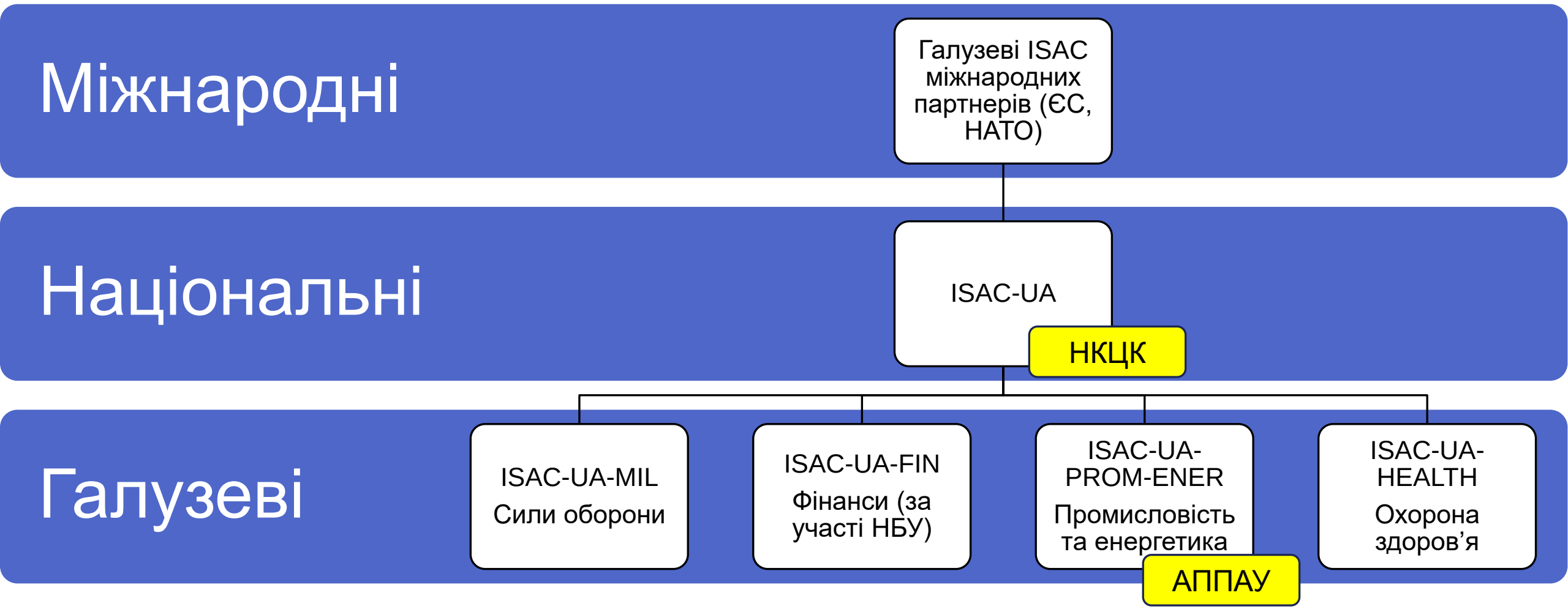


ОСНОВНІ ТИПИ ISAC

Типи ISAC детальніше розглянуті в додатках 1-3.

ЯК СТАТИ ЧЛЕНОМ ISAC

ЩО РОБИТИ ЯКЩО ДЛЯ ВАС НЕМАЄ ВІДПОВІДНОГО ISAC?



МОЖЛИВА СТРУКТУРА ISACІВ В УКРАЇНІ

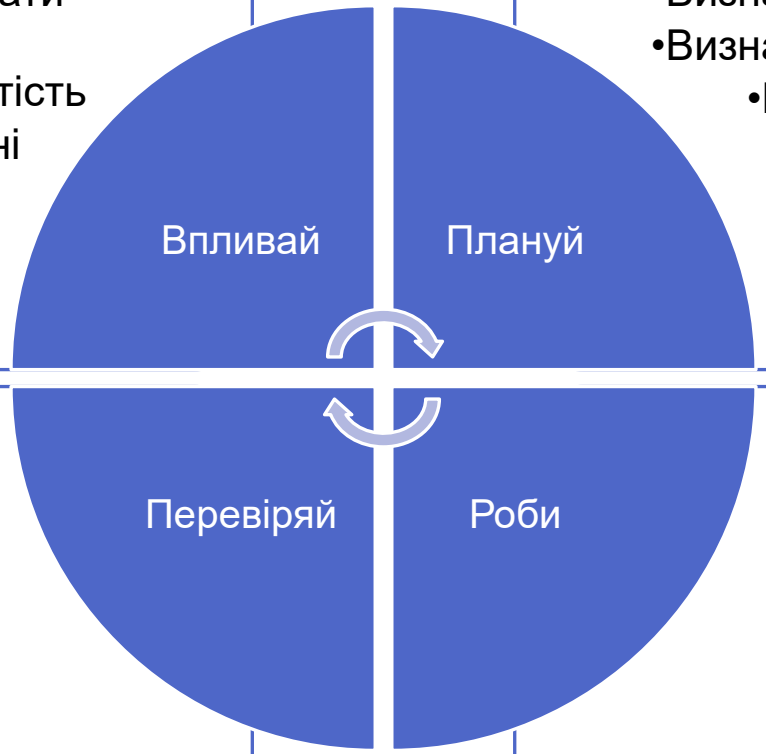
Легенда

Запропонований ISAC

Наявний прообраз ISAC

ТРЕБА СТВОРИТИ СВІЙ ВЛАСНИЙ ISAC

Як це зробити?



- Розробляти та покращувати наявні послуги
- Збільшувати додану вартість
- Залучати нові зацікавлені сторони

- Визначати цілі та призначення ISAC
- Визначати обсяг допустимої роботи
- Визначати вимоги до учасників
- Визначати структуру управління
- Визначати формат та правила обміну інформацією та комунікації
- Визначати порядок фінансування

- Отримувати зворотній зв’язок
- Оцінювати вплив ISAC

- Розбудовувати спроможності
- Розбудовувати довіру
- Проводити зустрічі
- Управляти згідно вимог

Джерело: ENISA ISAC toolbox

Детальна інструкція за посиланням

ВАЖЛИВО ПАМ’ЯТАТИ

	ISAC	**Галузева асоціація**
Цільова аудиторія	Фахівці з кібербезпеки, CISO	Галузеві фахівці, вище керівництво
Зона відповідальності	Обмін та аналіз інформації про кіберзагрози	Розвиток галузі

Q&A

ОСНОВНІ ДЖЕРЕЛА

- ENISA: Information Sharing and Analysis Center (ISACs) - Cooperative models
- ENISA: ISACs Toolbox
- Національний інститут стратегічних досліджень (НІСД): Аналітична доповідь "Державно-приватне партнерство у сфері кібербезпеки та можливості для України"
- National Council of ISACs (США)

Типи організацій-членів ISAC

- ► Служби кібербезпеки
- ► Національні компетентні органи
- > Правоохоронні органи
- > Національні органи розвідки
- ► Приватні виробники продуктів
- ► Приватні постачальники послуг

Структура управління

- > Ролі управління
- > Ролі підтримки
- > Без структури

Галузі

- ►Паливно-енергетичний сектор
- > Цифрові технології
- > Захист інформації
- > Системи життєзабезпечення
- > Харчова промисловість та агропромисловий комплекс
- > Державний матеріальний резерв
- > Охорона здоров'я
- > Ринки капіталу та організовані товарні ринки
- ► Фінансовий сектор
- ► Транспорт і пошта
- > Промисловість
- > Сектор громадської безпеки
- > Цивільний захист населення і територій
- > Міграція (імміграція та еміграція)
- > Охорона навколишнього природного середовища
- > Сектор оборони
- > Національна безпека
- > Правосуддя
- > Тримання під вартою
- > Наукові дослідження та розробки
- > Вибори та референдуми
- > Соціальний захист
- > Інформаційні послуги
- > Державна влада та місцеве самоврядування

Джерело: Перелік секторів критичної інфраструктури Постанова Кабінету Міністрів України від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури»

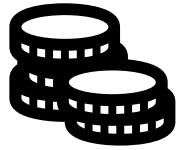
Стиль та засоби співпраці

- ► Регулярні зустрічі
- ► Робочі групи
- ► Конференції та
- ► Веб портали / платформи
- ► Електронна пошта та телеконференції

Розвиток спроможностей

- ► Аналіз вразливостей та загроз
- > Навчання та відпрацювання вправ
- > Аналіз трендів

Варіанти фінансування



- > Субсидії уряду
- ► Обов'язкові внески
- ► Добровольчі внески

ДОДАТОК 1. МІЖНАРОДНИЙ ISAC

Легенда
►В обсязі роботи ISAC
> Поза обсягом роботи ISAC

Джерело: ENISA: Information Sharing and Analysis Center (ISACs) - Cooperative models

Типи організацій-членів ISAC

- ► Служби кібербезпеки
- ► CERT / CSIRT
- > Національні компетентні органи
- > Правоохоронні органи
- > Національні органи розвідки
- > Приватні виробники продуктів
- > Приватні постачальники послуг

Структура управління

- > Ролі управління
- > Ролі підтримки
- ► Без структури

Галузі

- ►Паливно-енергетичний сектор
- ►Цифрові технології
- ►Захист інформації
- ►Системи життєзабезпечення
- ►Харчова промисловість та агропромисловий комплекс
- ►Державний матеріальний резерв
- ►Охорона здоров'я
- ►Ринки капіталу та організовані товарні ринки
- ►Фінансовий сектор
- ►Транспорт і пошта
- ►Промисловість
- ►Сектор громадської безпеки
- ►Цивільний захист населення і територій
- ►Міграція (імміграція та еміграція)
- ►Охорона навколишнього природного середовища
- ►Сектор оборони
- ►Національна безпека
- ►Правосуддя
- ►Тримання під вартою
- ►Наукові дослідження та розробки
- ►Вибори та референдуми
- ►Соціальний захист
- ►Інформаційні послуги
- ►Державна влада та місцеве самоврядування

Джерело: Перелік секторів критичної інфраструктури Постанова Кабінету Міністрів України від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури»

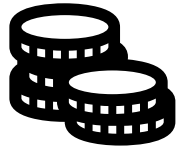
Стиль та засоби співпраці

- ► Регулярні зустрічі
- ► Робочі групи
- ► Конференції та
- ► Веб портали / платформи
- ► Електронна пошта та телеконференції

Розвиток спроможностей

- > Аналіз вразливостей та загроз
- > Навчання та відпрацювання вправ
- > Аналіз трендів

Варіанти фінансування



- ► Субсидії уряду
- ► Обов'язкові внески
- > Добровольчі внески

ДОДАТОК 2. НАЦІОНАЛЬНИЙ ISAC

Легенда
►В обсязі роботи ISAC
> Поза обсягом роботи ISAC

Джерело: ENISA: Information Sharing and Analysis Center (ISACs) - Cooperative models

Типи організацій-членів ISAC

- ▶ Служби кібербезпеки
- > Національні компетентні органи
- ▶ Правоохоронні органи
- ▶ Національні органи розвідки
- > Приватні виробники продуктів
- ▶ Приватні постачальники послуг

Структура управління

- ▶ Ролі управління
- ▶ Ролі підтримки
- > Без структури

Галузі

- ▶ Паливно-енергетичний сектор
- ▶ Цифрові технології
- ▶ Захист інформації
- ▶ Системи життєзабезпечення
- ▶ Харчова промисловість та агропромисловий комплекс
- ▶ Державний матеріальний резерв
- ▶ Охорона здоров'я
- ▶ Ринки капіталу та організовані товарні ринки
- ▶ Фінансовий сектор
- ▶ Транспорт і пошта
- ▶ Промисловість
- ▶ Сектор громадської безпеки
- ▶ Цивільний захист населення і територій
- ▶ Міграція (імміграція та еміграція)
- ▶ Охорона навколишнього природного середовища
- ▶ Сектор оборони
- ▶ Національна безпека
- ▶ Правосуддя
- ▶ Тримання під вартою
- ▶ Наукові дослідження та розробки
- ▶ Вибори та референдуми
- ▶ Соціальний захист
- ▶ Інформаційні послуги
- ▶ Державна влада та місцеве самоврядування

Джерело: Перелік секторів критичної інфраструктури
Постанова Кабінету Міністрів України від 09.10.2020 № 1109
«Деякі питання об'єктів критичної інфраструктури»

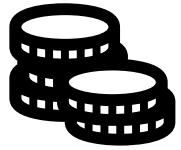
Стиль та засоби співпраці

- ▶ Регулярні зустрічі
- ▶ Робочі групи
- ▶ Конференції та
- ▶ Веб портали / платформи
- ▶ Електронна пошта та телеконференції

Розвиток спроможностей

- > Аналіз вразливостей та загроз
- > Навчання та відпрацювання вправ
- ▶ Аналіз трендів

Варіанти фінансування



- > Субсидії уряду
- ▶ Обов'язкові внески
- ▶ Добровольчі внески

ДОДАТОК 3. ГАЛУЗЕВИЙ ISAC

Легенда
▶ В обсязі роботи ISAC
> Поза обсягом роботи ISAC

Джерело: ENISA: Information Sharing and Analysis Center (ISACs) - Cooperative models