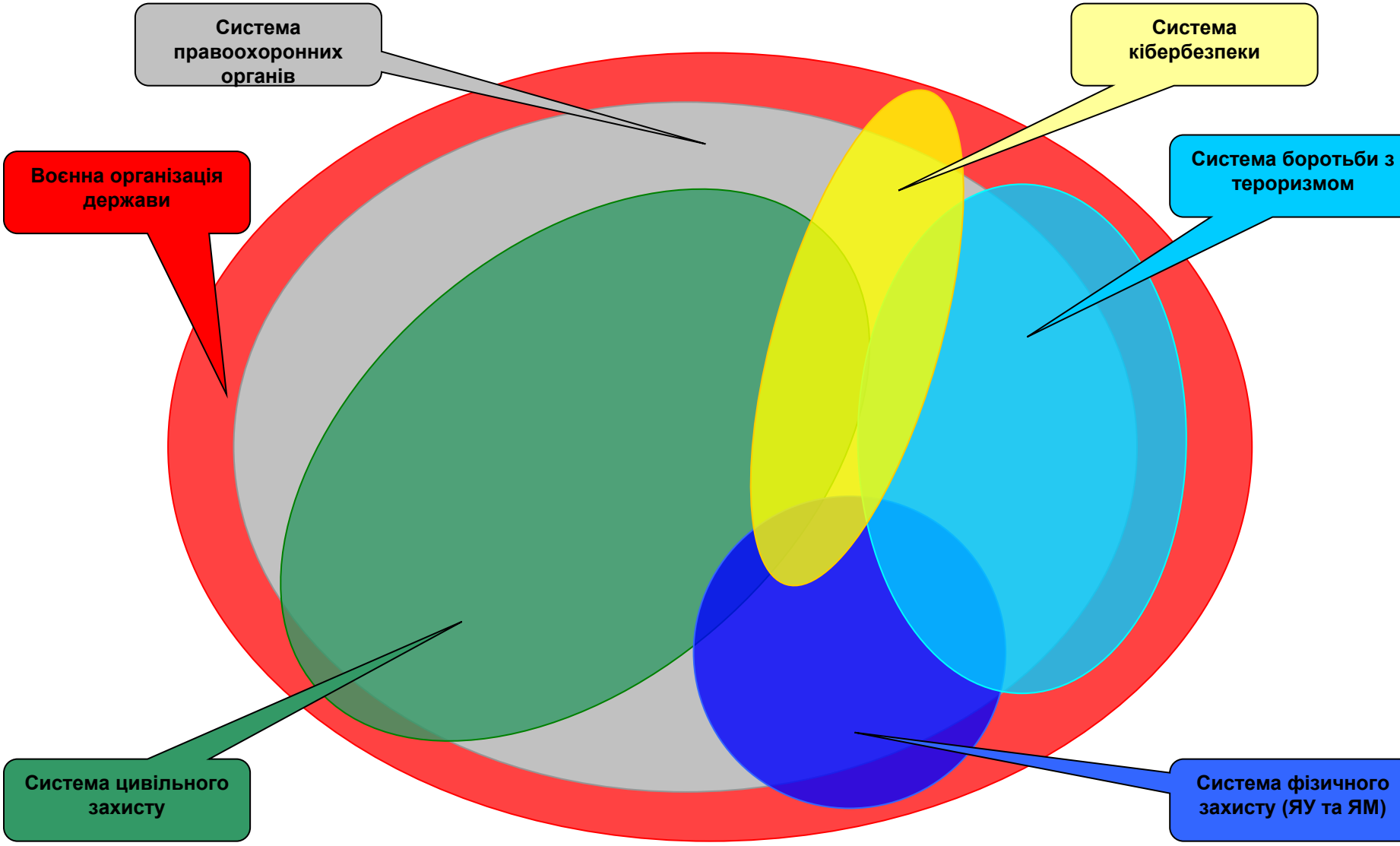
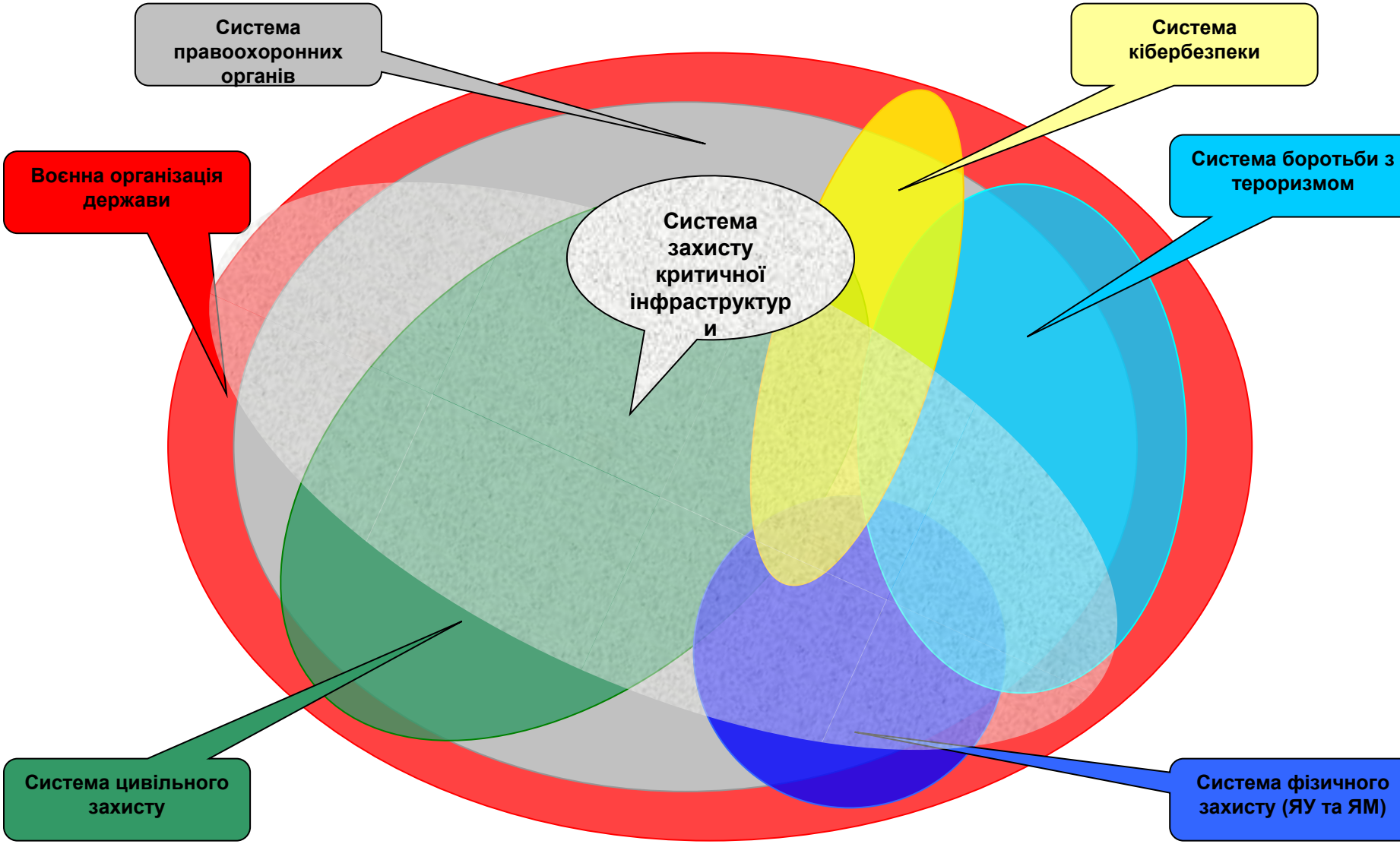
Проектна загроза та паспорти безпеки як ключові елементи системи захисту критичної інфраструктури

Бобро Дмитро
Провідний науковий співробітник
Відділ енергетичної та техногенної безпеки НІСД

Державні системи захисту



Державні системи захисту



Проблеми забезпечення стійкості критичної інфраструктури.

У нас узкая специализация…

К пуговицам претензии есть???

https://www.youtube.com/watch?v=Zlig5fgp7nY

https://www.youtube.com/watch?v=2wxL3DYen5g

Система цивільного захисту:

Закон України “Про об'єкти підвищеної небезпеки”

“ПОЛОЖЕННЯ про паспортизацію потенційно небезпечних об'єктів”

“РЕГЛАМЕНТ моніторингу потенційно небезпечних об’єктів”

Форми паспортів ПНО

Атомна енергетика:

Аналіз безпеки: Вимоги до структури та змісту Звіту з аналізу безпеки енергоблоків АЕС з реакторами з водою під тиском

Аварійні плани **Плани взаємодії на випадок диверсії**

Система фізичного захисту - фізичної ядерної безпеки:

Порядок проведення оцінки вразливості ядерних установок та ядерних матеріалів

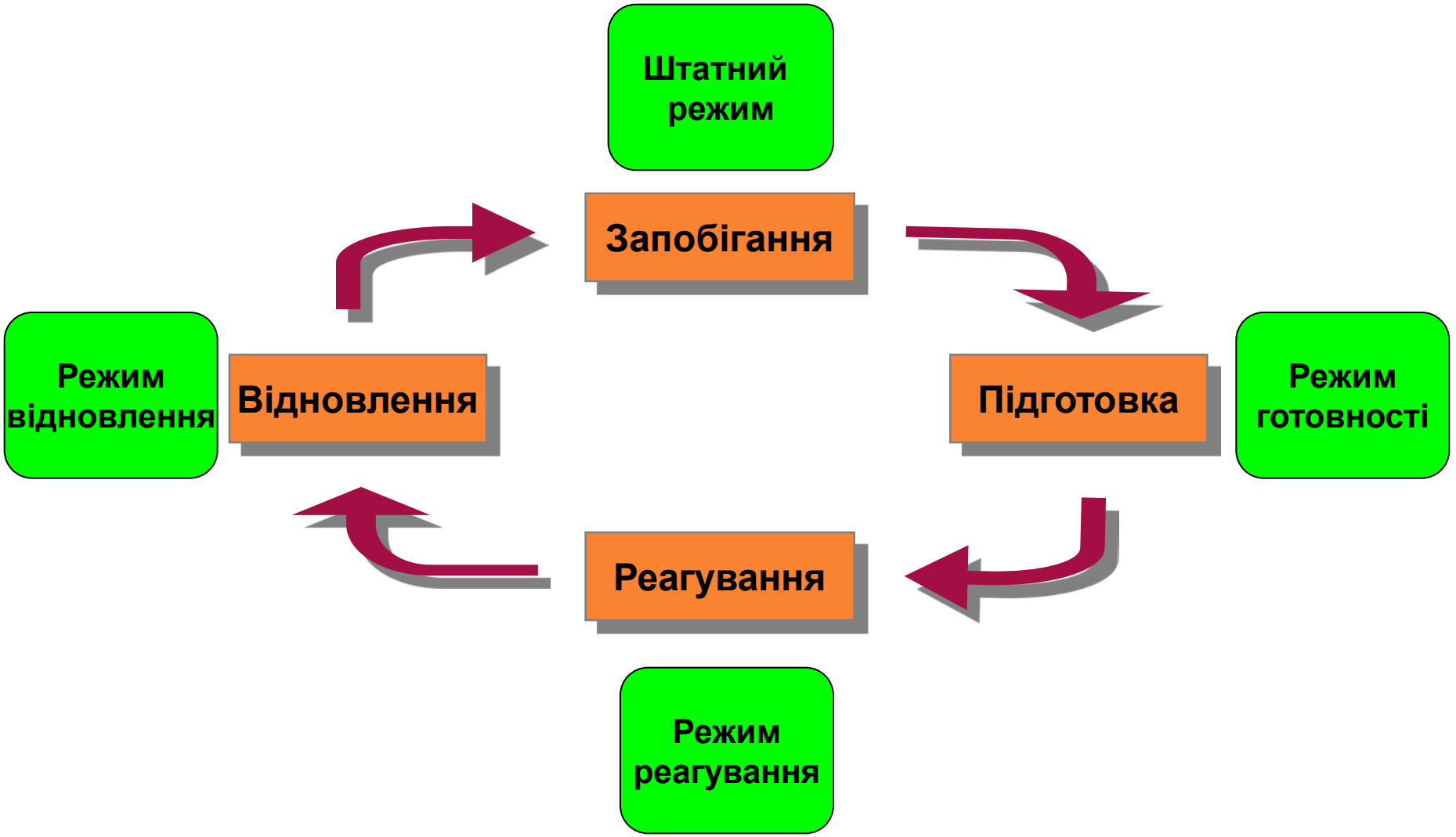
Система боротьби з тероризмом:

Проект Положення про порядок віднесення об'єктів до терористично вразливих

Проблеми забезпечення стійкості критичної інфраструктури.

- **Ключові поняття та терміни:**
  - **Критична інфраструктура**
  - **Безпека, захист, стійкість**
  - **Загрози, вразливість, ризик**
  - **Категоризація та паспортизація (рівень критичності та паспорт безпеки ОКІ)**
  - **Режим функціонування**
- **Методологія**
  - **Ризик-орієнтований підхід**
  - **Модель загроз**
  - **Паспорт безпеки**
- **Планування**
  - **Відповідність управлінському циклу**

Забезпечення стійкості – режими функціонування системи



Проблеми забезпечення стійкості критичної інфраструктури.

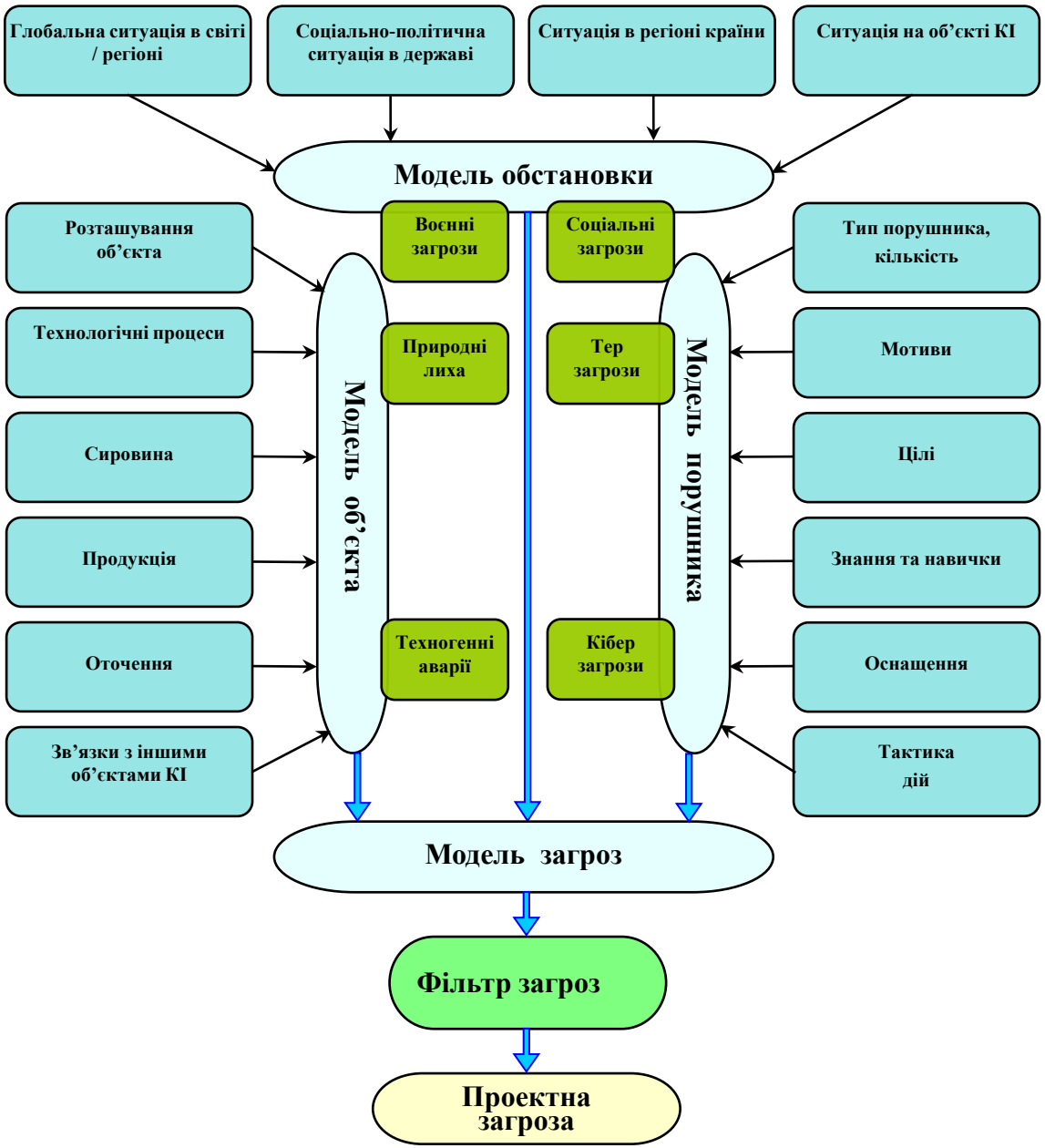
Яким же чином забезпечити захист КІ від загроз усіх типів?

1) В першу чергу потрібно визначитися, ***що саме потребує захисту*** – потрібно ідентифікувати об'єкти/системи/ресурси, які надають життєво важливі для безпеки людини, суспільства і держави послуги та функції.
2) По-друге, потрібно визначитися ***від чого потрібно захищати КІ*** – потрібно на національному рівні визначитися з переліком загроз критичній інфраструктурі усіх типів – опрацювати «Проектну загрозу критичній інфраструктурі на національному рівні», а на її основі розробити секторальні (галузеві) проектні загрози та об'єктові проектні загрози.
3) По-третє, потрібно визначитися, ***як саме захищати ОКІ від ідентифікованих загроз та оцінити ступінь захищеності ОКІ від цих загроз*** – розробити «Паспорт безпеки об'єкта критичної інфраструктури», в якому мають бути наведені дані про об'єкт, дані про небезпечні природні умови та технологічні процеси, дані щодо основних джерел небезпеки (включно із протиправними діями) та реципієнтів кризових ситуацій (тобто на які об'єкти та людей скажуться наслідки КС на цьому ОКІ, а також які КС на інших об'єктах скажуться на його функціонуванні),
4) По четверте, потрібно мати ***плани запобігання, реагування, взаємодії та відновлення***.

Забезпечення стійкості – основні документи

	На національному рівні	На об'єктовому рівні
Модель загроз	**Проектна загроза на національному рівні**	**Об'єктова проектна загроза**
Паспорт безпеки	**Вимоги до Паспортів безпеки об'єкта КІ**	**Паспорт безпеки об'єкта КІ**
Плани	**Національний план захисту та забезпечення стійкості КІ**	**Плани запобігання, реагування та відновлення**

Модель загроз та проектна загроза



Підходи до захисту КІ – паспортизація об'єктів КІ

В аспекті захисту та забезпечення стійкості критичної інфраструктури одним з ключових документів має стати ***Паспорт безпеки об'єкта КІ.***

НІСД пропонує наступну його структуру:

- Загальні відомості про об'єкт (довідкові дані, дані про територію, відомості про персонал та режим роботи, дані про основні фонди, відомості про внесення до державних реєстрів та кадастрів)*.
- Перелік відповідальних осіб.
- Дані про основні споруди та технологічне обладнання*.
- Дані про природно-кліматичні умови (середні та екстремальні, включно з небезпечними природними явищами)*.
- Дані про небезпечні технологічні процеси*.
- Дані про зв'язки з іншою інфраструктурою: розташування ОКІ по відношенню до місць проживання чи скупчення людей, транспортних систем, а також дані про постачальників, включно з джерелами енерго-, водо- та ресурсо- постачання, та дані про споживачів продукції.
- Оцінка стану аварійної готовності.
- Оцінка стану захищеності (включно з описом організації охорони та системи фізичного захисту ОКІ, інженерно-технічних засобів охорони, об'єктової проектної загрози та оцінки вразливості ОКІ).
- Встановлена категорії критичності ОКІ.

** Примітка - дані з Паспорту ПНО (у разі, якщо ОКІ внесено до реєстру ПНО).*

Підходи до захисту КІ – планування

План запобігання:
- Заходи зі зниження рівня загроз
- Заходи зі зниження вразливості
- Заходи з мінімізації можливої шкоди
- Заходи з підвищення технічної надійності
- Навчання та тренування

Важливо!

Посилання на усі ці плани має бути у Паспорті безпеки ОКІ

План реагування:
- Аварійний план
- План взаємодії на випадок диверсії
- План протидії кіберзагрозам
- План безперервності ведення бізнесу

План відновлення:
- Заходи з відновлення
- Заходи з диверсифікації (альтернативи)
- Заходи з резервування

Захист критичної інфраструктури та забезпечення її стійкості

1) Одним з ключових механізмів забезпечення стійкості критичної інфраструктури є **проведення паспортизації об'єктів критичної інфраструктури,** яка потрібна не лише для виявлення джерел небезпеки, але й **для оцінки здатності систем захисту КІ протистояти усім типам загроз.**
2) Наразі в Україні **відсутній державний орган, який має координувати діяльність у сферах протидії всім типам загроз**. У Великобританії цими питаннями опікується Урядовий офіс. Проектом Закону України "Про критичну інфраструктуру та її захист" передбачається створення **Державної служби із захисту КІ**, яка підпорядковуватиметься КМУ.
3) Для міжсистемної взаємодії державних систем реагування та захисту доцільним вбачається використання національної мережі ситуаційно-кризових центрів (НМ СКЦ). При цьому, одним із ключових елементів цієї мережі з точки зору захисту критичної інфраструктури має стати **Національний центр з питань захисту критичної інфраструктури**. Саме цей центр має здійснювати методологічне забезпечення заходів з ідентифікації, категоризації та паспортизації об'єктів критичної інфраструктури.

Дякую за увагу!

Ванька-встанька як приклад першої стійкої системи

Дмитро Бобро
Провідний науковий співробітник відділу енергетичної та техногенної безпеки НІСД