

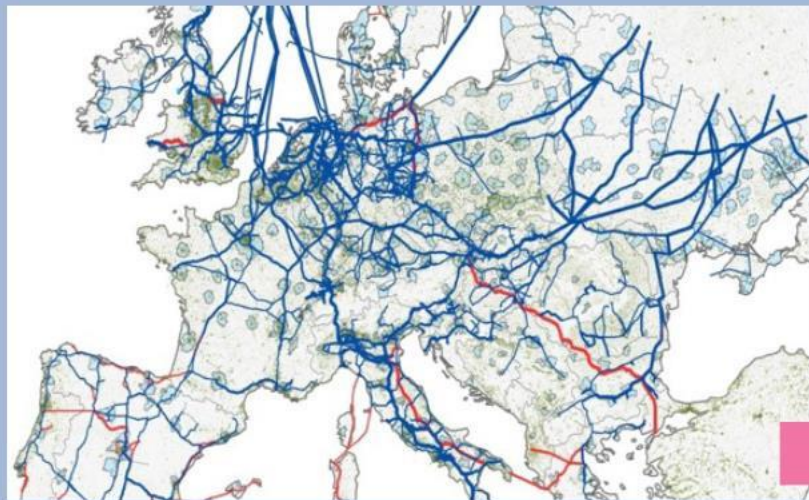


UKRAINIAN
INSTITUTE
FOR THE FUTURE

Кібербезпека.

Новий підхід в Україні

Трансформація економічної безпеки в XXI столітті



Основою економічної безпеки країн **була в першу чергу енергетична безпека**, а трубопроводи і газопроводи плюс система танкерної логістики були кровоносними судинами цієї системи.

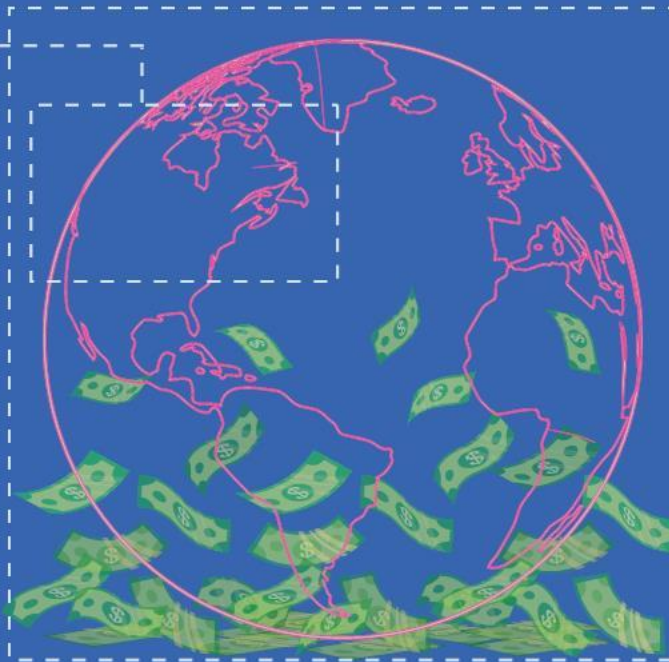
К 20-м рокам XXI століття **все більшу і більшу роль починає займати інформаційна безпека**. Дані та мережева архітектура набувають значення кровоносної системи нової економіки - економіки 21-го століття - економіки даних



Посилення пріоритетності заходів з кібербезпеки

\$10 млрд

Бюджет США
на кібербезпеку
виріс з \$1 млрд
в 2014 році
до \$10 млрд
в 2020-м



\$202,3 млрд

За оцінками компанії Frost & Sullivan загальні витрати на забезпечення кібербезпеки в світовому масштабі в 2021 році складуть понад \$202,3 млрд та будуть збільшуватися на 10,6% кожен рік



UKRAINIAN
INSTITUTE
FOR THE FUTURE

Україна в рейтингах кібербезпеки

14,914
млрд. грн

За даними інформаційно-аналітичного дайджесту Науково-дослідного інституту інформатики і права Національної академії правових наук в 2017 році завдяки вірусу NonPetya **Україна втратила 0.5% ВВП (14,914 млрд. грн.)**

51
місце

За рейтингом британської дослідницької компанії Comparitech серед 60 країн **(за показниками кібератак, зараження мобільних телефонів зловисним ПЗ, рівнем законодавства з кібербезпеки)**, Україна посіла 51 місце

54
місце

В рейтингу Global Cybersecurity Index Україна посіла 54 місце, Литва посіла 4 позицію, Російська Федерація – 26, Казахстан – 40

**найнижчі
ПОЗИЦІЇ**

На рівні регіону Центрально-Східної Європи, Україна займає найнижчі позиції за рівнем кібербезпеки

Це все створює реальну загрозу стабільному функціонуванню державним компаніям, бізнесу та економіки України в цілому

Перелік основних загроз

1.

Незаконне збирання, зберігання, використання, знищення, поширення **персональних даних**.

2.

Порушення штатних режимів роботи автоматизованих систем керування.

3.

Атаки на урядові та приватні веб-сайти в мережі Інтернет

4.

Невідповідність розвитку інфраструктури електронних комунікацій, об'єктів критичної інфраструктури, державних електронних інформаційних ресурсів держави рівню її захищеності

5.

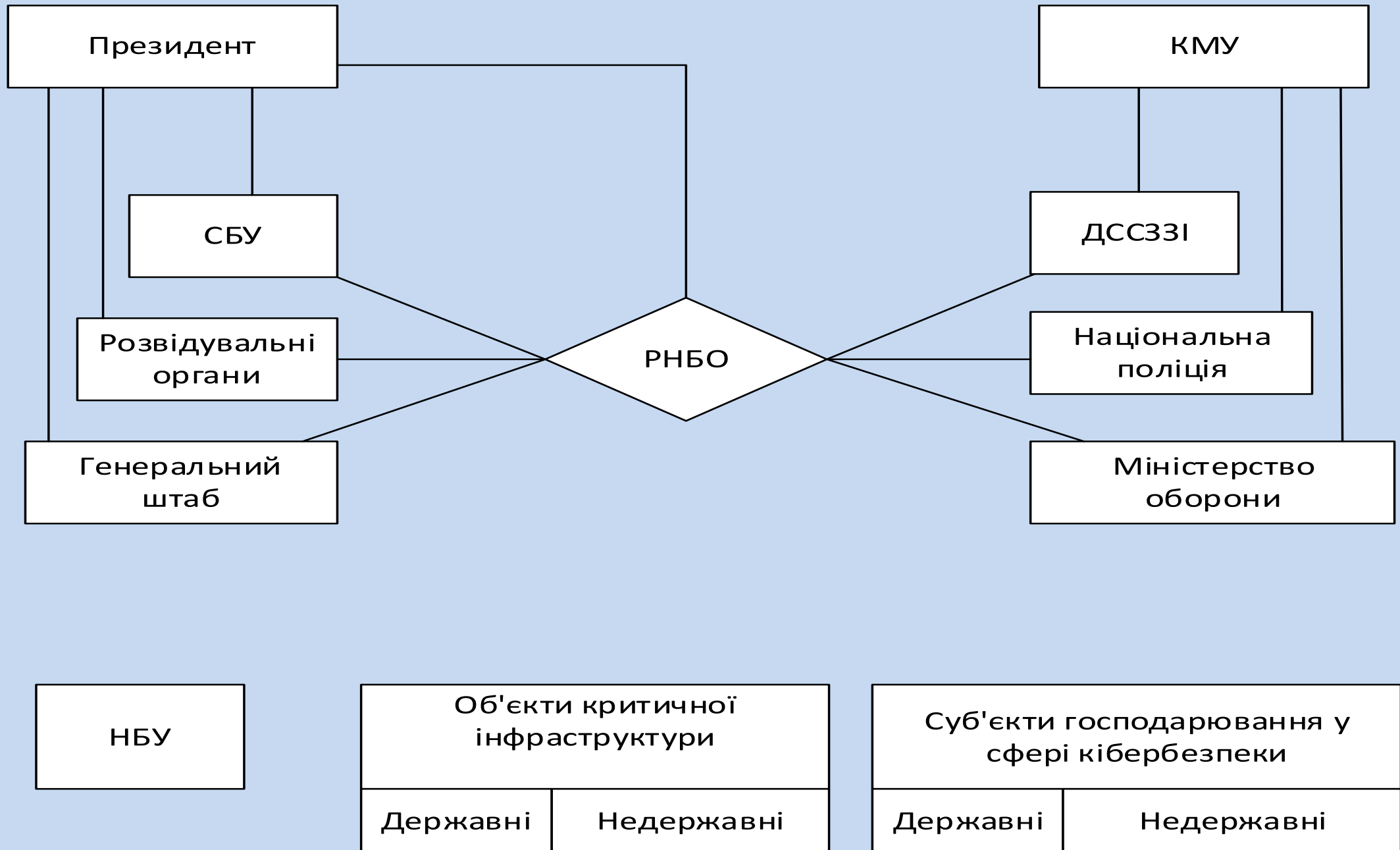
Недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру

6.

Слабкий рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки



Існуюча модель взаємодії суб'єктів сектору кібербезпеки



Проблемні питання реалізації наданих повноважень



Стратегія кібербезпеки

України застаріла та потребує оновлення



Щорічні Плани дій

востаннє було ухвалено у 2018 році



РНБО дуже

завантажене та йому бракує часу ефективно координувати та контролювати діяльність у сфері кібербезпеки



Відсутня єдина національна система

захисту критичної інфраструктури (КИ)



Відсутні правила щодо

проведення аудитів інформаційної безпеки об'єктів КІ та інших суб'єктів забезпечення кібербезпеки



Низькі зарплати, що

уряд платить фахівцям у сфері ІТ та кібербезпеки



Жоден орган не бере на себе повну відповідальність

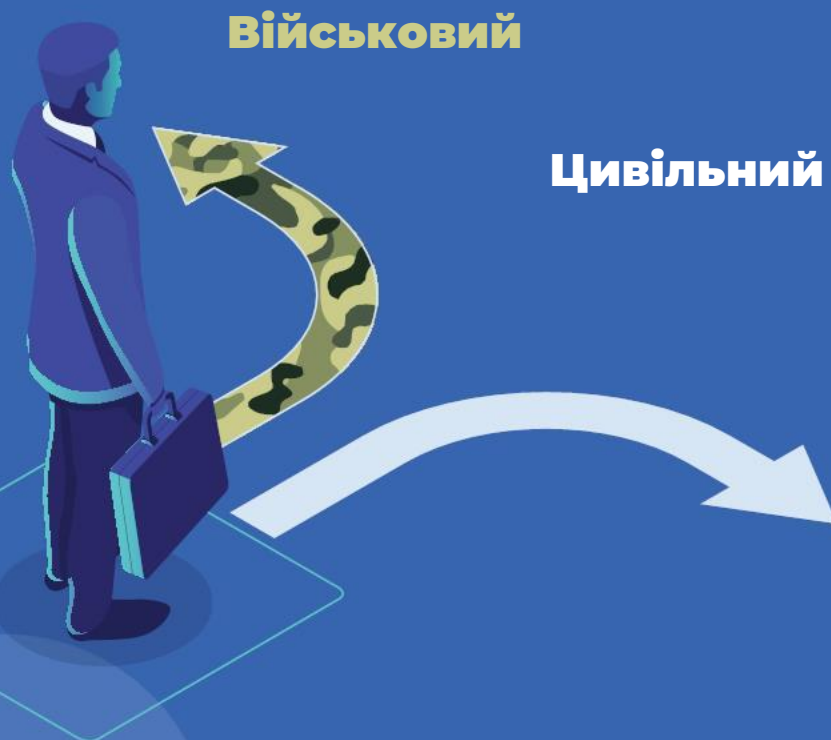


UKRAINIAN
INSTITUTE
FOR THE FUTURE

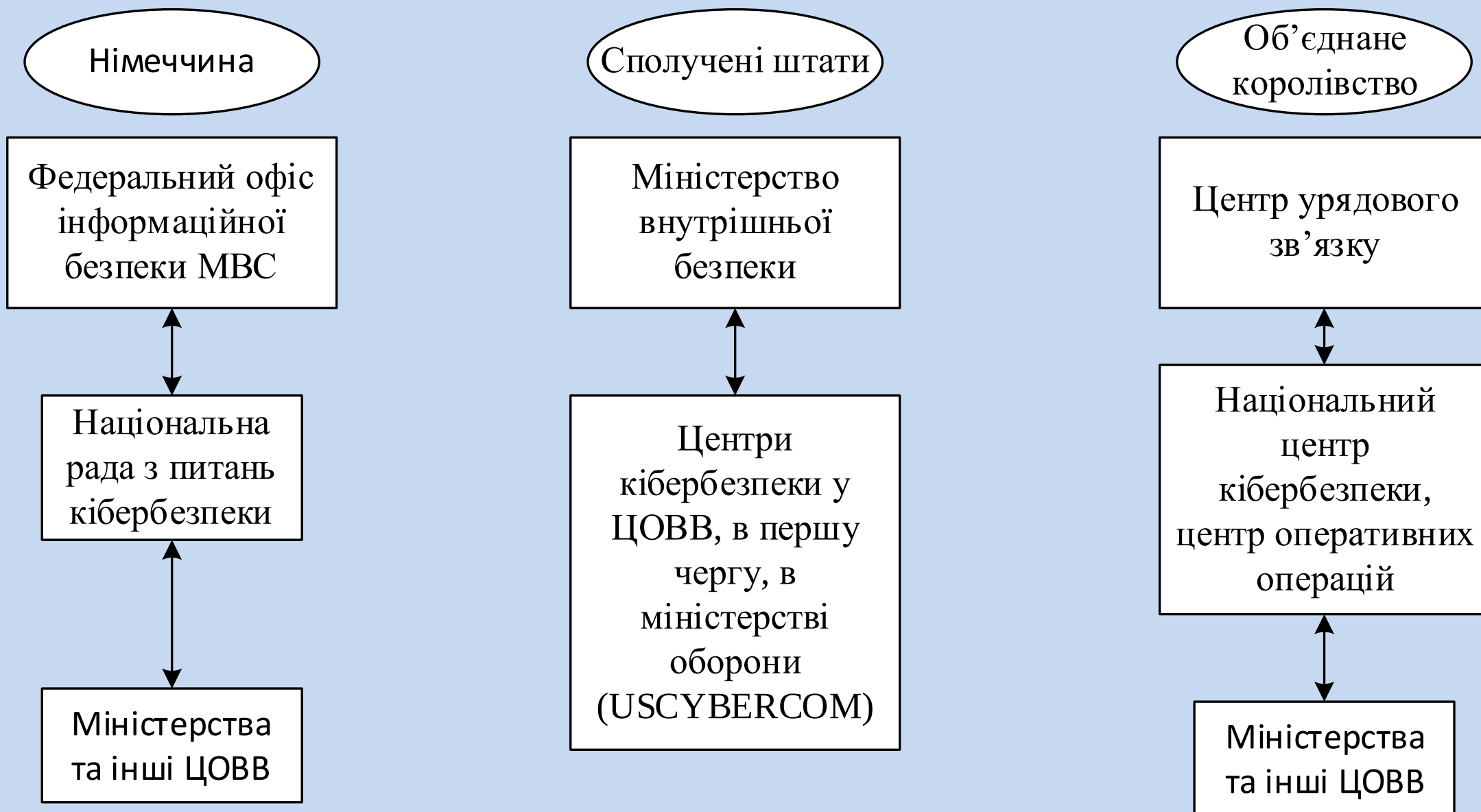
Питання, що потребує вирішення

Існує два підходи:
військовий або цивільний відповідальний за
розбудову системи кібербезпеки.

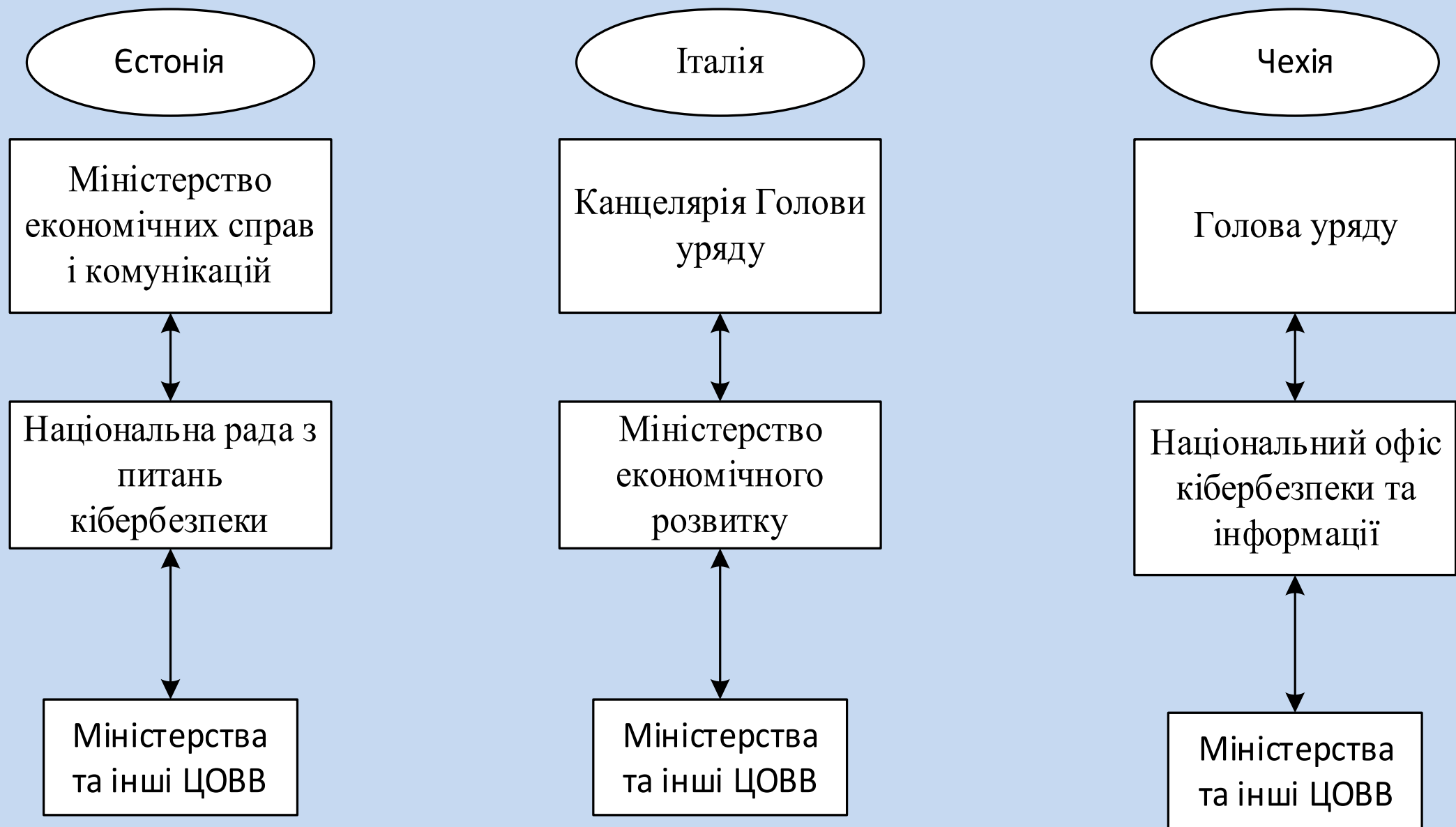
Треба обрати кращий шлях для України.



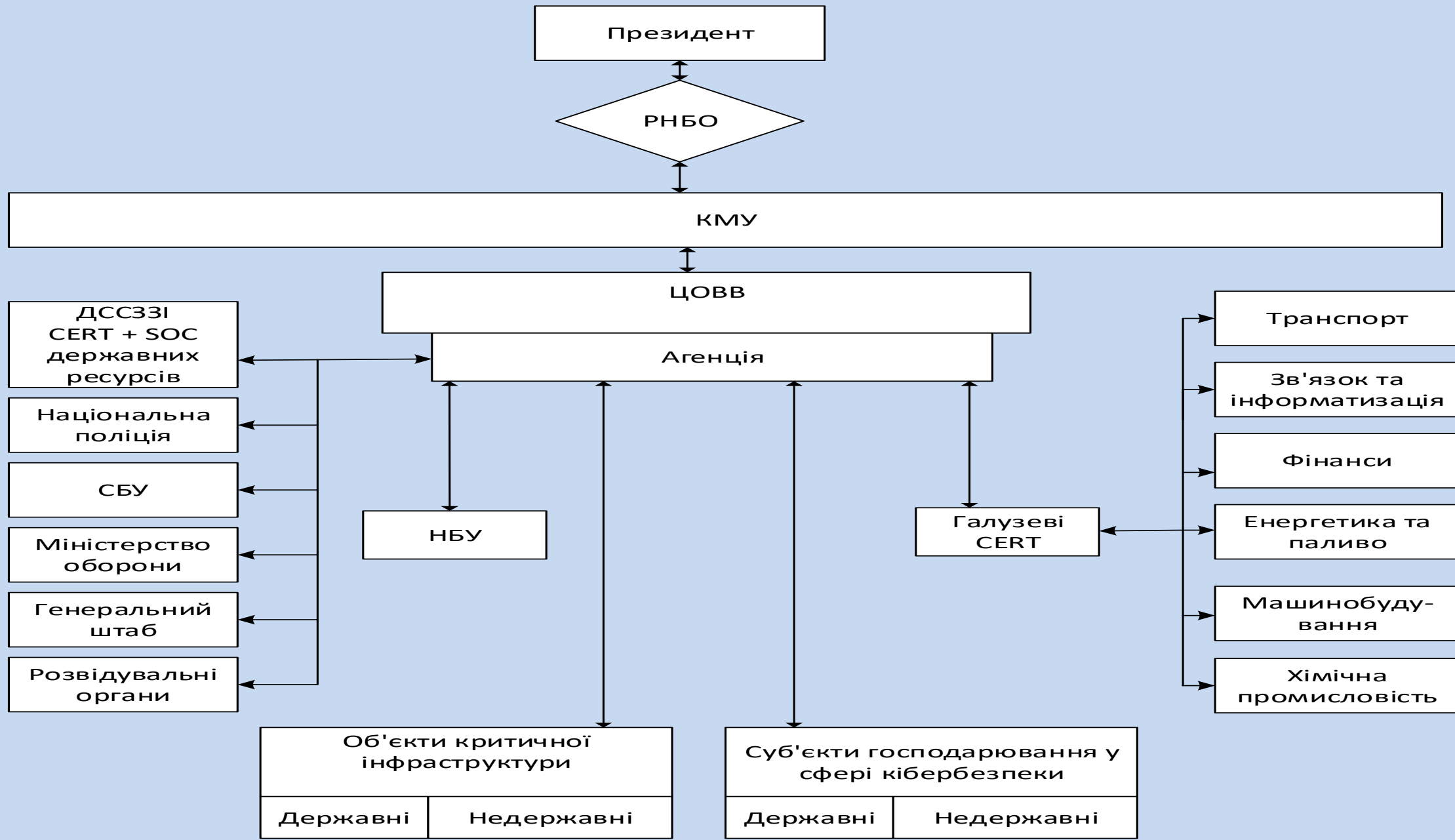
Військовий відповідальний – досвід провідних країн



Цивільний відповідальний – досвід провідних країн



Потенційна модель побудови системи кібербезпеки України



Переваги потенційної моделі



Зменшення впливу

правоохоронних та спеціальних державних органів на суб'єктів господарювання



Усунення дублювання

функцій та боротьби за сфери впливу



Пріоритетність захисту

економіки країни



Збільшення довіри

суб'єктів кіберзахисту до державних органів



Прозоре формування та

розподіл бюджетного, позабюджетного та грантового фінансування заходів із розбудови системи кібербезпеки



Розвиток виробничих і

технологічних ресурсів для кібербезпеки



Підвищення ролі

державно-приватного партнерства



Легалізація «білих» хакерів



UKRAINIAN
INSTITUTE
FOR THE FUTURE

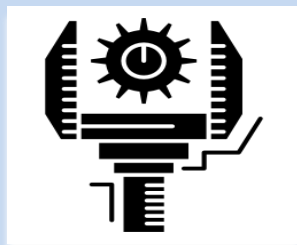
Агенція



Дослідження
інцидентів

Узагальнення та
аналіз, оперативне
інформування,
методична допомога,
профілактика

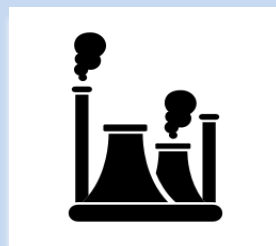
Центр
кібербезпеки



Інцидент

Оперативний
моніторинг,
виявлення та
реагування

Об'єкт



Подія

Порушення штатних
режимів роботи

Суб'єкт



Подія

Порушення
цілісності й
конфіденційності
персональних даних

АГЕНЦІЯ

основні завдання

Національний банк знань з кібербезпеки

Plan

Розробка нормативної бази з кібербезпеки

Розвиток та методологічна підтримка фахової освіти в галузі кібербезпеки

Act

Інформування організацій та фізичних осіб щодо методології кіберзахисту

Взаємодія з державними, приватними, публічними організаціями та фізичними особами

Do

Кіберполігон

Аналітика загроз

Check

Взаємодія з CERT-UA та міжнародними CERT



Створення Агенції та застосування цивільного підходу до реформування системи кібербезпеки дозволить

1. Завершити розбудову єдиної системи кібербезпеки України.
2. Посилити взаємодію між державними, приватними, публічними організаціями та фізичними особами.
3. Гарантувати учасникам взаємодії надійний кіберзахист та надання невідкладної методичної допомоги.
4. Інформувати всіх учасників сектору кібербезпеки та суспільство про необхідні дії при виникненні кіберінцидентів та засоби їх профілактики.
5. Впровадити масштабну цифровізацію, усунути зайві перепони розвитку цифрової економіки, електронної комерції, бізнесу та забезпечити функціонування безпечного інформаційного суспільства в цілому.

Першочергові заходи (дорожня карта)

1.

Розробити Стратегію кібербезпеки України до 2025 року;

2.

Опрацювати питання створення незалежної Агенції кібербезпеки;

3.

Внести відповідні зміни до Закону № 2163-VIII від 5 жовтня 2017 року “Про основні засади забезпечення кібербезпеки України”;

4.

Прийняти Закон про критичну інфраструктуру та її захист;

5.

Розробити законодавчі акти, що реалізують положення Конвенції Ради Європи про кіберзлочинність (Будапештська Конвенція);

6.

Оновити постанови Кабінету Міністрів України з питань кібербезпеки.



UKRAINIAN
INSTITUTE
FOR THE FUTURE

Резюме

1. Проведений аналіз дозволяє зробити висновок щодо доцільності застосування цивільного підходу при розбудові системи кібербезпеки України.
2. З цією метою пропонується створити цивільну незалежну Агенцію з кібербезпеки зі статусом ЦОВВ.
3. Для опрацювання цього питання запропонувати Міністерству цифрової трансформації та Держспецзв'язку створити спільну робочу групу до якої залучити інших досвідчених фахівців з кібербезпеки та експертів Українського інституту майбутнього.