



МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

ЗАСІДАННЯ

РОБОЧОЇ ГРУПИ З ПИТАНЬ

РОЗБУДОВИ КІБЕРЗАХИСТУ ОБ'ЄКТІВ

КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ЕНЕРГЕТИЧНОЇ ГАЛУЗІ

МІНІСТЕРСТВА ЕНЕРГЕТИКИ

УКРАЇНИ

ІЗ СВІТОВИМИ ВИРОБНИКАМИ -

ЛІДЕРАМИ В СФЕРІ КІБЕРБЕЗПЕКИ ТА

ЦИФРОВИХ ТРАНСФОРМАЦІЙ

24-25 ВЕРЕСНЯ 2020 РОКУ

М. ОДЕСА, УКРАЇНА



HUAWEI

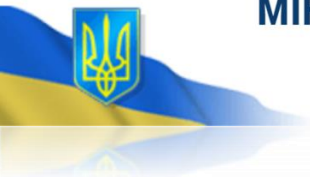


TREND
MICRO



FORTINET





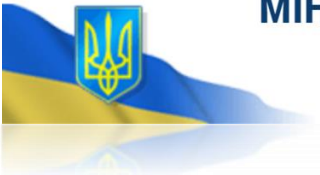
МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

ВІТАЛЬНЕ СЛОВО

Т.В.О.
МІНІСТРА
ЕНЕРГЕТИКИ УКРАЇНИ

ОЛЬГА БУСЛАВЕЦЬ





МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

ВІДКРИТТЯ ЗАСІДАННЯ

ГОЛОВА

РОБОЧОЇ ГРУПИ З ПИТАНЬ
РОЗБУДОВИ КІБЕРЗАХИСТУ ОБ'ЄКТІВ
КРИТИЧНОЇ ІНФРАСТРУКТУРИ
ЕНЕРГЕТИЧНОЇ ГАЛУЗІ



ВІКТОРІЯ ГНАТОВСЬКА





ДОРОЖНЯ КАРТА
РОЗБУДОВИ КІБЕРЗАХИСТУ
ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
ЕНЕРГЕТИЧНОЇ ГАЛУЗІ



ДОРОЖНЯ КАРТА
РОЗБУДОВИ КІБЕРЗАХИСТУ
ОБ'ЄКТІВ КРИТИЧНОЇ
ІНФРАСТРУКТУРИ
ЕНЕРГЕТИЧНОЇ ГАЛУЗІ

step 1

ПРОЕКТНИЙ ОФІС

для секторальної координації реалізації ініціативи та залучення міжнародної технічної допомоги;

1. Розробка політики у сферах галузевих стандартів кібербезпеки та вимог до критичної інфраструктури
2. Розробка стратегії кібербезпеки для критичної інфраструктури енергетичного сектору
3. Реалізація секторальних проектів з кібербезпеки

Проектний офіс з питань кібербезпеки - це дорадчий орган Міненерго, команда експертів та менеджерів проектів, яка тісно координує свою діяльність з Міністерством енергетики України з основною метою - підвищення стійкості до кібербезпеки в енергетичному секторі України шляхом формування політики, розробки та координації проектів з кібербезпеки.





ДОРОЖНЯ КАРТА
РОЗБУДОВИ КІБЕРЗАХИСТУ
ОБ'ЄКТІВ КРИТИЧНОЇ
ІНФРАСТРУКТУРИ
ЕНЕРГЕТИЧНОЇ ГАЛУЗІ

step 2

АУДИТ СТАНУ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЕНЕРГЕТИЧНОГО СЕКТОРУ

Основні напрямки оцінки:

- Персонал
- Процеси
- Технології



Аудит кібербезпеки критичної інфраструктури енергетики - це процес збору інформації про поточний рівень стійкості кібербезпеки в енергетичному секторі України



СЕКТОРАЛЬНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

1. Прискорення впровадження секторальної енергетичної кібербезпеки
2. Покращення безпеки та можливості аварійного відновлення
3. Секторальний обмін даними з кібербезпеки

Секторний центр кібербезпеки повинен забезпечити передовий захист від кіберзагроз, запобігти вторгненню, зменшити ризики впливу, запобігти новим та, у разі загроз, ефективно реагувати на секторальному рівні

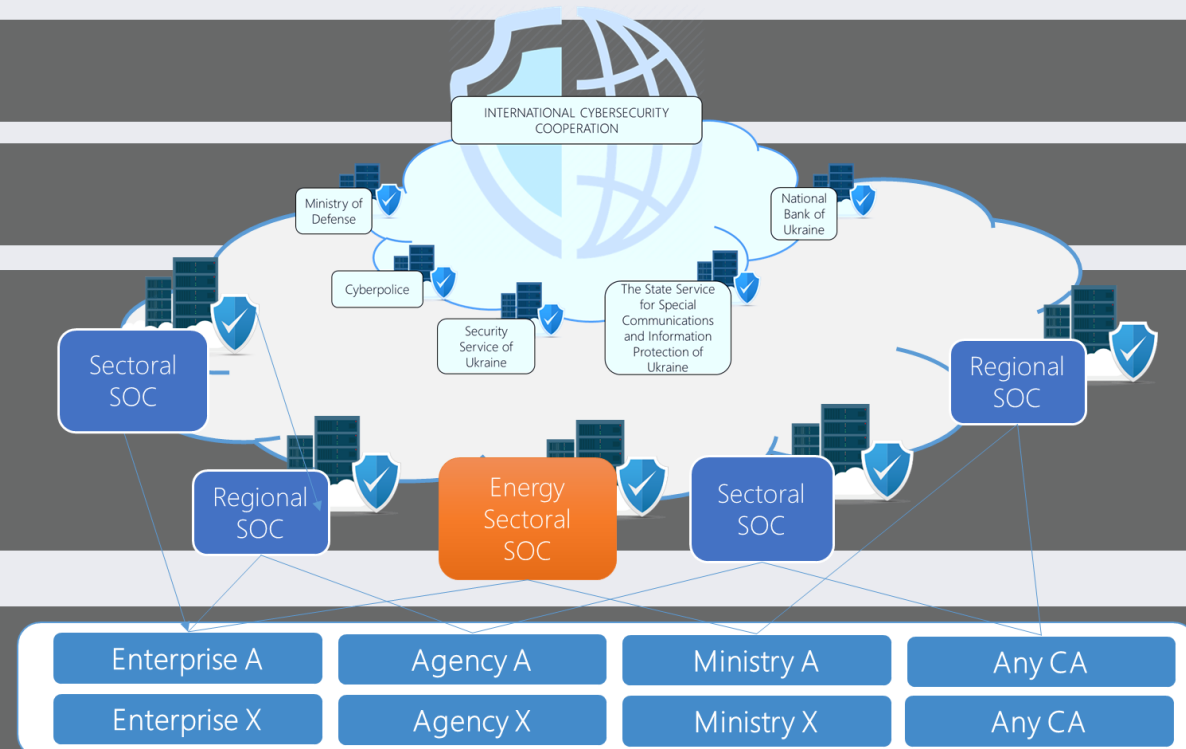
ДОРОЖНЯ КАРТА
РОЗБУДОВИ КІБЕРЗАХИСТУ
ОБ'ЄКТІВ КРИТИЧНОЇ
ІНФРАСТРУКТУРИ
ЕНЕРГЕТИЧНОЇ ГАЛУЗІ
step 3

1 GLOBAL LAYER

2 NATIONAL LAYER

3 SECTORAL / REGIONAL LAYER

4 ENTERPRISE LAYER





step 1

ПРОЕКТНИЙ ОФІС З
КІБЕРБЕЗПЕКИ

step 2

АУДИТ СТАНУ КІБЕРБЕЗПЕКИ
КРИТИЧНОЇ ІНФРАСТРУКТУРИ
ЕНЕРГЕТИЧНОГО СЕКТОРУ

step 3

СЕКТОРАЛЬНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

ДОРОЖНЯ КАРТА

РОЗБУДОВИ КІБЕРЗАХИСТУ

ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ЕНЕРГЕТИЧНОЇ ГАЛУЗІ





Міністерство
енергетики
України

ЗАСІДАННЯ

**РОБОЧОЇ ГРУПИ З ПИТАНЬ РОЗБУДОВИ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
ЕНЕРГЕТИЧНОЇ ГАЛУЗІ**

МІНІСТЕРСТВА ЕНЕРГЕТИКИ УКРАЇНИ

ІЗ

СВІТОВИМИ ВИРОБНИКАМИ - ЛІДЕРАМИ В СФЕРІ КІБЕРБЕЗПЕКИ ТА ЦИФРОВИХ ТРАНСФОРМАЦІЙ

**24-25 вересня 2020 року
м. Одеса, Україна**



Міністерство
енергетики
України

ЗАСІДАННЯ

**РОБОЧОЇ ГРУПИ З ПИТАНЬ РОЗБУДОВИ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
ЕНЕРГЕТИЧНОЇ ГАЛУЗІ**

МІНІСТЕРСТВА ЕНЕРГЕТИКИ УКРАЇНИ

ІЗ

СВІТОВИМИ ВИРОБНИКАМИ - ЛІДЕРАМИ В СФЕРІ КІБЕРБЕЗПЕКИ ТА ЦИФРОВИХ ТРАНСФОРМАЦІЙ

**24-25 вересня 2020 року
м. Одеса, Україна**



МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

Н А К А З

м. Київ

Про План заходів із забезпечення кібербезпеки об'єктів критичної інфраструктури енергетичної галузі

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України»; Правил про безпеку постачання електричної енергії, затверджених наказом Міністерства енергетики та вугільної промисловості від 27.08.2018 № 448 (зарєєстрованим у Міністерстві юстиції України 19.09.2018 за № 1076/32528); з урахуванням п.2.2 наказу Міністерства енергетики України від 19.06.2020 № 389 «Про Робочу групу з розбудови кіберзахисту об'єктів критичної інфраструктури енергетичної галузі»; з метою створення дієвої системи кібербезпеки об'єктів критичної інфраструктури енергетичної галузі України

н а к а з у ю:

1. Затвердити План заходів із забезпечення кібербезпеки об'єктів критичної інфраструктури енергетичної галузі (далі – План заходів), що додається.

2. Управлінню цифрової політики та безпеки (Валерій КУЛИК-КУЛИЧЕНКО), керівникам державних підприємств, установ та організацій, що належать до сфери управління Міненерго, господарських товариств, щодо яких Міненерго здійснює повноваження з управління корпоративними правами держави та господарських структур, контроль за діяльністю яких здійснює Міністерство, забезпечити виконання Плану заходів, затвердженого цим наказом.

3. Робочій групі з розбудови кіберзахисту об'єктів критичної інфраструктури енергетичної галузі, утвореній згідно з наказом Міністерства енергетики від 19.06.2020 № 389, у разі потреби надавати пропозиції щодо внесення змін до Плану заходів з урахуванням нормативно-правових актів Уряду.

4. Контроль за виконанням цього наказу покласти на заступника Міністра БОЙКА Юрія.

В. о. Міністра

Ольга БУСЛАВЕЦЬ

ЗАТВЕРДЖЕНО
Наказ Міністерства енергетики
України

№ _____

План заходів із забезпечення кібербезпеки об'єктів критичної інфраструктури енергетичної галузі

1. Визначення (оновлення, актуалізація, формування) Переліку об'єктів енергетичної галузі, що можуть бути віднесені до об'єктів критичної інфраструктури, зокрема шляхом повторного опитування (доручення Кабінету Міністрів України від 16.04.2020 № 10512/1/1-20) відповідно до опитувального листа, розробленого Державною службою спеціального зв'язку та захисту інформації України, та отриманої інформації від організацій, відповідальних за такі об'єкти, що належать до сфери управління Міністерства енергетики України.

Термін – IV квартал 2020 року.

2. Розробка проекту *Правил/Рекомендацій забезпечення кібербезпеки об'єктів критичної інфраструктури енергетичної галузі* з метою приведення до єдиних вимог кіберзахисту об'єктів енергетичної галузі.

Термін – IV квартал 2020 року.

3. Розробка проекту Галузевого документу з кібербезпеки об'єктів критичної інфраструктури енергетичної галузі (у виконання пункту 1 частини п'ятої статті 10 Закону України «Про основні засади забезпечення кібербезпеки України»; пункту 14 Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19.06.2019 № 518) з метою побудови дієвого захисту об'єктів критичної інфраструктури енергетичної галузі та забезпечення постійного моніторингу кіберінцидентів.

Термін – IV квартал 2020 року.

4. Розроблення Плану побудови кіберцентру.

Термін – IV квартал 2020 року.

5. Здійснення всебічного вивчення наявного стану забезпечення кібербезпеки об'єктів енергетичної галузі, що належать до сфери управління Міненерго, зокрема – шляхом проведення аудиту стану забезпечення кібербезпеки на об'єктах критичної інфраструктури енергетичної галузі.

Термін – постійно.

**Начальник Управління
цифрової політики та безпеки**

В. Кулик-Куличенко



МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

ЗАСІДАННЯ

РОБОЧОЇ ГРУПИ З ПИТАНЬ

РОЗБУДОВИ КІБЕРЗАХИСТУ ОБ'ЄКТІВ

КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ЕНЕРГЕТИЧНОЇ ГАЛУЗІ

МІНІСТЕРСТВА ЕНЕРГЕТИКИ

УКРАЇНИ

ІЗ СВІТОВИМИ ВИРОБНИКАМИ -

ЛІДЕРАМИ В СФЕРІ КІБЕРБЕЗПЕКИ ТА

ЦИФРОВИХ ТРАНСФОРМАЦІЙ

24-25 ВЕРЕСНЯ 2020 РОКУ

М. ОДЕСА, УКРАЇНА



HUAWEI



TREND
MICRO



Hewlett Packard
Enterprise



FORTINET



Цифрова трансформація енергетичного сектору

На порозі змін

MARKET TRENDS & CYBERTHREATS



FROM MICHAEL MANN
blackhat
OFFICIAL TRAILER 2

MARKET TRENDS & CYBERTHREATS



MARKET TRENDS & CYBERTHREATS

HACKED

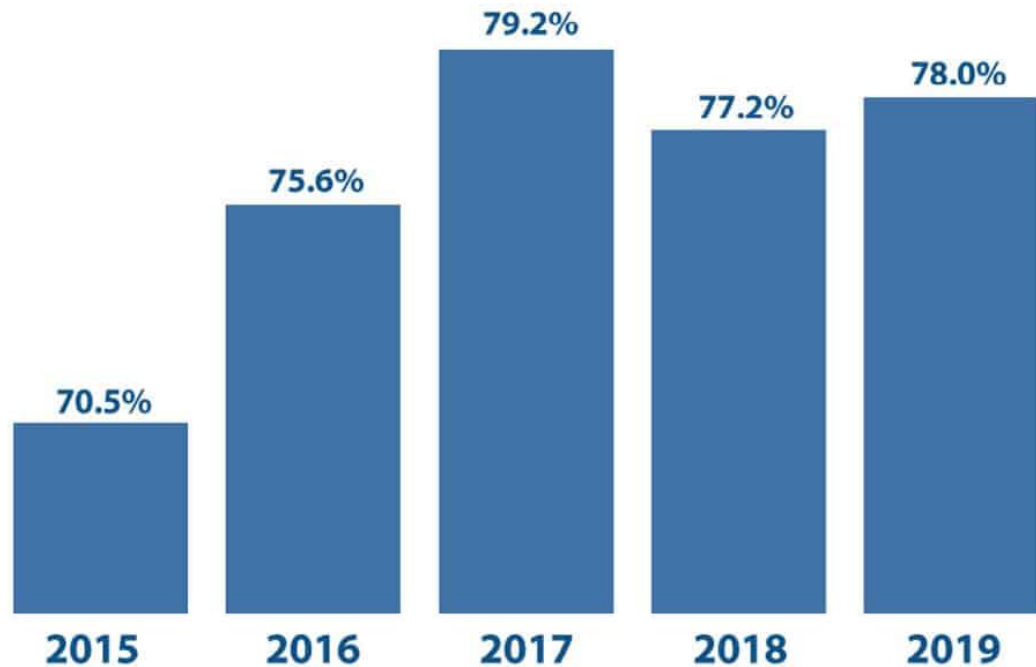


Figure 1: Frequency of successful attacks by year.

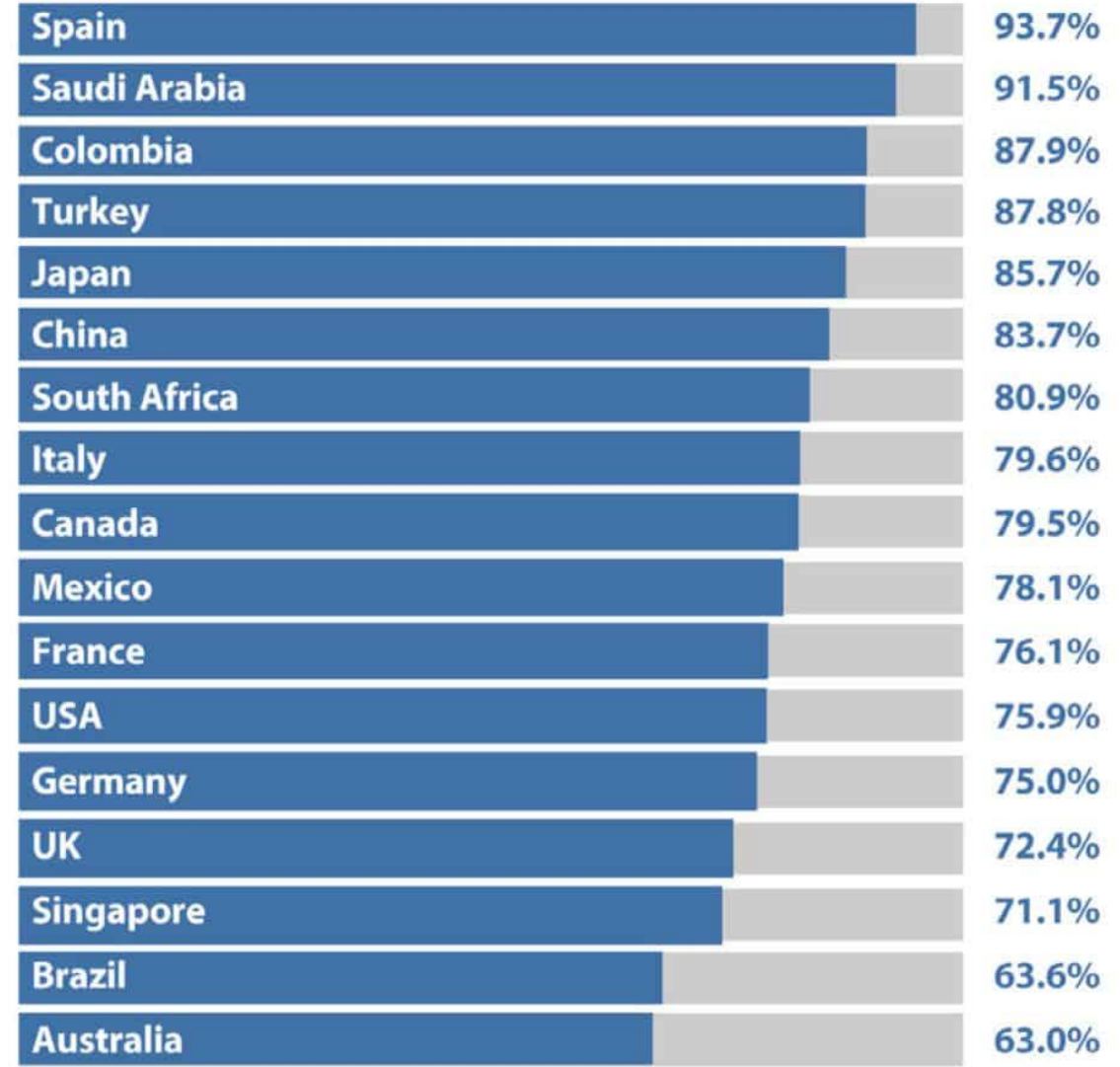


Figure 2: Percentage compromised by at least one successful attack in the past 12 months.

NATIONAL CYBERSECURITY OVERVIEW

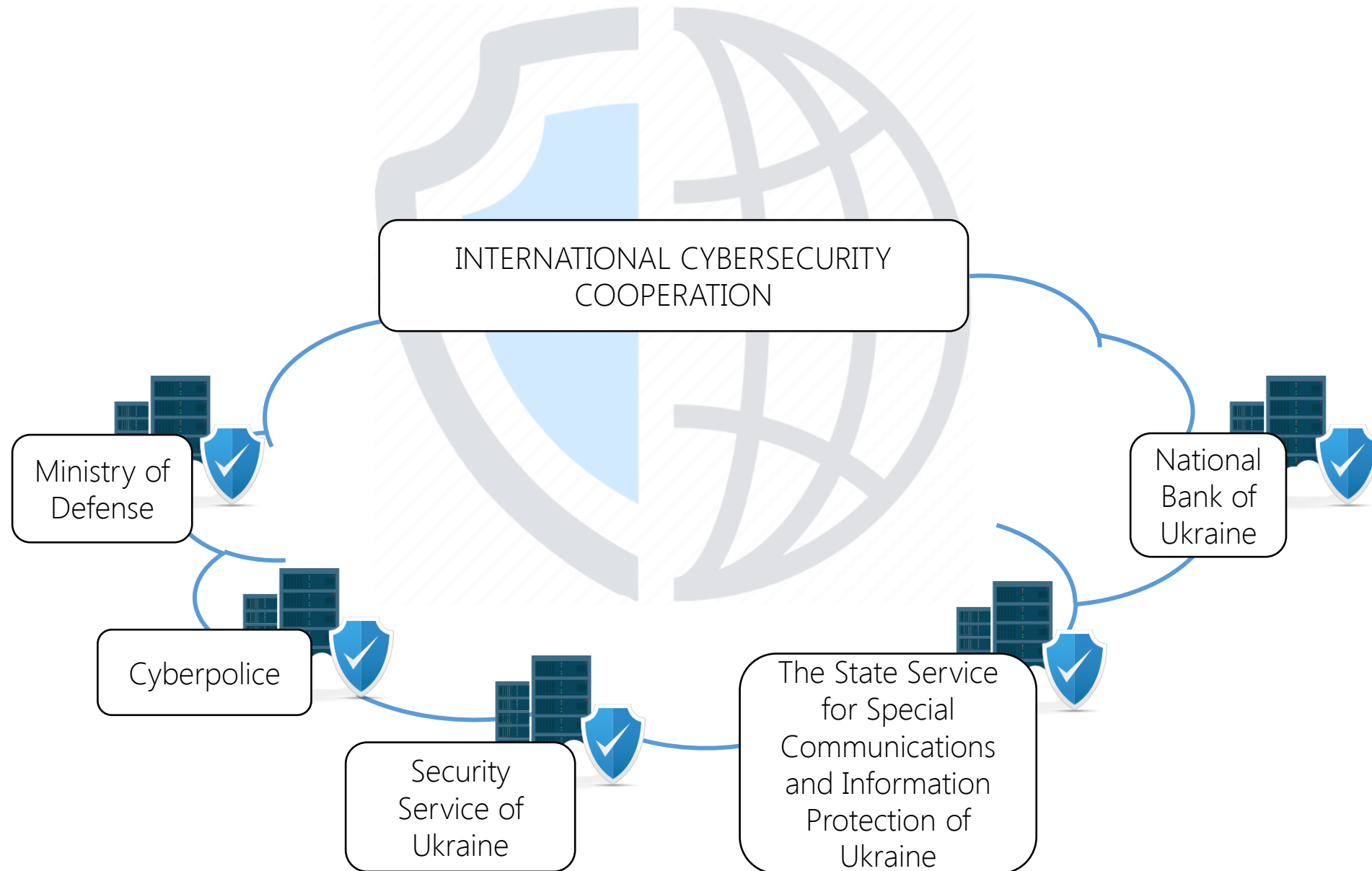
The Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine"

National Cybersecurity Strategy of Ukraine

The concept of the development of the digital economy and society of Ukraine for 2018-2020

The Law of Ukraine "On the National Program of Informatization"

The Ukraine–European Union Association Agreement
European Union Association Agreement between the European Union, Euratom, Ukraine and the EU's 28 member states



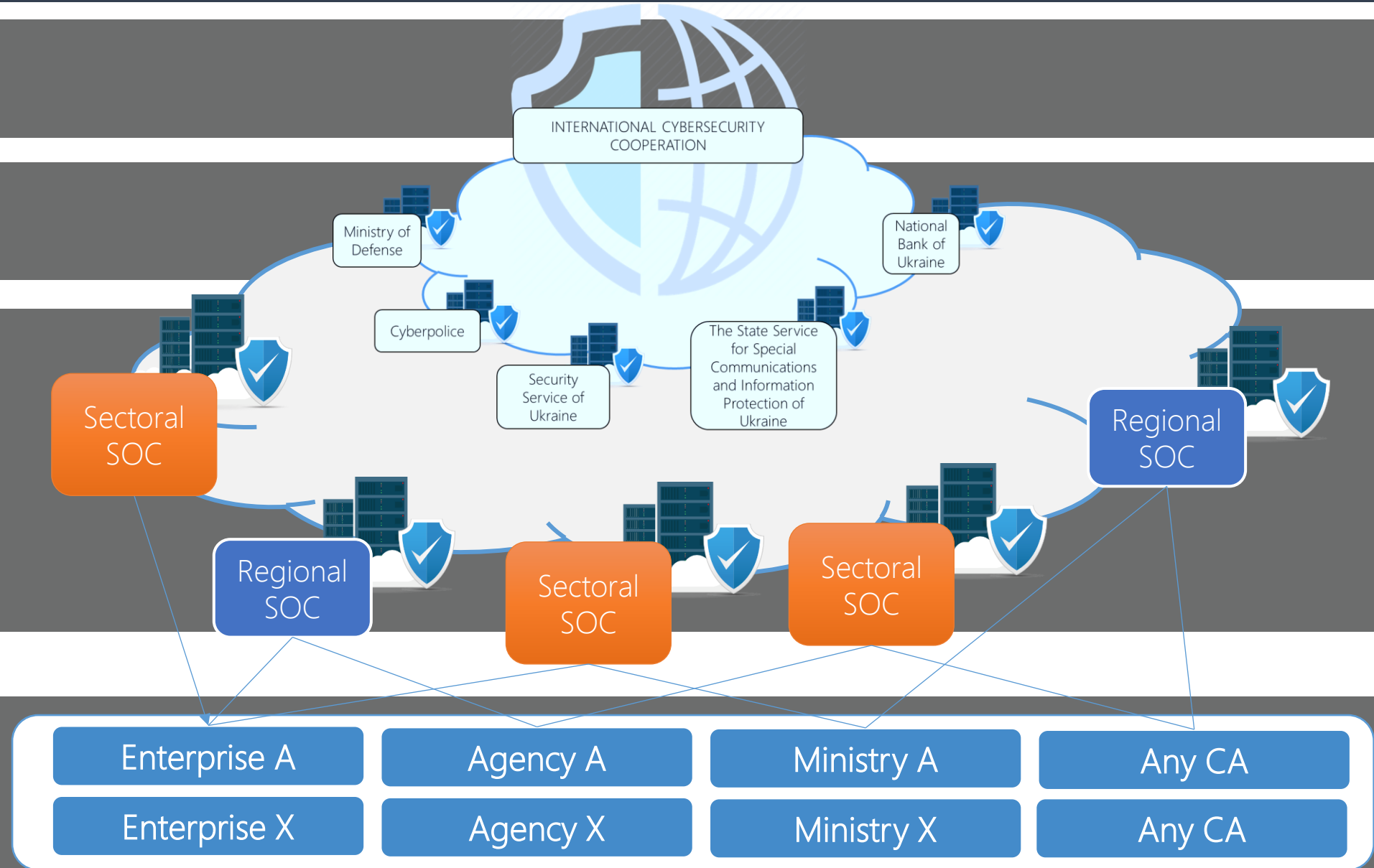
NATIONAL CYBERSECURITY OVERVIEW

1 GLOBAL LAYER

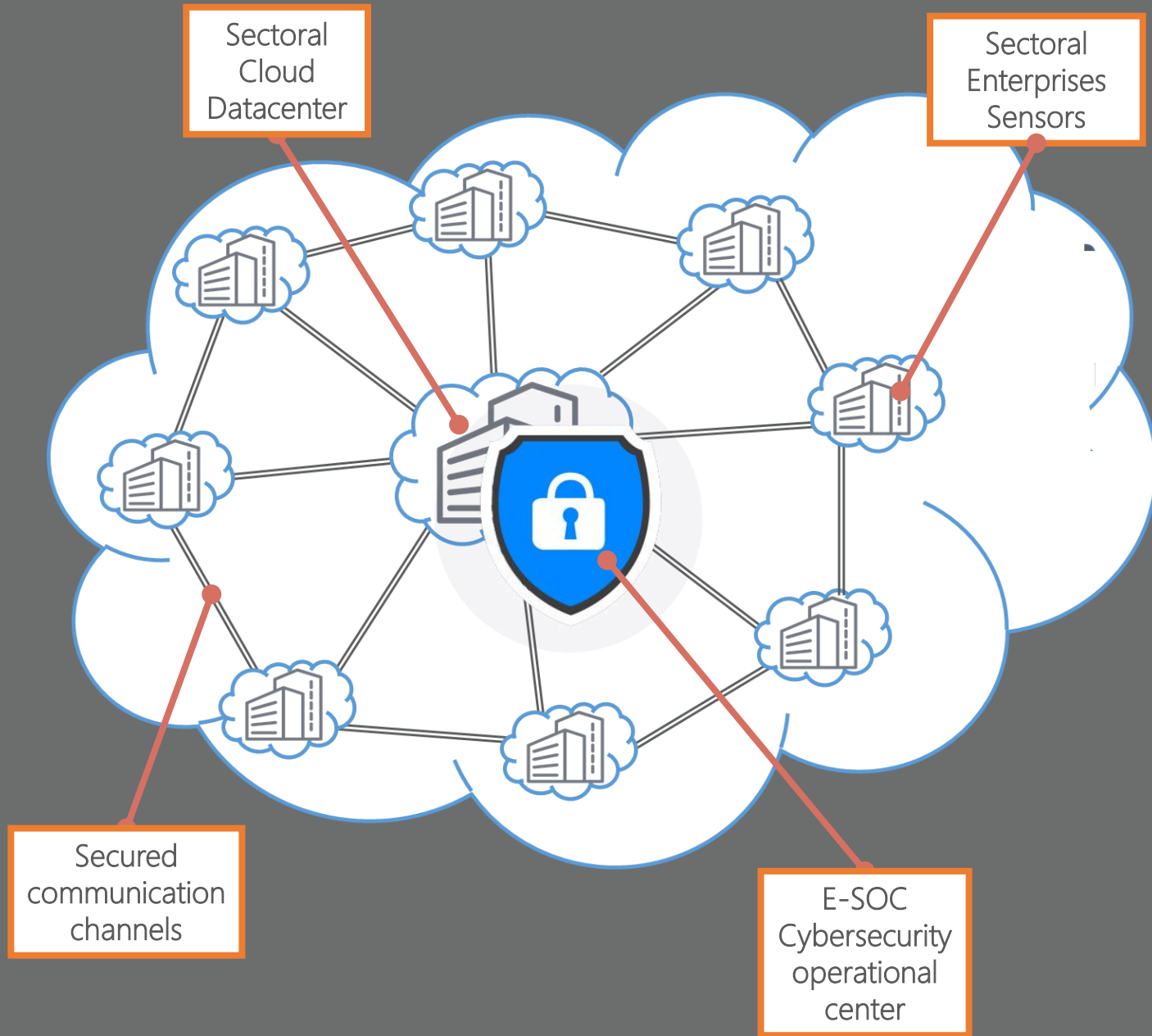
2 NATIONAL LAYER

3 SECTORAL / REGIONAL LAYER

4 ENTERPRISE LAYER



E-CYBER – SECTORAL CYBERSECURITY VISION



MISSION : Sectoral Center for Cybersecurity should provide a front line of defense against cyber threats, prevent intrusions, reduce current vulnerabilities, prevent new ones and, in the event of threats, effectively response.

EXPECTED RESULTS: Cybersecurity and cyber defense from the full spectrum of threats of the Ministry of Energy, enterprises, institutions and organizations belonging to the sphere of management.

BENEFITS:

- Acceleration of the implementation of sectoral cybersecurity
- Improvement of security and disaster recovery
- 10x cost reduction

TECHNICAL MODEL

consists of two zones and the corresponding interaction between them:

- 1. CyberCenter (E-SOC)** – The centralized zone, where the aggregation of the determined information and services takes place. Such aggregation is approached within the cyberspace monitoring and detecting tools for the purpose of prompt and systematic prevention of cyberthreats, the distribution of information (proofing) to other entities of the Ministry of Energy and Coal Industry of Ukraine;
- 2. CyberNet** – decentralized zone, represented by sectoral entities of the system, that are users of information systems, telecommunication networks, computer equipment, etc. - in general, any tools where information and telecommunication technologies are used for storing, processing and data exchange.

COMPONENTS

E-SOC

Security operations Center - software & hardware

DataCenter

Uptime Institute Tier III Certified Facility

Cybersecurity sensors

for Monitoring and prevention of Cyberthreats

Secured communication channels

E-CYBER ROADMAP

To Do

Legislation & Policy

Operations & Processes

Technology

Education and cyber hygiene

How To Do

Cybersecurity Coordination Office

Audit of Sectoral Cybersecurity

Cyber Hygiene awareness

E-SOC – Sectoral Cybersecurity Center

PROJECT MANAGEMENT OFFICE FUNCTIONAL STRUCTURE AND STAFFING

6 EXPERTS

Legislation & Policy

Operations & Processes

Technology

Education and cyber hygiene

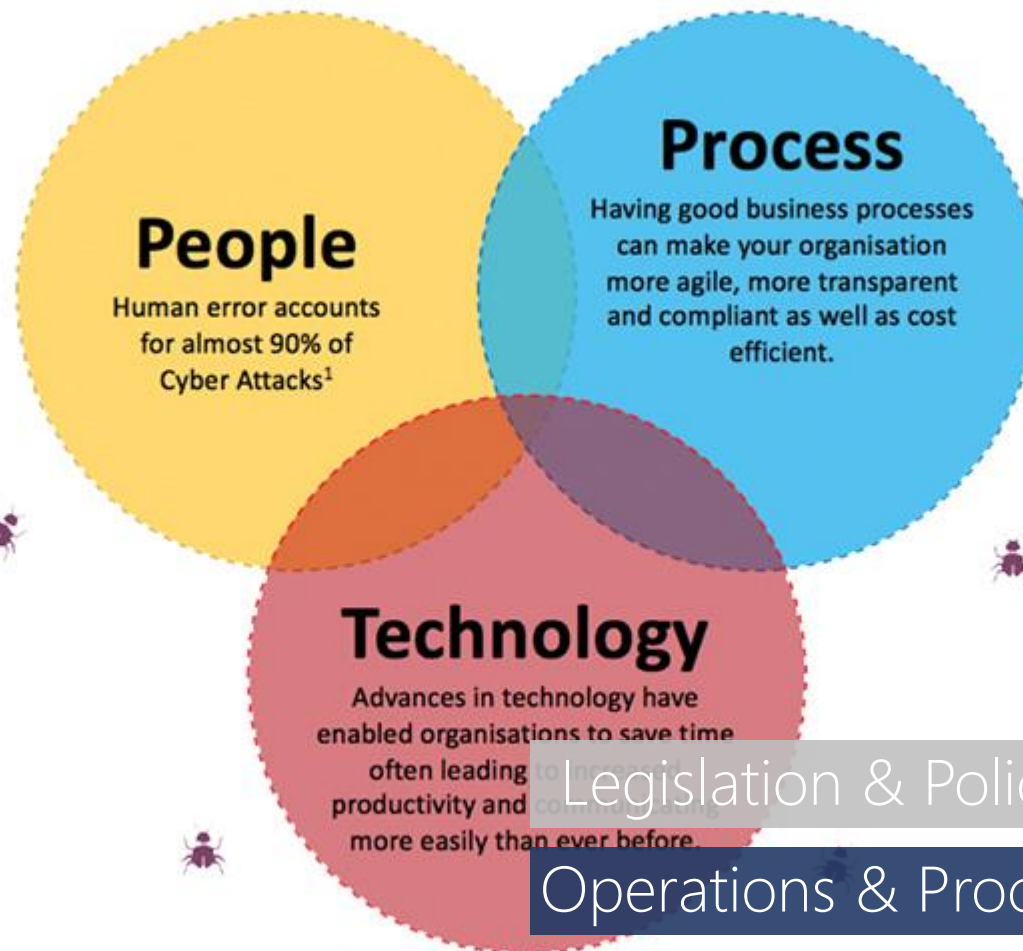
#	Position	Major Functions
1	Director of the Office	Coordination of the project, communication with the government officials and donors, management of the Cybersecurity team, support of approval the official documents
2	Legal Counsel	Development and approval of the legal acts necessary for sustainable functioning of the Industry Center for Cybersecurity
3	Legal Expert	Supports the Legal Counsel in his/her assignments, drafting tender documentation
4	Project Manager	Management of the project: development of the design and concept of the project of the Industry Center for Cybersecurity
5	Financial Analyst	Supports the Project Manager in financial modelling of the project and development of methodology for the cybersecurity fees
6	Technical Analyst	Supports the Project Manager with the technical consultation regarding the hardware and software components

E-CYBER ROADMAP

AUDIT OF SECTORAL CYBERSECURITY



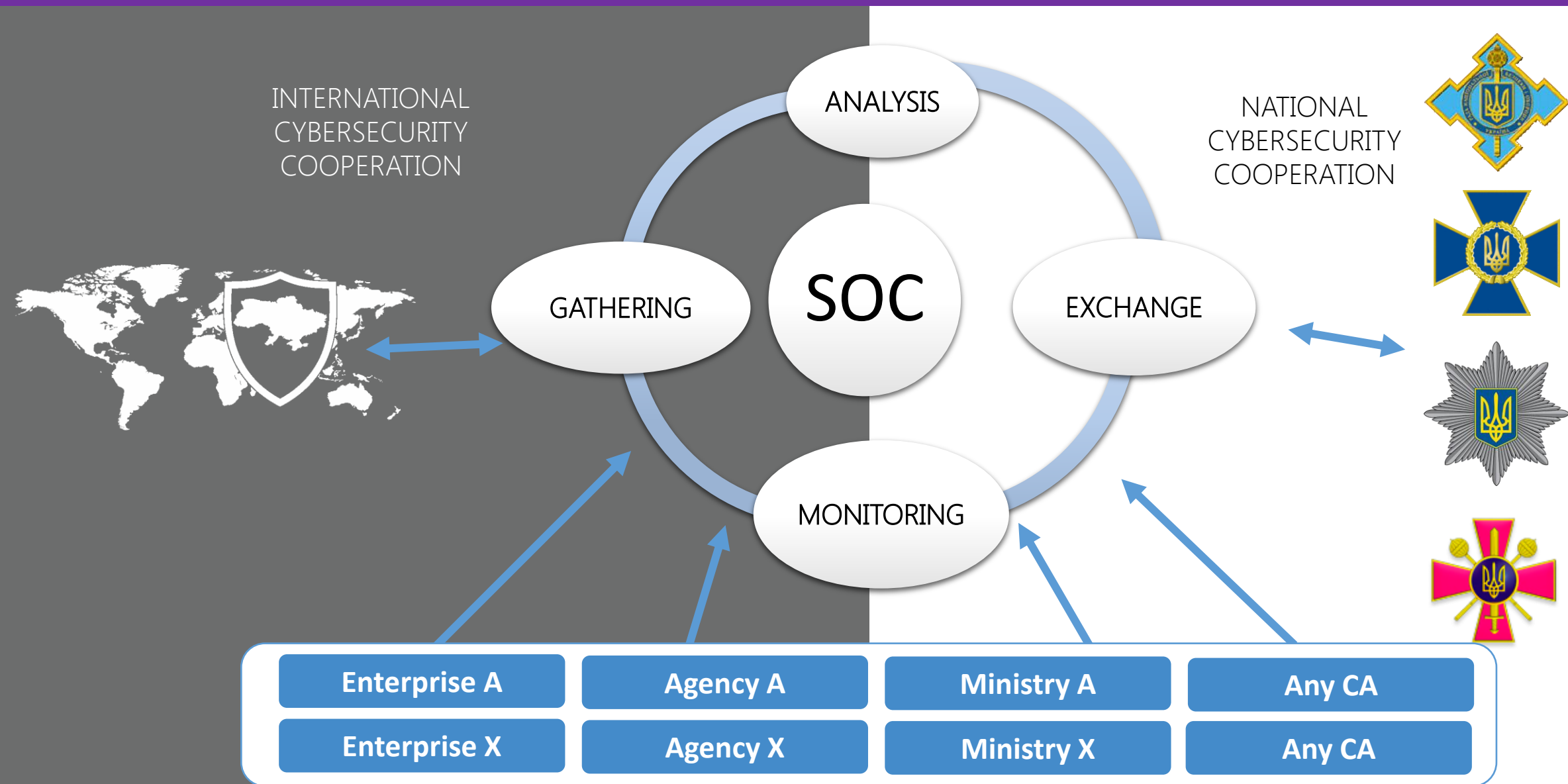
© FMB Solutions. All rights reserved



- Legislation & Policy
- Operations & Processes
- Technology
- Education and cyber hygiene

E-CYBER ROADMAP

E-SOC – SECTORAL CYBERSECURITY CENTER



E-CYBER ROADMAP

E-SOC – SECTORAL CYBERSECURITY CENTER

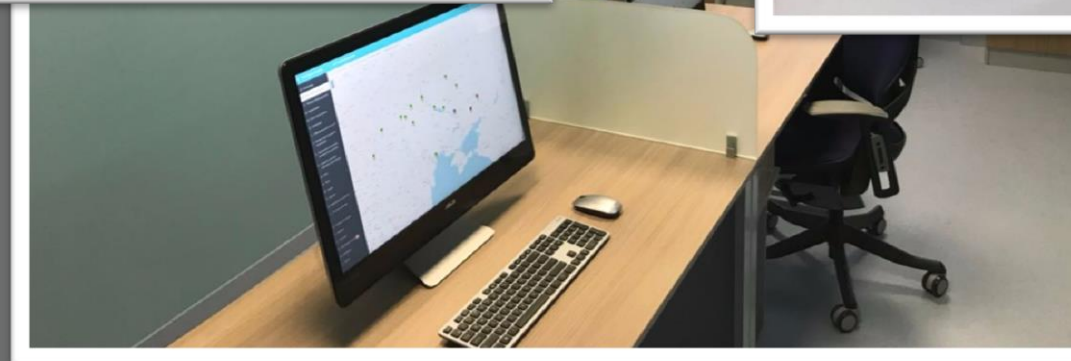


Legislation & Policy

Operations & Processes

Technology

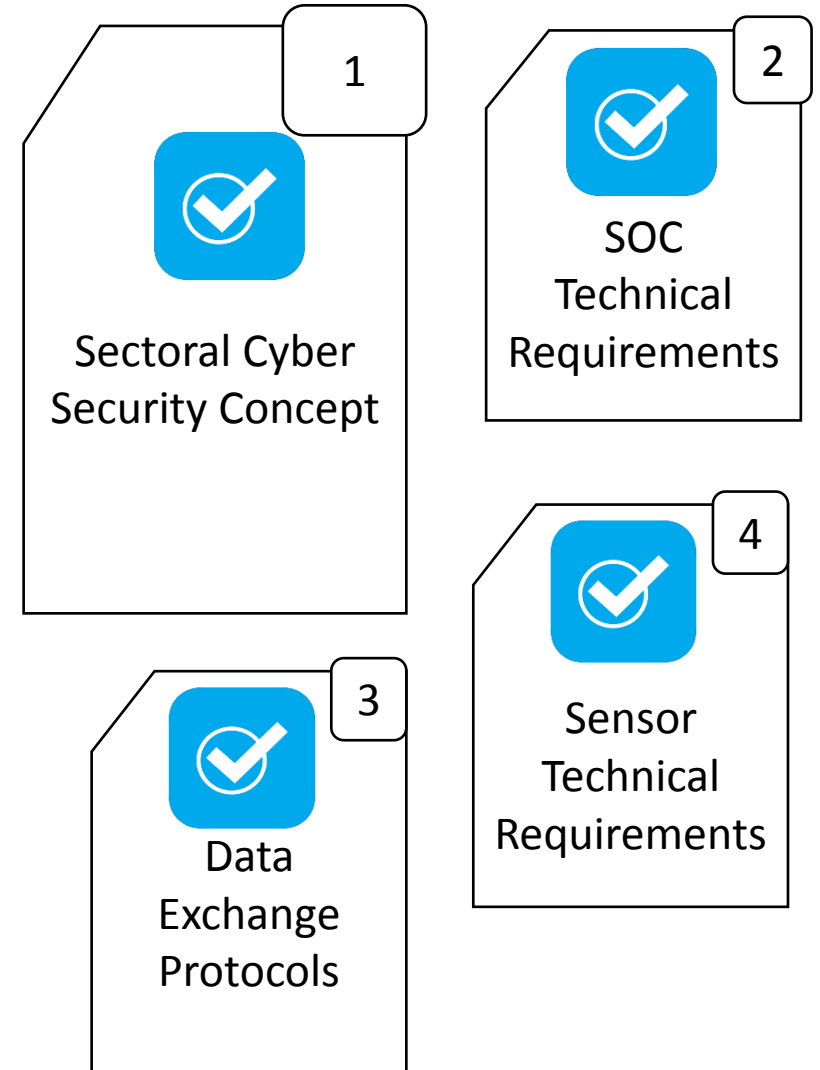
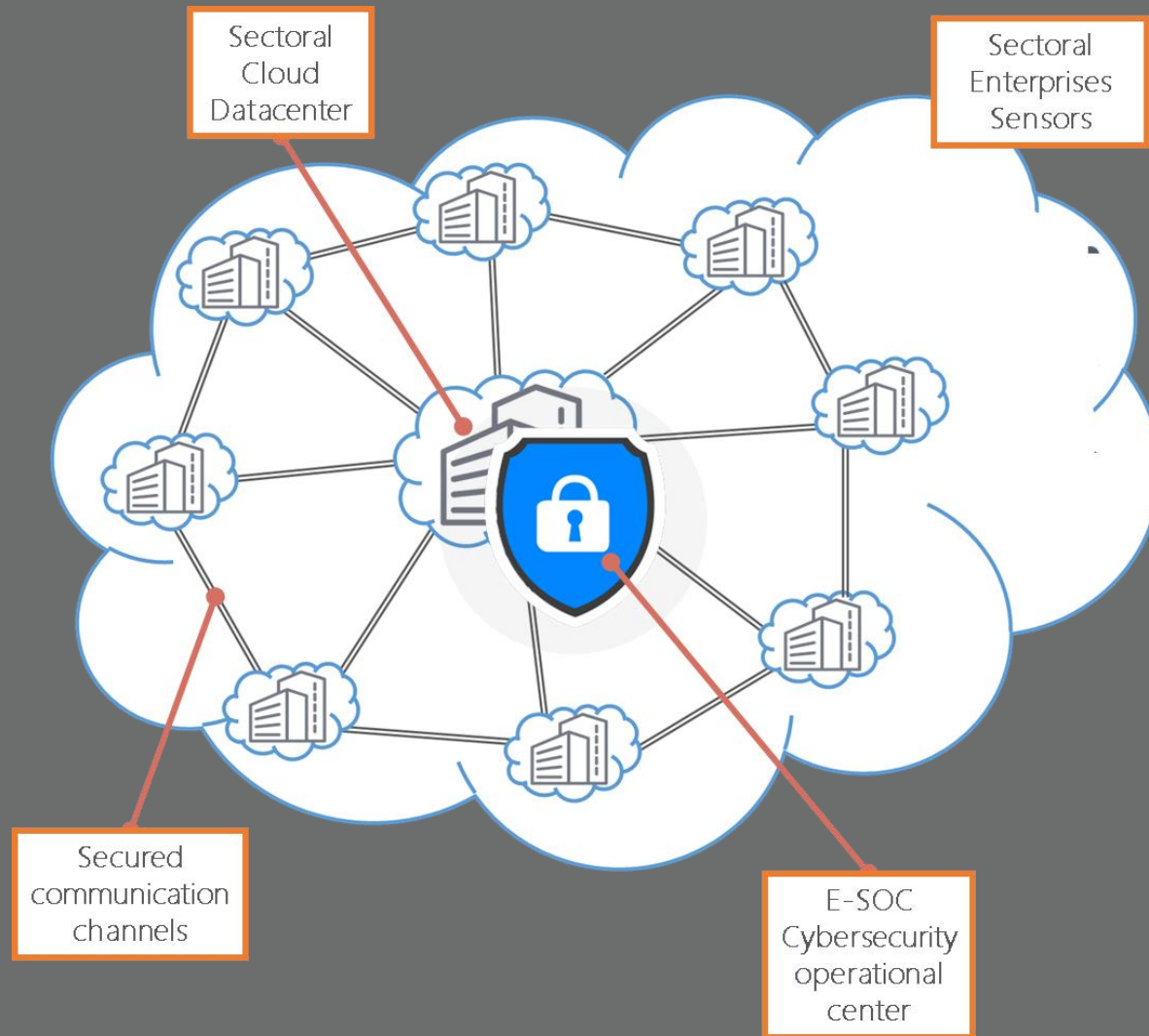
Education and cyber hygiene



© National Center for Cyberdefense
The State Service for Special
Communications and Information
Protection of Ukraine

E-CYBER ROADMAP

E-SOC – SECTORAL CYBERSECURITY CENTER



E-CYBER ROADMAP

CYBER HYGIENE AWARENESS



Згідно зі звітом IBM за 2018 рік, людський фактор - причина

90%
випадків зламу баз даних

КУРС ПРОВОДИТЬСЯ НА ОСНОВІ МЕТОДОЛОГІЇ НАВЧАННЯ ДОРΟΣЛИХ



Адаптовано для учасників виборчого процесу

Орієнтовна тривалість:

4
години



ПРИЧИНИ, З ОГЛЯДУ НА ЯКІ

ПИТАННЯ КІБЕРГІГІЄНИ

МАЄ БУТИ ПРІОРИТЕТНИМ ДЛЯ ВАШОЇ ОРГАНІЗАЦІЇ

ВСТУП ДО КІБЕРГІГІЄНИ - це інтерактивний навчальний курс, спрямований на підвищення рівня обізнаності з ризиками, пов'язаними з поведінкою в Інтернеті, та вироблення розуміння того, які заходи можуть допомогти захистити користувачів та їхні робочі місця від тих зловмисників, які прагнуть завдати шкоди демократичному процесу. Це стосується як посадовців виборчих комісій, так і представників будь-яких інших організацій, які стикаються з подібними загрозами.

ХТО МАЄ ПРОЙТИ ЦЕЙ КУРС:

- Курс підходить для всіх, хто використовує Інтернет у своїй роботі, чи то вебсайти, чи то електронна пошта, чи соціальні мережі.
- Інформація, що надається протягом курсу, стосується будь-яких пристроїв, в яких є вихід в Інтернет.
- Підходить для слухачів всіх рівнів. Немає вимоги наявності у слухачів попередніх знань з кібербезпеки.

- Реагування на фішингову атаку
- Кращі практики використання паролів
- Резервне копіювання даних та їх безпека
- Оновлення програмного забезпечення та встановлення антивірусу

Про Міжнародну фундацію виборчих систем
З 1994 року Міжнародна фундація виборчих систем (IFES) є міжнародною організацією, що спеціалізується на наданні технічної допомоги та навчання в сфері кібербезпеки виборчого процесу; навчання на основі міжнародних стандартів та кращого досвіду; академічних кіл та посилення громадянської участі; законодавства про вибори та політичне фінансування виборчого процесу; недостатньо представлених груп населення; зв'язків із виборами та політичною системою. Для IFES відвідайте: www.ifes.org/ukraine

КУРС ЗОСЕРЕДЖЕНИЙ НА ТРЬОХ ОСНОВНИХ НАПРЯМКАХ:



Міністерство енергетики та вугільної промисловості України

2 августа · 🌐

Кібербезпека починається з кібергігієни

3 ініціативи державного секретаря Максима... Ещѐ



Legislation & Policy

Operations & Processes

Technology

Education and cyber hygiene



Ця ініціатива стала можливою завдяки підтримці Агентства Сполучених Штатів з питань міжнародного розвитку (USAID) та уряду Великої Британії. Дякуємо за підтримку та спонсорство USAID, уряду Сполучених Штатів або уряду Великої Британії.

SCOPE OF WORK



RESULTS

Cybersecurity Coordination Office

Audit of Sectoral Cybersecurity

Cyber Hygiene Awareness

E-SOC – Sectoral Cybersecurity Center

**WE NEED
YOUR
SUPPORT**

12 month

Legislation & Policy

12 month

Operations & Processes

36 month

Technology

~

Education and cyber hygiene



Міністерство
енергетики
України

ЗАСІДАННЯ

**РОБОЧОЇ ГРУПИ З ПИТАНЬ РОЗБУДОВИ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
ЕНЕРГЕТИЧНОЇ ГАЛУЗІ**

МІНІСТЕРСТВА ЕНЕРГЕТИКИ УКРАЇНИ

ІЗ

СВІТОВИМИ ВИРОБНИКАМИ - ЛІДЕРАМИ В СФЕРІ КІБЕРБЕЗПЕКИ ТА ЦИФРОВИХ ТРАНСФОРМАЦІЙ

**24-25 вересня 2020 року
м. Одеса, Україна**