



Кібербезпека ЄС: генеза та сучасний стан

CIA triad

Confidentiality

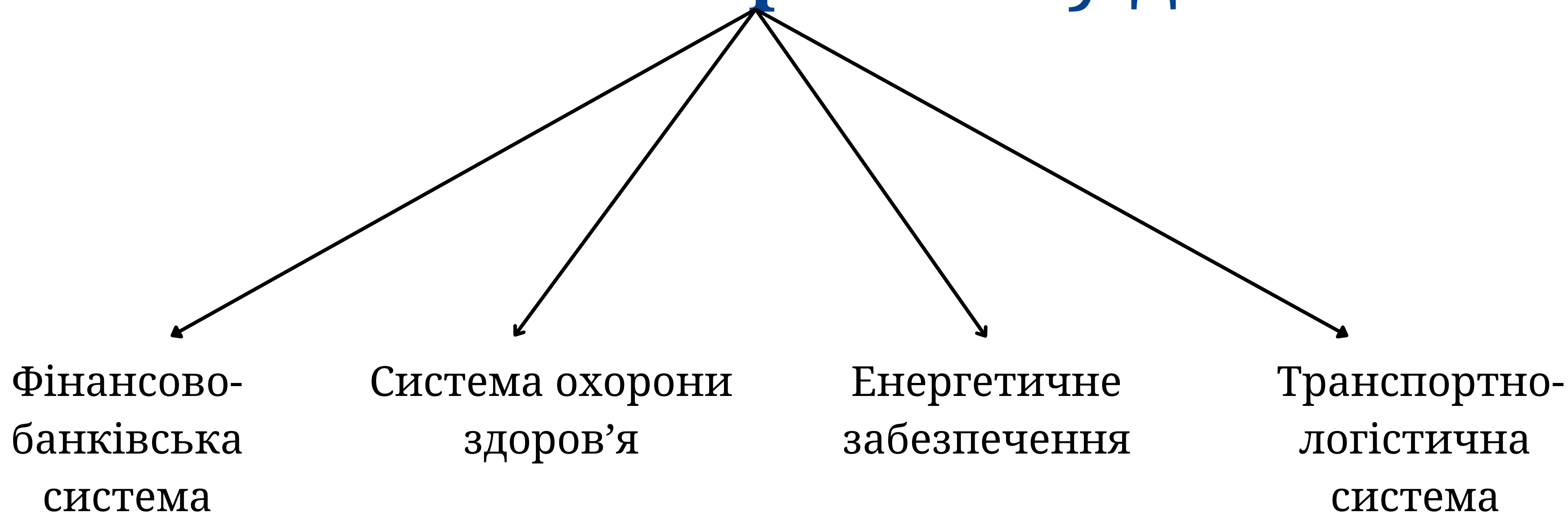
Integrity

Availability

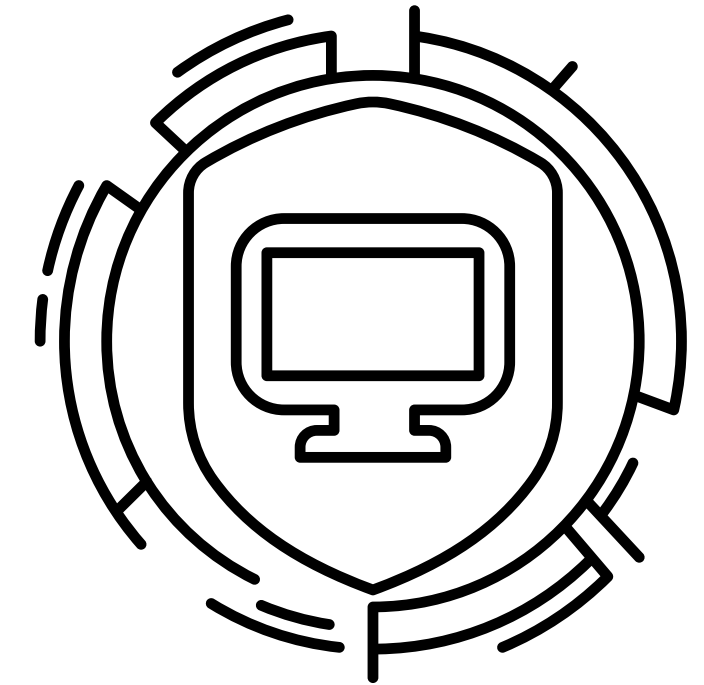
ICONS: JANE KELLY/ADOBE STOCK
©2021 TECHTARGET. ALL RIGHTS RESERVED



Важливість кіберзахисту для ЄС:



Ключові цілі Європейської Комісії (ЄК) у політиці кібербезпеки:



1. Зробити ЄС більш потужним гравцем у сфері кібербезпеки на міжнародному та світовому рівні.

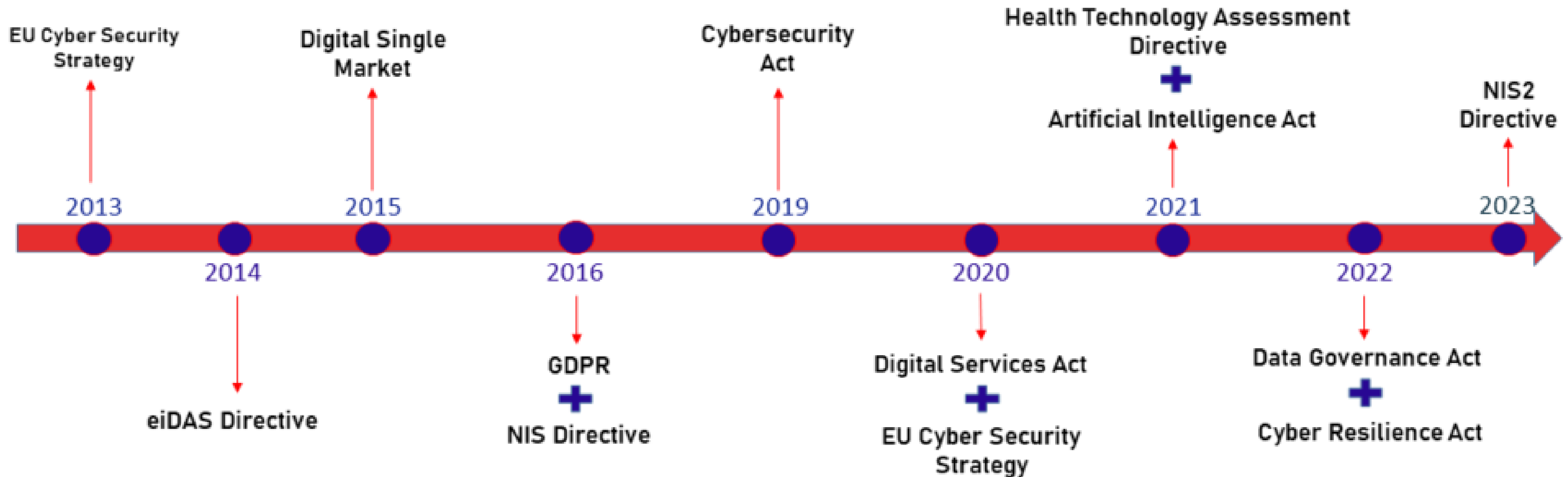
2. Інтеграція кібербезпеки до спільної політики безпеки та оборони ЄС.

3. Підвищення можливостей ЄС у сфері кібербезпеки та обміну інформацією між країнами-членами Європейського Союзу.



European
Commission





Формування нормативно-правової бази політики кібербезпеки ЄС:



Стратегія кібербезпеки ЄС | EU Cyber Security (2013)



П'ять основних пріоритетів Стратегії Кібербезпеки ЄС (2013):

- Підвищення кіберстійкості.
- Скорочення кібер-злочинної діяльності.
- Розробка політики ЄС щодо кіберзахисту та поглиблення можливостей до посилення спільної політики безпеки та оборони ЄС (CSDP).
- Розвиток промислових і технологічних ресурсів для посилення й забезпечення кібербезпеки ЄС.
- Створення узгодженої політики між країнами-членами ЄС в кіберпросторі і просування основних цінностей ЄС на міжнародному рівні.



Стратегія кібербезпеки ЄС | The EU's Cybersecurity Strategy for the Digital Decade (2020)



- Посилення лідерства у сфері міжнародних норм і стандартів у кіберпросторі.
- Захист європейських цінностей і прав у кіберпросторі.
- Збільшення рівня кіберстійкості критично важливих державних і приватних секторів.
- Залучення штучного інтелекту до архітектури європейської кібербезпеки



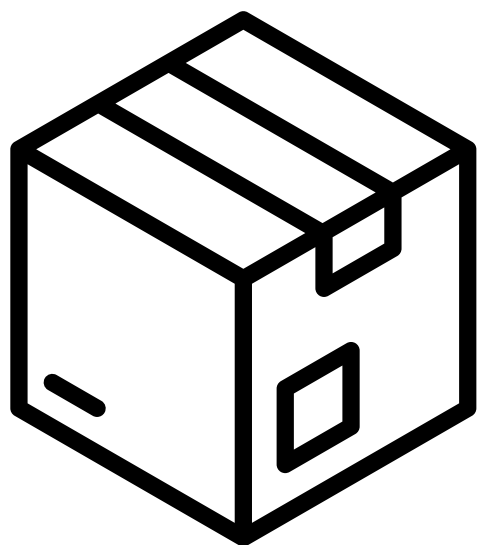


СТРУКТУРА ЄВРОПЕЙСЬКОЇ КІБЕРБЕЗПЕКИ



CSA

Cybersecurity Act



- Продукти та послуги в інформаційно-технологічному секторі

DORA

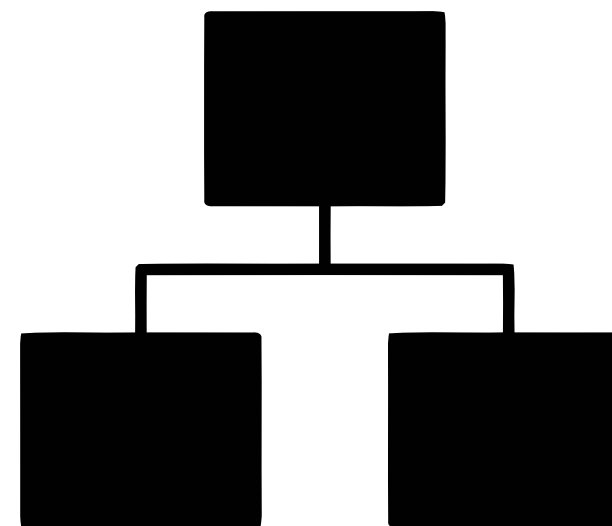
Digital Operational
Resilience Act



- Робота фінансових інституцій

CRA

Cyber Resilience Act



- B2B
- B2C
- Software
- Hardware

CER & NIS2

Critical Entities
Resilience Directive

Network and
Information Systems
Directive



- Організації, що працюють в критичних секторах

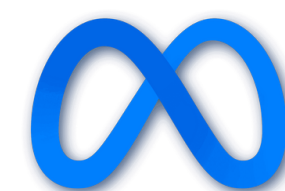


DMA

Digital Market Act

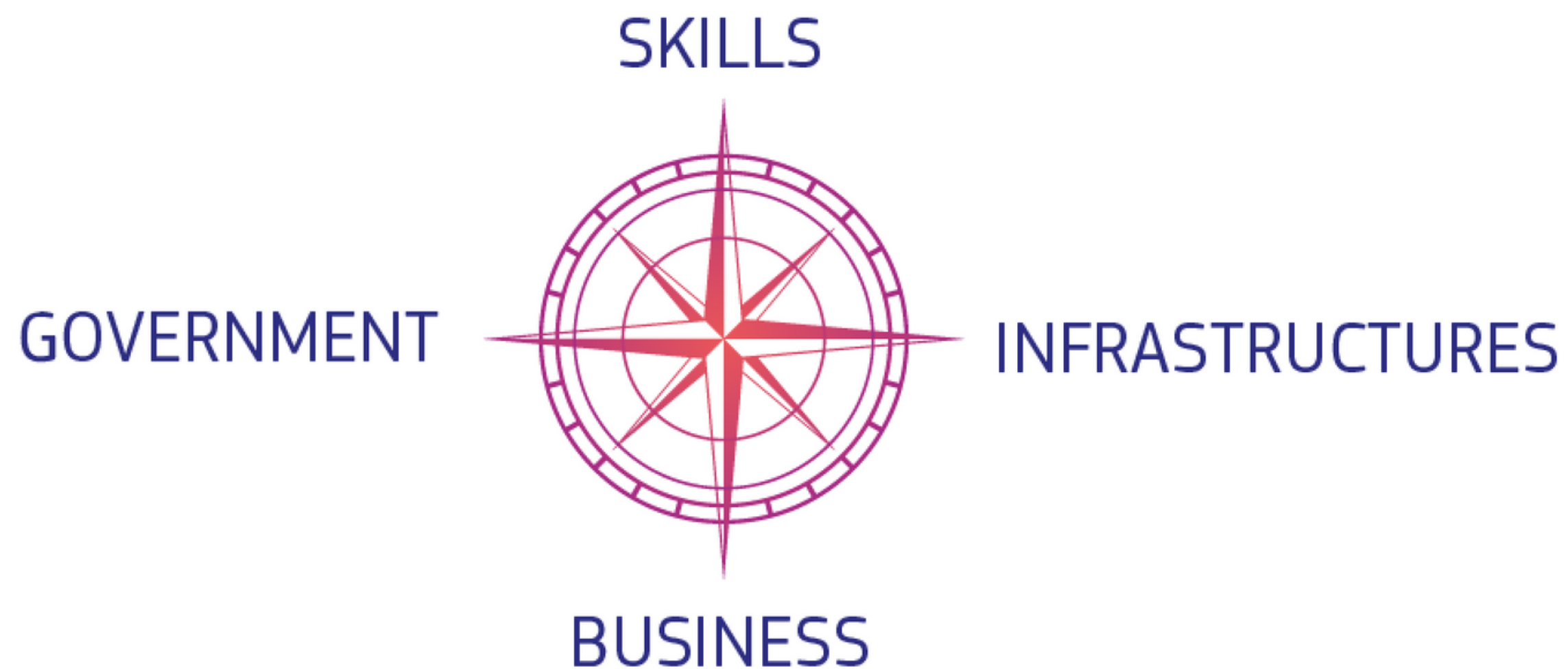


Акт спрямований на те, щоб зробити ринки в цифровому секторі більш справедливими та конкурентоспроможними. Для цього DMA встановлює набір чітко визначених об'єктивних критеріїв для ідентифікації «гейткіперів».

 Meta

Alphabet







People at the centre

Digital technologies should protect **people's rights, support democracy, and ensure that all digital players act responsibly and safely**. The EU promotes these values across the world.



Freedom of choice

People should benefit from a **fair online environment, be safe from illegal and harmful content**, and be empowered when they interact with new and evolving technologies like artificial intelligence.



Safety and security

The digital environment should be **safe and secure**. All users, from childhood to old age, should be empowered and protected.



Solidarity and inclusion

Technology should **unite, not divide, people**. Everyone should have access to the internet, to digital skills, to digital public services and to fair working conditions.



Participation

Citizens should be able to **engage in the democratic process at all levels and have control over their own data**.



Sustainability

Digital devices should support sustainability and the **green transition**. People need to know about the environmental impact and energy consumption of their devices.



Заснування Європейського агентства мережевої та інформаційної безпеки (ENISA) було затверджено 10 березня 2004 р. регламентом № 460/2004 Європейського парламенту.

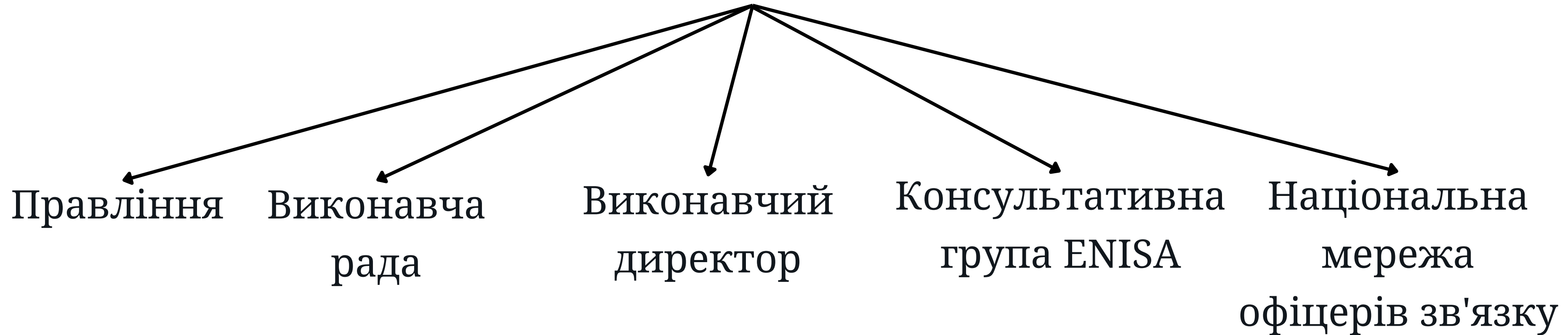
- Штаб: Афіни, Греція



Структура та організація ENISA передбачена регламентом 2019/881 Європейського парламенту від **17 квітня 2019 року**.



АДМІНІСТРАТИВНА ТА УПРАВЛІНСЬКА СТРУКТУРА ENISA



МЕРЕЖІ | ОРГАНІЗАЦІЇ:



The EU Computer Emergency Response Team (CERT-EU) було створено в 2012 році з метою надання ефективної та дієвої реакції, що полягає в здійсненні ефективної протидії можливим інцидентам та кібер-загрозам у кібер-просторі ЄС.

The Europol's Cybercrime Centre (ECC) був створений у 2013 році як невід'ємна частина Європолу та став координаційним центром з запобігання транскордонної кіберзлочинності.



Social engineering threats

Threats that attempt to exploit a human error or human behaviour to gain access to information or services.

82% of data breaches involved a human element.



Threats against data

Attacks to gain unauthorised access to data and to manipulate data to interfere with the behaviour of systems.

Servers were the assets most often targeted by an attack (almost 90%).



Internet threats

Attacks with an impact on the availability of the internet. For example BGP (Border Gateway Protocol) hijacking.

As of June 2022, 15% of the internet infrastructure in Ukraine has been destroyed by Russia.

Top cyber threats in the EU



Ransomware attacks

Attacks where cybercriminals take control of a target's asset and demand a ransom to restore its availability.

60% of affected organisations may have paid ransom demands.

Distributed denial-of-service (DDoS) threats

Attacks preventing users of a network or a system from accessing relevant information, services and other resources.

July 2022 saw the largest ever recorded attack against a European customer.



Malware

Malicious software designed to damage, disrupt or gain unauthorised access to a device.

In June 2022 alone, adware trojans were downloaded around 10 million times.



Disinformation – misinformation

An intentional attack that consists of creating or sharing false and misleading information to manipulate public opinion.

Mass disinformation campaigns were already targeting Ukraine before Russia launched its invasion.



Supply-chain attacks

An attack strategy targeting an organisation through vulnerabilities in its supply chain with the potential to induce cascading effects.

Supply chain incidents accounted for 17% of intrusions in 2021 compared to less than 1% in 2020.





Тік-Ток як провідна кіберзагроза Європейського Союзу та Заходу:

У лютому 2023 року Європейська комісія постановила рішення для співробітників, що вимагало видалення ТікТок-у зі своїх телефонів і корпоративних пристроїв.

Слідом за Європою уряд Канади оголосив про заборону соц-мережі на телефонах державних співробітників.

"Я підозрюю, що коли уряд робить важливий крок, повідомляючи всім федеральним службовцям, що вони більше не можуть використовувати ТікТок на своїх робочих телефонах, багато канадців, від бізнесменів до приватних осіб, мають замислитись про безпеку персональних даних", - прем'єр Міністр Джастін Трюдо.



ВИСНОВКИ:

1. В останнє десятиліття ЄС почав активне вивчення можливостей з використання кібер-простору та запустив ґрунтовні механізми забезпечення кібер-безпеки серед країн-членів ЄС і провідних європейських інституцій.
2. ЄС володіє широкою нормативно-правовою базою, яка регулює питання кібербезпеки, загалом ЄС визначає кібер-безпеку та стабільність у цьому просторі як стратегічно важливий напрямок розвитку ЄС.
3. Визначення кібер-загроз для ЄС є важливим чинником, що впливає на формування спільної політики безпеки та оборони ЄС.
4. Кібер-політика ЄС націлена на сприяння розвитку малого бізнесу та демонополізацію ринку у сфері ІТ.