



**PROBLEMS AND PROSPECTS OF IMPLEMENTING
ASSESSMENT OF THE LEVEL OF MATURITY OF
CYBER SECURITY PROCESSES OF CRITICAL
INFRASTRUCTURE OBJECTS OF THE ENERGY
SECTOR OF UKRAINE IN ACCORDANCE WITH
THE NIST CYBERSECURITY FRAMEWORK**

Chaikin M.M.

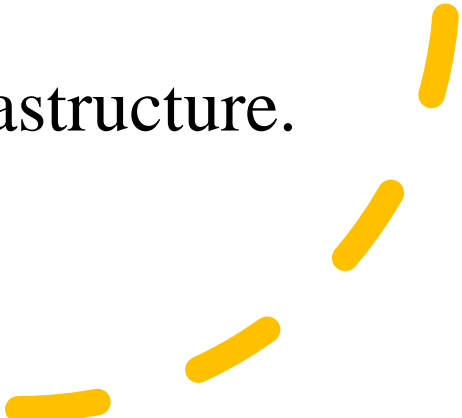
PhD student

G.E. Pukhov Institute for Modelling in Energy Engineering

National Academy of Sciences of Ukraine

A large orange circle is positioned on the left side of the slide, partially cut off by the edge.

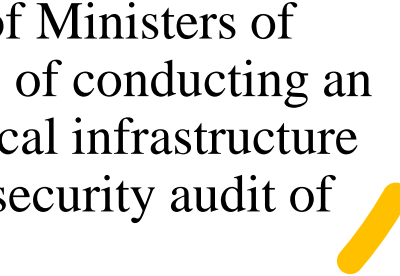
Ukrainian legal documentation

- Law of Ukraine On the Basic Principles of Cybersecurity in Ukraine;
 - Law of Ukraine On information protection in information and communication systems;
 - Resolution of the Cabinet of Ministers of Ukraine On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects;
 - Law of Ukraine On Critical Infrastructure.
- 
- A series of yellow dashed lines are located in the bottom right corner of the slide, forming a curved shape.

Governing body in matters of critical infrastructure

In 2021, the Administration of the State Service for Special Communications and Information Protection of Ukraine published Order No. 601 dated October 6, 2021, containing "Methodical recommendations on increasing the level of cyber protection of critical information infrastructure"[6]. Changes to this order, which were approved by the orders of the State Special Communications Administration dated 12.10.2021 No. 616 and dated 10.07, were published later. 2022 No. 343. These recommendations are developed taking into account the Framework for Improving Critical Infrastructure Cybersecurity issued in 2014 and updated in 2018 by the National Institute of Standards and Technology of the United States of America (NIST Cybersecurity Framework - NIST CSF).

As a next step, on March 24, 2023, the Cabinet of Ministers of Ukraine adopted the Resolution on "Some issues of conducting an independent audit of information security at critical infrastructure facilities", which introduced a mandatory cyber security audit of critical infrastructure facilities every 2 or 3 years



3 different ways to confirm compliance with cyber security

Construction of a comprehensive information protection system with confirmed compliance (KSZI);

Building an information security management system (ISMS);

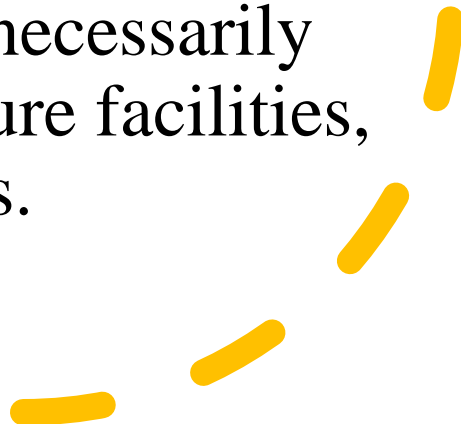
Audit for compliance with NIST CSF requirements and re-audit following implementation of recommendations.

New cybersecurity regulation in energy- sector in EU

In January 2022, the European Network of Transmission System Operators for Electricity (ENTSO-E) announced the details of its new cybersecurity code. The Network Code on Cybersecurity (NCCS) is the first network code that will be developed according to the new rules established by the European Union on the internal market for electricity and is expected to enter into force by January 2024. The network code aims to set a European standard for the cybersecurity of cross-border electricity flows. It focuses on improving cybersecurity resilience through the enhancement of threat detection and incident reporting and proposes various measures to improve cybersecurity resilience that are essential to preserving the continuity of the services. On January 14, 2022, the preparation of the draft document was completed.

Resolution No. 518 of the Cabinet of Ministers of Ukraine

State Service for Special Communications and Information Protection of Ukraine and the Cabinet of Ministers of Ukraine, with the active help of international partners, are working on updating Resolution No. 518 of the Cabinet of Ministers of Ukraine dated June 19, 2019 "On the approval of General requirements for cyber protection of critical infrastructure objects", which will lead to the acquisition of NIST CSF status is necessarily the standard for critical infrastructure facilities, instead of a recommendation status.



A large orange circle is positioned on the left side of the slide, partially cut off by the edge. It serves as a background for the title text.

New challenges for Ukraine by NIST CSF

The need to train specialists in audit and implementation of NIST;

Determining the priority of the requirements for building a cyber protection system in the energy industry;

The need for simultaneous harmonization of the regulatory framework with US and EU requirements at the same time



Thank you for
attention!