
# Ukraine-U.S. cooperation in cybersecurity area reaches a new level

News

28.07.2022 08:55

The SSSCIP has signed a Memorandum of Cooperation with the Cybersecurity and Infrastructure Security Agency (CISA) under the United States Department of Homeland Security.

Deepening cybersecurity collaboration with our American partners is another important step towards the integration of Ukrainian cyber defenders into the global expert environment. The U.S. and Ukraine are the two countries upon which the greatest number of cyberattacks has been waged. This is why sharing our experience and joining our efforts in resisting cyber aggression would help both countries protect their information resources more efficiently.

“This memorandum of cooperation represents an enduring partnership and alignment in defending our shared values through increased real-time information sharing across agencies and critical sectors and committed collaboration in cultivating a resilient partnership,” said Mr. Oleksandr Potii, Deputy Chairman, SSSCIP.

CISA Director Jen Easterly pointed out that the signed document would deepen CISA cybersecurity collaboration with its Ukrainian partners. “I applaud Ukraine’s heroic efforts to defend its nation against unprecedented russian cyber aggression and have been incredibly moved by the resiliency and bravery of the Ukrainian people throughout this unprovoked war. Cyber threats cross borders and oceans, and so we look forward to building on our existing relationship with SSSCIP to share information and collectively build global resilience against cyber threats.”

The key areas of collaboration between the two cybersecurity agencies will be:

- studying methodology and practices of the U.S. critical infrastructure security,
- cooperation in cyber threat indicators, protective actions and information regarding cybersecurity risks and incidents,
- information exchanges and sharing of best practices on cyber incidents to enhance relevant incident management systems, response systems and post-incident recovery systems by establishing bilateral information exchange channels between the parties to identify and respond to threats in cyberspace,
- understanding how both parties cooperate with the private sector in the cybersecurity area,
- sharing of best practices and participation in cybersecurity through studies, training and joint exercises,
- implementation of joint cybersecurity projects.