One of the key problems of Ukrainian internal cyber-market performance and integration with the EU markets is the lack of a single centre of competence and trust. This is especially relevant for consumers of goods and services not capable of assessing the competence and reliability of different “sellers” in this market. Respectively, incompetent and dishonest players remain in the market damaging other players’ reputation and reducing the level of trust in the industry as a whole.

The root cause of this is systemic distrust among cybersecurity goods and services market players, although most of them are ready to form a professional association, and many have stressed the need for such an association for the entire market.

One of the most notable problems is an inconsistent state policy aimed to protection of the national interests of Ukraine in cyberspace. There is neither clear agreement nor common vision of the national cybersecurity development options among the cybersecurity system principals.

The current Ukrainian national cyber-legislation is outdated and poorly correlated with modern cyber-threats and challenges landscape.

The issue of personal data protection is one of the most alerting in Ukraine in 2021.
This domain has been virtually removed from urgent task list; there is no effective protection of citizens’ personal data but only simulation of such.

The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and GDPR require establishing a national-scale independent competent authority responsible for personal data protection. Forming such an authority in Ukraine is an urgent need and priority task on the way to a comprehensive resolution of information and cybersecurity problems.

Ukrainian legislation does not prevent interference in the Internet operation, nor does it protect the rights of citizens to free access to information on the Internet and freedom of lawful information dissemination.

The measures taken by the Ukrainian authorities to improve national cybersecurity, as well as current international assistance programmes in this area are hardly effective. Thus, it is appropriate to focus the efforts of international donors and supporters of Ukraine on improving the national cybersecurity system foundation, i.e. building trust among stakeholders, with maximum involvement of the expert community and Ukrainian cyber business.

Building trust among all key stakeholders in the Ukrainian cybersecurity sector within the framework of a new project funded by a group of international donors will become the first developmental milestone in creating a working prototype of the national cybersecurity model for Ukraine.

The project support by all key stakeholders and their vote of confidence can be used to establish effective interaction within the country, in

particular, to build a working prototype of the National incident information exchange hub.

The working prototype of the incident information exchange hub could provide a blueprint for an effective national cybersecurity system in all economy domains (including critical infrastructure). Such a system would significantly improve the cybersecurity in Ukraine and accelerate the country's integration into the DSM.