

XII Ukrainian Internet Governance Forum

IGF-UA

IV Youth IGF-UA

Kyiv, 28, 11-12 November 2021
Annual Report

CONTENT

Introduction	1
Organizational process	2
Agenda	3
Participants	4
Financing	4
Conclusions	5
Report on the preparation and holding of the Fourth Ukrainian Youth Internet Governance Forum.....	13
Contacts	17

INTRODUCTION

The first Ukrainian Internet Governance Forum (IGF-UA) took place in September 2010 in Kyiv. Since then, the annual IGF-UA has become a continuation of a global series of Forums aimed at discussion of the most important issues of information society development, consolidation of the efforts of state authorities, business, Internet society, professional and academic elites aimed at accelerating the implementation of IT capabilities, creating conditions for comprehensive development of Internet technologies for the public benefit. IGF-UA always gathers together participants from around the world who represent international organizations, state authorities, non-governmental and commercial organizations in the field of ICT and the mass media.

The Twelfth Ukrainian Internet Governance Forum IGF-UA was held on November 11-12, 2021 via video conference. **The fourth IGF-UA Youth Internet Forum** took place on November 10 via video conference.

The 12th IGF-UA was attended by participants from Ukraine and other European countries representing state authorities, international organizations, the private sector, civil society, academic and technical communities, and the mass media.

IGF-UA continues to be an important component of the national discussion on the future of the Internet in Ukraine.

ORGANIZATIONAL PROCESS

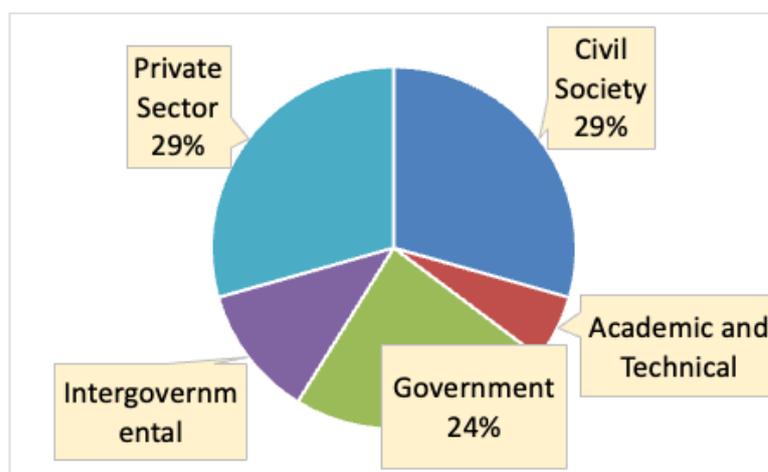
The activities of the IGF-UA Organizing Committee are based on the "Guidelines for Holding the Ukrainian Internet Governance Forum IGF-UA (Memorandum of Understanding)". This document was developed to implement the decisions made during the 4th IGF-UA.

"Guidelines for the Ukrainian Internet Governance Forum IGF-UA (Memorandum of Understanding)": <http://igf-ua.org/docs/Principles.doc>.

All representatives of the Internet community, who came up with a proposal on the inclusion of his/her candidacy into the Organizing Committee and agreed with the "Guidelines...» were elected to the Organizing Committee. Thus, the Organizing Committee included 17 people who in a balanced manner represented various stakeholder groups: state authorities, international organizations, the private sector, civil society, scientific and technical communities.

Members of the IGF-UA Organizing Committee

	Name	Organisation	Stakeholder group
1.	Mikhail Anisimov	ICANN	International organizations
2.	Oleksandr Arutiunian	The Ukrainian Internet Association	Private sector
3.	Oleksandr Baranov	State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine".	The academic and technical community
4.	Volodymyr Zvieriev	The National Security and Defense Council of Ukraine	Government organizations
5.	Yurii Kargaplov	NGO "ISOC Chapter Ukraine"	Private sector
6.	Dmytro Kohmanyuk	Independent Expert	Private sector
7.	Volodymyr Kukovskyi	Secretary of the Organizing Committee	Civil society
8.	Yurii Matsyk	Ministry of Digital Transformation of Ukraine	Government organizations
9.	Vitalii Moroz	NGO "Internews-Ukraine"	Civil society
10.	Ivan Pietukhov	Commission on Science and IT of the Ukrainian League of Industrialists and Entrepreneurs (ULIE)	Private sector
11.	Oksana Prykhodko	European Media Platform	Civil society
12.	Andrii Semenchenko	National Commission for the State Regulation of Communications and Informatization	Government organizations
13.	Oleksii Semeniaka	RIPE NCC	International organizations
14.	Yurii Smielianskyi	Public Association Commission on Science and Information Technology	Civil society
15.	Svitlana Tkachenko	Hostmaster Ltd	Private sector
16.	Anastasia Tkachuk	Independent expert, representative of the IGF-UA Youth Community	Civil society
17.	Ihor Cherniak	Security Service of Ukraine	Government organizations



Participation of representatives of various stakeholder groups in the IGF-UA Organizing Committee

The IGF-UA Organizing Committee had been working not only during the actual preparation of the IGF events but throughout the period between the 11th and 12th IGF-UA. During this period, seven meetings of the Organizing Committee took place – on 17.08.2021, 06.09.2021, 21.09.2021, 04.10.2021, 19.10.2021, 27.10.2021, 03.11.2021 (<http://igf-ua.org>).

The Organizing Committee has appointed the list of five Organizers of IGF-UA: The Ukrainian Internet Association (UIA), Commission on Science and IT of the Ukrainian League of Industrialists and Entrepreneurs, RIPE NCC (RIPE Network Coordination Centre), NGO "Internews-Ukraine", and Hostmeister LLC. Three organizations have sponsored IGF-UA: Internet Corporation for Assigned Names and Numbers (ICANN), IGF Supporting Association (IGFSA), and Internet Society.

The forum was supported by the Ministry of Digital Transformation of Ukraine, the National Commission for State Regulation of Communications and Informatization, the Office of the National Security and Defense Council of Ukraine, and the International NGO European Media Platform.

Among the organizers of the IGF-UA and the organizations that supported the Forum, various stakeholders are represented in a balanced manner:

- Civil Society/Private Sector: The Ukrainian Internet Association, Commission on Science and IT of the Ukrainian League of Industrialists and Entrepreneurs;
- Civil society: NGO "Internews-Ukraine", International NGO "European Media Platform";
- Private sector: RIPE Network Coordination Centre; Hostmaster LLC;
- Governmental organizations: Ministry of Digital Transformation of Ukraine, National Commission for State Regulation of Communications and Informatization, Office of the National Security and Defense Council of Ukraine;
- International organizations: Internet Society, IGF Supporting Association (IGFSA), Internet Corporation for Assigned Names and Numbers (ICANN).

Media partners were as follows: I-UA.tv – general information sponsor; Interfax-Ukraine – general media partner; HB – a media partner.

AGENDA

The main goal of IGF-UA is to develop Internet governance in Ukraine through multilateral dialogue, as well as to promote partnerships aimed at coordinating stakeholders for the best and most balanced development of the Internet for the benefit of Ukrainian citizens. Based on this goal, the Organizing Committee identified a list of main topics for discussion at the IGF-UA. 11 sections for discussions and debates were formed based thereon.

Section No1. Cybersecurity and Human Rights in Ukraine. Cybersecurity Standards.

Section No 2. Internet Freedom and Digital Rights.

Section No 3. Emerging Technologies and Artificial Intelligence.

Section No 4. Cyber-Secure Cities, Smart Cities.

Section No 5. Internet of Things and Security Issues.

Section No 6. Trends in the Internet Governance Development.

Section No 7. Telecommunications Infrastructure; Introduction of the Law on Electronic Communications.

Section No 8. Stakeholders of Ukraine's Integration into the Digital Single Market (Users Role).

Section No 9. Covid-19 and Digital Transformation.

Section No 10. The Impact of Policy on the Internet and Internet Technical Solutions.

Section No 11. Internet Standards: Where They Come from, Who Creates, How They Work, Whether Ukraine Participates in the Development of Standards.

The results of the Forum were summed up at the **Final Plenary Session**. *The full version of the programme of the 12th IGF-UA is available at: <http://igf-ua.org/programa-igf-ua-2021>.*

PARTICIPANTS

The Forum was attended by a significant number of participants from Ukraine and other European countries representing state authorities, international organizations, the private sector, civil society, the academic and technical community, the mass communication media and the youth.

As the forum was held via video conference, everyone could participate therein without registration. Participants had the opportunity to provide their feedback via chat and e-mail.

FINANCING

Following the Guidelines of the Ukrainian Internet Governance Forum IGF-UA (Memorandum of Understanding), the necessary resources in terms of the preparation and conduct of the Forum were provided by the Organizers and Sponsors of IGF-UA.

Exchange Rates 10.2021	Organizer/ Sponsor	Balance from 2020 (including the exchange rate ratio 10.2020/ 10.2021)	Proceeds in 2021			Expenses in 2021		Balance	
			Responsible	currency	UAH	Items of expenses	Amounts, UAH		
30,47 ₴	RIPE NCC (2019)	16 522,49 ₴	Prykhodko			Development of the National IGF-UA website	30 000,00 ₴	0,00 ₴	
	IGF-SA (2019)	48,80 ₴	Prykhodko			Development of the Youth IGF-UA website	30 000,00 ₴		
	IGF-SA (2020)	52 014,60 ₴	Prykhodko			Settlement and cash services	2 450,00 ₴		
26,27 ₴	IGF-SA (2020)	52 014,60 ₴	Prykhodko			Development of the Youth IGF-UA logo	3 150,00 ₴		
	ICANN (2019)	4 986,61 ₴	Kargapolov			Promotion of IGF-UA and Youth IGF-UA	2 985,89 ₴	0,00 ₴	
	RIPE NCC (2021)		Prykhodko	750,00 €	22 852,50 ₴	Settlement and cash services	4 986,61 ₴		
	ICANN (2021)		Tkachenko	\$1 500,00	40 290,00 ₴	Translation of the IGF-UA report	2 027,50 ₴	9 205,00 ₴	
26,86 ₴	Hostmaster Ltd (2021)		Tkachenko		13 710,00 ₴	Simultaneous translation	3 370,00 ₴		
	Commission of ULIE (2021)		Pietukhov		6 000,00 ₴	Providing and supporting an online platform	8 250,00 ₴	0,00 ₴	
	l-ua.tv		Pietukhov		30 000,00 ₴	Organization and provision of 2 broadcast channels (stream)	54 000,00 ₴	0,00 ₴	
	Internet Society (2021)		Prykhodko	\$1 000,00	26 270,00 ₴		0,00 ₴	\$1 000,00	
	RIPE NCC (2021)		Kargapolov	983,06 €	29 953,84 ₴		0,00 ₴	983,06 €	
Balance 2019-2020:		73 572,50 ₴	Proceeds 2021:			169 076,34 ₴	Amounts 2021:	177 220,00 ₴	
							Balance на 2022:	65 428,84 ₴	

By its decision, the Organizing Committee approved the formation of a unified budget of the IGF-UA and the Youth IGF-UA, including fundraising and spending.

According to the decision of the Organizing Committee, the remaining balance will be used to hold IGF-UA events in Ukraine in 2022.

CONCLUSIONS

The final statements were made by the panel moderators at the final discussion panel. The emphasis was made on the fruitfulness of the discussions, the importance of implementing international experience in Ukraine and the role of the 11th IGF-UA discussions in further improving the Internet governance.

Section 1. "CYBER SECURITY AND HUMAN RIGHTS IN UKRAINE. CYBER SECURITY STANDARDS"

Moderator: I. Pietukhov (UUIE), co-moderator: O. Semeniaka (RIPE NCC).

Participants of the section summarized the answers to a range of topical issues in this area:

1. There is a problem of proper understanding of key concepts in the field of cybersecurity, their proper delineation and correlation, which is critical for creating an effective mechanism for counteracting threats in cyberspace, as well as an effective mechanism for legal support in this area.

It is required to:

- develop clearly defined regulatory documents;
- determine which organizational, legal, technical, educational activities should be carried out by responsible entities;
- add security measures to the practical measures to ensure human cybersecurity, and provide a relevant definition thereof.

2. The role of cybersecurity standards in ensuring cybersecurity is extremely important. At the national level, it is necessary to constantly analyze and summarize the experience of such institutions as ITU, ISO / IEC, NIST.

It is necessary to:

- Develop and adopt the national standards in the field based on international and regional ones.
- Implement and adapt the standards of the member states of the relevant standardization organizations with which relevant international agreements are concluded

3. Choosing a model for building a security system in cyberspace, the current Ukrainian government has chosen the wrong Russian way: providing security for the government itself.

Identified threats and risks:

- The part of individual freedom to be ceded as payment for protection against threats from cyberspace is not defined.
- The price of "refusal from freedom" to achieve security from such threats poses additional threats to social and political and social and economic instability and, as a consequence, additional threats to Ukraine's national security.
- The level of security of citizens that the state can guarantee has never been identified.

Therefore, it is impossible to determine the adequacy of the price of "refusal from freedom" concerning the level of security guaranteed by the authorities from the threats arising from cyberspace.

It is recommended for the Ukrainian government to abandon the erroneous and dangerous "Russian" way of forming a security system in cyberspace.

4. The authors of the Law of Ukraine "On Electronic Communications" define the security of networks and services. However, in addition to defining the concept of "security of networks and services", the Law of Ukraine "On Electronic Communications" does not contain criteria (methodology) for defining "security of service in the field of electronic communications".

It is required to approve at the legislative level the following:

- clear, understandable and measurable criteria for the security of electronic communications services.
- the basic principle of work on the Internet, namely the principle of openness.

5. When considering the issue "Risks and threats to the security of critical infrastructure in the information space of Ukraine" the main features of critical infrastructure and information security, as well as practical issues, were considered.

The big risks posed by the draft Law on Critical Infrastructure No. 5219 dated March 9, 2021, were indicated.

The participants of the section suggested that the deputies of the Verkhovna Rada refrain from violating the constitutional rights of citizens and private property.

Section 2. **"FREEDOM OF THE INTERNET AND DIGITAL RIGHTS"**

The section was moderated by Vitalii Moroz, attended by Vita Volodovska, Director of the Digital Security Lab, Gulsanna Mamedieva, Director of the Directorate for European Integration of the Ministry of Digital Transformation of Ukraine and Ihor Rozkladai, Deputy Director, Chief Expert in Media Law of CEDEM (the Centre for Democracy and Rule of Law).

Key theses/conclusions:

- At present, the concept of "Internet security" has been gradually displacing the idea of "Internet freedom" as the Internet becomes more fragmented, the countries impose more and more regulations, and this may pose a threat of narrowing of many digital rights, including the right to anonymity.
- A key challenge for the Ukrainian government in the protection of personal data is the implementation of actions and steps to restore the violated rights of users.
- The private sector does not always understand the value of personal data protection, occasionally uses the category of "digital rights", and on providers' websites often instead of privacy policy - only the provision of telecommunications services. At the same time, market leaders are aware of the need to prescribe privacy and personal data protection policies.
- The effectiveness of personal data protection for government institutions (Government Figures) is not the number of fines imposed, but changes in private sector privacy policies. The government sector is interested in clarifying, working with the private sector, so that companies learn to apply the law correctly.
- The private sector in Ukraine will need to prepare for the implementation of the new law on personal data protection. At the same time, the adoption of the Law on Personal Data Protection contains potential risks for the private sector. First, the lack of time in the private sector to implement new practices. Second, there is a lack of clearly stated definitions in the law regarding company liability and possible sanctions.

Section 3. **“EMERGING TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE”**

The section was moderated by Vitalii Moroz, attended by Tetiana Avdieieva, CEDEM lawyer, Volodymyr Khilchuk, Into-Sana Innovation Manager, COO Lab24.com.ua, Oleksandr Baranov, Doctor of Laws, Head of the Scientific Centre for Digital Transformation and Law of the State Scientific Institution “Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine”.

Key theses/conclusions:

- Changes in society for the introduction of artificial intelligence (AI) will come much sooner than we expect. Models of artificial intelligence can lead us to anti-utopias like Orwell’s or Bradbury’s ones, or vice versa – to the functioning of smart cities meeting the needs of the residents
- There is a high probability of class division in the future related to access to data, non-awareness of the value of this data by users may lead to the deepening of this division. The role of large companies will become more significant.
- AI is widely used worldwide in the field of health care, but for Ukraine AI has not been actively used yet, and there are fewer data. At the same time, start-ups in the IT sector have been rapidly developing, focusing on the use of AI.
- AI certification was one of the key issues during the discussion that is establishing basic safety requirements for the use of technology for humans. Certification can be made in several ways, including that by companies on their own.

Section 4. **“CYBER-SAFE CITIES, SMART CITIES”**

Moderator: Svitlana Tkachenko, Speakers: Olena Hunko, Head of the Information Technology Department of the Lviv City Council; Solomiia Paslavaska, Project Manager of the Ministry of Digital Transformation of Ukraine, Volodymyr Kondziolka, Director of the Drohobych City Institute, Roman Khimich, Expert, Roman Chornenkyi, ELKO Ukraine, Maksym Blagonravin, Hostmaster LLC.

Key theses/conclusions:

- smart cities are built based on the Internet of Things, big data, cloud computing, artificial intelligence, etc., where the Internet becomes their main technology
- application of the concept of smart city and data-based management helps not only to make life more comfortable for the city residents and optimize the management of city infrastructure but also to analyse and reduce inefficient expenditures of the city budget
- it is impossible to ensure equal opportunities and the same level of access to services, cooperation with different departments of the city without increasing digital competence.
- Having a “digital leader” in the community helps to involve stakeholder groups in preparing, adopting and implementing decisions on the use, development and accountability of digital technologies in cities. The task of the relevant ministries is to assist the digital leaders in gaining the necessary knowledge on urban governance and digital transformation.
- The introduction of new technologies carries risks and vulnerabilities in terms of cybersecurity. It is necessary to pay special attention to the safe use of data, to ensure the integrity and quality of basic services, the reliability of information systems.

Section 5. **THE INTERNET OF THINGS AND SECURITY ISSUES**

Moderator: Yu. Kargapolov (ISOC Chapter Ukraine).

The session was attended by Wout de Natris – a world-renowned security expert, Chairman of the Cybercrime Working Group at RIPE NCC, Chairman of the IGF Dynamic Coalition for Internet Standards, Safety and Security; Baranov O.A - Doctor of Law, Head of the Research Centre for Digital Transformations and Law of the Research Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine; Peter Waher – a world-renowned expert in the field of cybersecurity IoT, developer of IoT systems, a consultant on IoT implementation, author of books on IoT; Mark Carvell – a world-renowned Internet Governance expert having extensive experience in the UK, who coordinates UK government support for the IGF and is a member of the IGF Steering Committee, and represents the UK in ITU and other multilateral Internet Governance forums.

The "Internet of Things and Safety Issues" session began with the announcement of participants who are widely known international specialists in the development of IoT technologies and counteracting cybercrimes. A range of issues for discussion was defined. The session was included in the agenda of preparation for holding IGF 2021 in Katowice and was to show the relevant agenda issues, including the work of the DC-ISSS (<https://www.intgovforum.org/multilingual/content/dynamic-Coalition-Tone-InTernet-Standards-Security-and-Safety-DC-ISSS>). Therefore, the issues that were viewed at the session were relevant for the global IGF agenda and included framework aspects, technical, technological, organizational, and procurement aspects of standardization and implementation of BCP.

At first, the sessions covered issues that can be attributed to the Framework in the activities of the DC-ISSS. Wout de Natris spoke about the goals and objectives, as well as the results of the Coalition obtained during the first year. The results of the survey were presented, which characterized the most problematic IoT security issues from the point of view of surveyed professionals around the world and various stakeholders. It is noted that the task of the Coalition is not to develop specific means of countering harmful effects but to determine the directions and trends on which the efforts of various stakeholders and actors should be focused to prevent the occurrence of threats.

Peter Waher spoke about the experience of implementing projects, technical regulation and standardization policies; he pointed out that the practice of responding to unauthorized implementations in the IoT systems falls predominantly on the reactive response to the threats that have already occurred. There are very few means to counteract new threats. A big security issue exists on the task loop of authentication and authorization of access rights to objects of the IoT systems.

Mark Carvell reported about the approach to the creation of regulatory rules, which would enable building a comprehensive system of support for the safe IoT environment. Mark Carvell presented the thesis of "Security by Default" and a set of relevant IoT security actions that must be taken by all stakeholders involved in the provision of IoT security.

One of the proposals that sounded during the discussion was the creation of the National Internet Governance Steering Committee, which would include different actors on the principles of multi-stakeholderism. The decision of such a committee must be made on the principle of consensus. The tasks of such a committee may include the development and implementation of harmonized specific Internet governance policies, learning and adaptation of the best current practices for the application of Internet Governance in the country.

Wout de Natris called on Ukrainian developers and users of the IoT systems to join DC-ISSS, noting that such work will allow being involved in modern trends and enriching the materials being prepared by the Coalition.

Section 6. “TRENDS IN THE DEVELOPMENT OF INTERNET GOVERNANCE”

Moderator: Yu. Kargapolov (ISOC Chapter Ukraine).

The session was attended by: Grigory Saghian – a famous expert in the field of Internet Governance, Vice-Chair of the ISOC Chapter Armenia; Andrii Paziuk – a Doctor of Science, well-known expert and specialist in the field of international information law and communication law, cyber-law, Internet Governance; Valeriia Filinovich – a Doctor in Law, well-known Ukrainian expert in Internet Governance, copyright, industrial property law, Internet law, cybersecurity, information law; Roman Perun – a founder and CEO of the National Operator of Network Slicing "IT-KARKAS", founder of the International IT Forum "IT-KARKAS", All-Ukrainian IT-Forum of the System Administrators

The session included a discussion of the issues that define the architecture of the Internet and the challenges that remain unresolved Internet issues, legal issues of the Internet, new concepts of Internet Governance, issues related to the market access to technical and technological solutions and how they affect organizational and administrative regulatory processes access and development of technologies for access to Internet services.

Grigory Saghian spoke about the experience of implementing Internet Governance principles and policies in Armenia. He informed about the process of establishing a permanent commission on the Internet issues established by the initiative of ISOC Chapter Armenia by the Order of the Cabinet of Ministers. The commission includes various stakeholders, the balance of interests is maintained by delegating a proportionate number of representatives of government agencies, business, academia, etc., and decisions are made by consensus.

Andriy Paziuk spoke about the models of creating a national cybersecurity centre. In the UK, participants include both the large market players and small and medium market members. The state is conducting explanatory work. The policies of such centres, which include business and educational institutions, are not aimed at blocking resources, but rather at developing the content. In Ukraine, the trend is aimed at monopolizing the state's cybersecurity efforts. The best practices of Europe, America, and Asia are that the state implements the model of "cybersecurity as a service", which is based on the described centres. There was a proposal to reflect this concept in the draft law on cybersecurity.

Discussion of such a model on the example of the Petya virus attack showed that such an existing model of countering threats in Ukraine is ineffective and is aimed not at forming mechanisms for developing and operational protection against new threats, but rather at blocking already known ones. Participants noted that after the Petya virus attack, the authorities did not change their approach to countermeasures.

Valeria Filinovich spoke about the protection of personal data and trends that are typical for modern market development.

An analysis of the current situation in the field of personal data protection was provided, in particular, that of the lack of effective legislation in Ukraine to combat the leakage of personal data, abuse and manipulation of personal data; on the inconsistency of Ukrainian norms with the provisions of the GDPR, the lack of the right to trust, clear definitions of the controller and operator of personal data, etc. The trend in the development of the Internet is that the rights of consumers of services should be protected at the national and international levels.

There was a proposal to support the provisions of the draft law on amendments to existing regulations on personal data protection.

Trust's Ecosystem remains the main trend in creating an effective Internet Governance system at the national level.

Roman Perun pointed out that the modern market of Internet services has stopped growing on the one hand, and on the other hand, it is characterized by the lack of breakthrough ideas. Therefore, from the practical side of the Internet operator's work, trends in the field of Internet management are to create mechanisms for new markets and their further development. A practical example is a project of creating an infrastructure operator in the market of services to the final consumer. Experience shows that this may be a new trend in building a system of relationships between operators based on the implementation of win-win strategies. It was emphasized that the creation of such a market will be reflected in the creation of new financial and economic models of relationships with a large number of condominiums.

The participants of the session noted that there is no platform for permanent dialogue between state authorities and the rest of the stakeholders and this is an undesirable trend in the development of the Internet market in Ukraine.

Section 7. "TELECOMMUNICATIONS INFRASTRUCTURE; IMPLEMENTATION OF THE LAW OF UKRAINE ON ELECTRONIC COMMUNICATIONS"

Moderator: O. Harutyunyan (The Ukrainian Internet Association).

The session was attended by: Oleksandr Fedienko (Deputy Chairman of the Verkhovna Rada Committee on Digital Transformation); Andrii Semenchenko (member of the National Commission for the State Regulation of Communications and Informatization); Viktoria Troshchenko (member of the National Commission for the State Regulation of Communications and Informatization); Mykola Tkachenko (member of the National Commission for the State Regulation of Communications and Informatization); Yurii Matsyk (Director of the Directorate for Digital Infrastructure Development of the Ministry of Digital Transformation), Oleksandr Savchuk (Chairman of the Board of InAU); Hnat Serhuta (Head of Regulatory Relations and Strategy at LIFECELL).

The session discussed the issues in the context of the implementation of the Law on Electronic Communications and the adoption of the Law of Ukraine on the Regulator:

- how the network sharing will work
- procedure for identifying and defining the markets
- protection of small and medium business and economic competition,
- methods of counteracting the expulsion of small players from the market,
- settlement of disputes between providers of electronic services and networks in the field of access to telecommunications infrastructure (National Commission for the State Regulation of Communications and Informatization as an arbitrator),

Ways to improve the legal framework in the field of access to telecommunications infrastructure were also discussed, including the need to amend the Law of Ukraine on Access to Construction, Transport and Electricity Facilities to develop telecommunications networks.

The emphasis was made on the threats to the implementation of state programmes of digitalization and internalization of villages in the context of the decision of the Kyiv District Administrative Court on the actual introduction of a non-market duty on wire and cable products over 20% by judicial reversal of the Interdepartmental Commission on International Trade.

It was also noted that the increase in tariffs for access to the telecommunication cable ducts of JSC Ukrtelecom should be preceded by economic justification and appropriate calculations.

Section 8. “STAKEHOLDERS OF UKRAINE'S INTEGRATION INTO THE SINGLE DIGITAL MARKET (ROLE OF USERS)”

Moderator: O. Prykhodko (International NGO “European Media Platform”).

The session was attended by: Oleksandr Fedienko (Deputy Chairman of the Verkhovna Rada Committee on Digital Transformation); Yulia Hariacha (Ministry of Digital Transformation), Olha Kvashuk (International Renaissance Foundation), David Frochi (Director for European Government and Regulatory Affairs, ISOC), Oleksii Semeniaka (RIPE NCC), Mikhail Anisimov (ICANN), Olha Bolshakova (NAM), Oleksandr Isavnin (Free Moscow University).

It was noted that Ukraine has made significant progress on the path to the EU Digital Single Market and has a chance to become the first of the third countries to receive access to the EU's internal digital market. This still requires a lot of effort, and the level of progress in different areas is very different (the greatest progress has been reached in the field of trust services, and the least one has been reached in the field of audiovisual services).

Solving the problem of audiovisual services is possible only by making a political resolution of the parliament on the implementation of European norms in Ukrainian legislation; in other areas more pressing issues include the interpretation of existing legislation, cooperation in a multi-stakeholder environment, taking into account the opinions of all stakeholders.

In this environment, decisions are made through a variety of mechanisms, and working with the larger community requires sufficient attention to bottom-up mechanisms and more active involvement of Ukrainian stakeholders in decision-making processes at the European and international levels (including through greater cooperation with the European Commission, Internet Society, ICANN communities, RIPE NCC, International Renaissance Foundation, etc.).

Such decisions, in their turn, must clearly distinguish the content and infrastructure levels of cyberspace.

Section 9. “COVID-19 AND DIGITAL TRANSFORMATIONS”

Moderator: O. Prykhodko (International NGO European Media Platform), D. Kohmanyuk (Hostmaster).

The session was attended by: Sean Brian Townsend (Ukrainian Cyber Alliance); Lilia Oleksiuk, (freelance adviser to the Verkhovna Rada Committee on Digital Transformation); Anastasia Tkachuk (moderator IV Youth IGF-UA).

The COVID-19 pandemic has significantly accelerated the pace of digitalization of our lives, and neither governments (lacking an understanding of cybersecurity threats and the need to protect personal data) nor the population (lacking digital literacy and cyber hygiene skills) was prepared for this.

Further digitization should take into account the risks of discrimination against certain segments of the population and make it impossible for government digital solutions to be unalterable. Digital solutions should be aimed at avoiding the danger of centralizing information and sharing risks and taking into account the world best practices.

Section 10. **“THE IMPACT OF POLICY ON THE INTERNET AND INTERNET TECHNICAL SOLUTIONS”**

Moderator: Svitlana Tkachenko (Hostmaster), co-moderator Oleksii Semenyaka (RIPE NCC).

The section was attended by Mandy Carver (Senior Vice President for cooperation between Governments and Intergovernmental Organizations, ICANN); Veni Markowski (ICANN Vice President); Mikhail Anisimov (ICANN Senior Manager for Eastern Europe and Central Asia), Vesna Manojlovic (Community Builder RIPE NCC), Oleksandr Isavnin (Moscow Free University).

Conclusions of the section:

- States increase their activity on the Internet by introducing new regulations.
- These regulations do not always contribute to the development of the Internet; sometimes they significantly interfere with its work, and sometimes they are little implemented or not implemented at all at the current level of technology development.
- In this situation, the lack of dialogue with other stakeholders (primarily the technical community) leads to fatal consequences for the "network of networks", which is the Internet. The process of developing policies and regulations must be very careful and take into account the technical principles of the Internet infrastructure.
- At the same time, the Internet cannot be a "dictatorship of engineers."
- The end-users must be the real beneficiaries. At the same time, the processes of setting up the Internet must identify discriminated groups of users and eradicate the identified discrimination.
- I* organizations are actively involved in these activities within the mandates they have received from the online community. Thus, it is the civic activity of the Internet community that is the cornerstone of the balance system on the Internet.

Section 11. **“INTERNET STANDARDS: WHERE IT COMES FROM, WHO CREATES, HOW IT WORKS, WHETHER UKRAINE PARTICIPATES IN THE DEVELOPMENT OF STANDARDS”**

Moderator Oleksii Semenyaka (RIPE NCC), co-moderator Svitlana Tkachenko (Hostmaster)

The section was attended by: Oleh Muravskiy (RIPE NCC), Dmytro Beliaevskiy (Red Hat) and Maria Pleskach (online community, PhD).

Experts discussed in detail how Internet standards are created in:

- Internet Engineering Task Force (IETF)
- the RIPE community
- organizations responsible for developing cybersecurity.

The latest results of some groups for the development of the TLS and ESNI standards were presented and it was clarified what are the goals and objectives of these bodies, how the standards are discussed and approved.

Standards development teams are open to participation and collaboration. The Technical Community of Ukraine needs to be more actively involved in all processes of development, discussion, approval of IETF standards and RIPE policy. We expect support from the state and concrete steps to promote this participation, for example, through the provision of targeted grants.

The participation of not only engineers and technicians but also that of the representatives of the legislature and standardization bodies is important. Development of national standards based on the work of international committees and taking into account thereof will ensure the compatibility and development of the national system. The inconsistency and unconformity of the national standardization system with international systems is becoming a factor hindering its development.

It is also important to note that the main working language is English. It is a language of international cooperation, and for the development of standards, it is almost the only opportunity to cooperate. Therefore, steps are needed to be made by the state and business to improve the training professionals in the English language to reduce the language barrier.

REPORT ON THE PREPARATION AND CONDUCT OF THE FOURTH UKRAINIAN YOUTH FORUM ON INTERNET GOVERNANCE

Introduction

The fourth Ukrainian Youth Internet Governance Forum (Youth IGF-UA) was held online on November 10, 2021, in Kyiv. The core mission of the conference was to involve young people in developing solutions to current problems of Internet governance - from understanding key issues to event planning and active participation.

Near 60 participants took part in the 4th Youth IGF-UA, representing government agencies, international organizations, the private sector, civil society, academic and technical community, and the media. Young Ukrainian people got an opportunity to learn about the youth projects from reliable organizations, like RIPE NCC, Internet Society, ICANN as well as share their experience of participating in these programs. Among other topics, we also discussed the development of the green internet in Ukraine, the gamification of the future from the digital and real-life point of view, and who is responsible for delivering internet services of high quality in different regions.

Organizational Process

The activity of the Initiative Group is based on the “Code of Conduct of the Youth Coalition on Internet Governance (YCIG)”

“Code of Conduct of the Youth Coalition on Internet Governance (YCIG)”:

<https://ycigweb.wordpress.com/code-of-conduct/>

Ukrainian translation is here:<https://youth-igf-ua.org/>

The initiative group of the Ukrainian Youth Internet Governance Forum was created in February 2018 as a result of consensus between participants and supporters of the Youth IGF-UA Pro event held on October 5, 2017, in Kyiv. During the event, experts discussed the establishment of a new platform for young people’s engagement in Internet Governance. For that to happen at Youth IGF-UA (February 2018) Valerie Dubitskaya (European Media Platform) initiated the creation of the Youth IGF-UA Multistakeholder Organizing Team. Messages about this initiative were sent to VIII IGF-UA (October 6, igf-ua.org), IGF Secretariat, EuroDIG, SEEDIG.

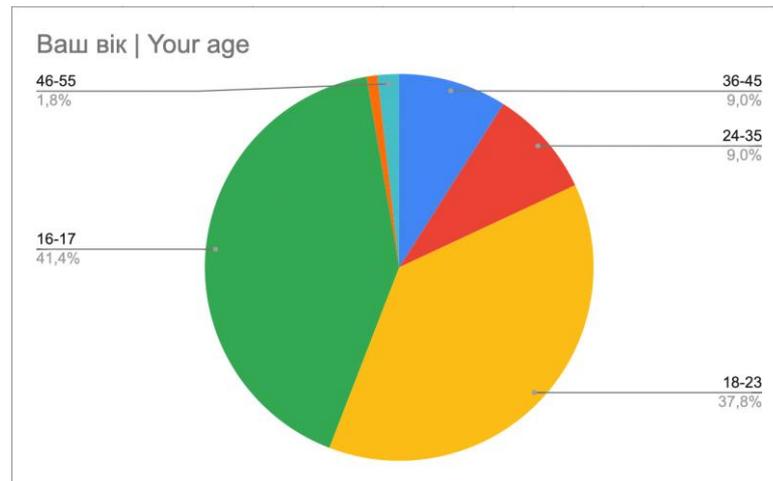
The founding of the Fourth Ukrainian Youth Internet Government Forum (IV Youth IGF-UA) began on October 27, 2021, on the basis of the decision of the Organizing Committee of the Ukrainian Internet Forum IGF-UA). Anastasia Tkachuk, an independent expert, representative of the Youth IGF-UA Initiative Group, a member of the Ukrainian Internet Governance Forum Organizing Committee, was appointed a moderator of the event.

Participants

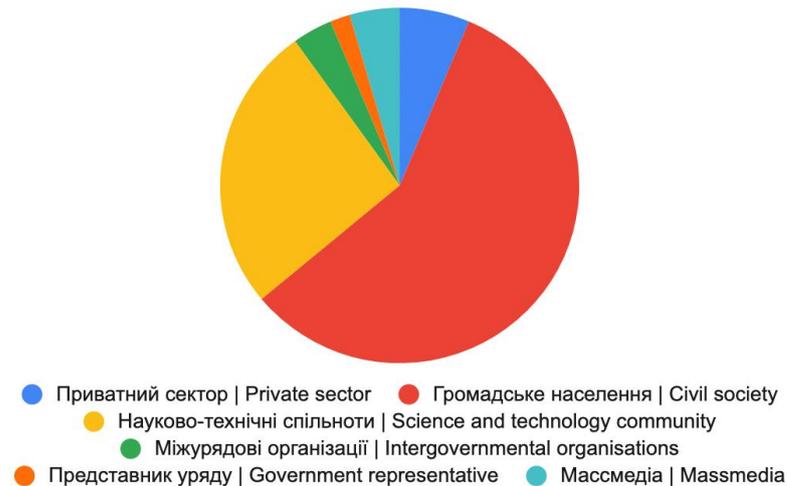
Since the IV Youth IGF-UA was held online in the videoconference format, participants could join either via the Adamant platform or by watching the video stream on YouTube.

To be able to participate in the discussion and ask questions, a participant had to register via the online form. There were 111 registrations and 62 attendees at the event. Many registered

participants were not able to join us via the Adamant platform because of technical issues. They followed the forum via a YouTube video stream.



До якої групи стейкхолдерів ви себе відносите? | What group of stakeholders do you belong to?



Financial issues

IV Youth IGF-UA supporters and sponsors provided the necessary resources within the framework of the preparation and holding of the Forum.

Conclusions

Information about the event date, topics, and terms of participation was shared through the Youth IGF-UA official website (<https://youth-igf-ua.org>), Facebook page

(<https://www.facebook.com/YouthIGFUA>), as well as through the information channels of the Junior Academy of Sciences of Ukraine, Kyiv National University of Trade and Economics, and other information channels.

The terms of participation in the Youth IGF-UA was completed in accordance with

Fundamental Principles of the Youth Coalition for Internet Governance (prescribed in the Statute and the Code of Ethics).

The initiative group received 12 proposals for topics for discussion. On the basis of the received applications the following program was formed:

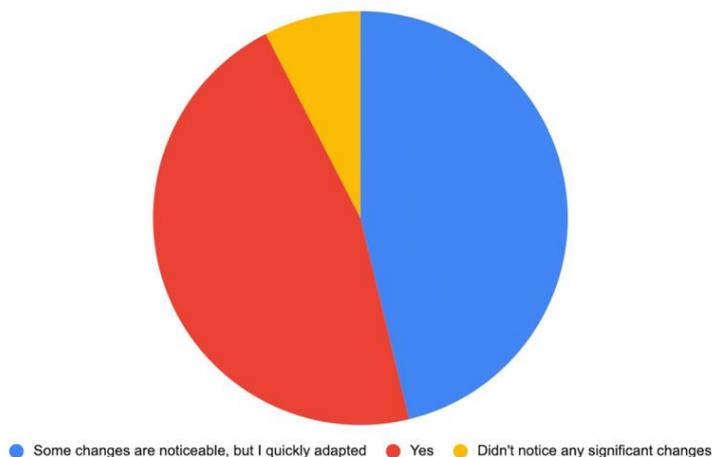
1. Welcome word from organizers and sponsors (Alex Semenyaka, Mikhail Anisimov, Vitaliy Moroz, Valentin Protopopov, Alejandra Prieto)
2. Section 1: Youth Programs by Internet Society (Alejandra Prieto), RIPE NCC (Alex Semenyaka), ICANN (Mikhail Anisimov).
3. Section 2: Green Interned (Valentyn Protopopov)
4. Section 3: Cybersecurity from the point of view of Ukrainian youth (Ilya Pravosud)
5. Section 4: Experience in participating in the international youth programs (Valeria Dubytska, Eileen Kwiponya, Lisa Kukowska)
6. Section 5: Gamification of the Future (Pavlo Kravchenko, Natalia Katashynska)
7. Section 6: Internet 101 (Vahan Hovsepyan)
8. Summing up (Anastasiia Tkachuck, Oksana Prykhodko)

The moderator of the event was Anastasiia Tkachuk, an independent expert, representative of the Youth IGF-UA Initiative Group, a member of the Ukrainian Internet Governance Forum Organizing Committee.

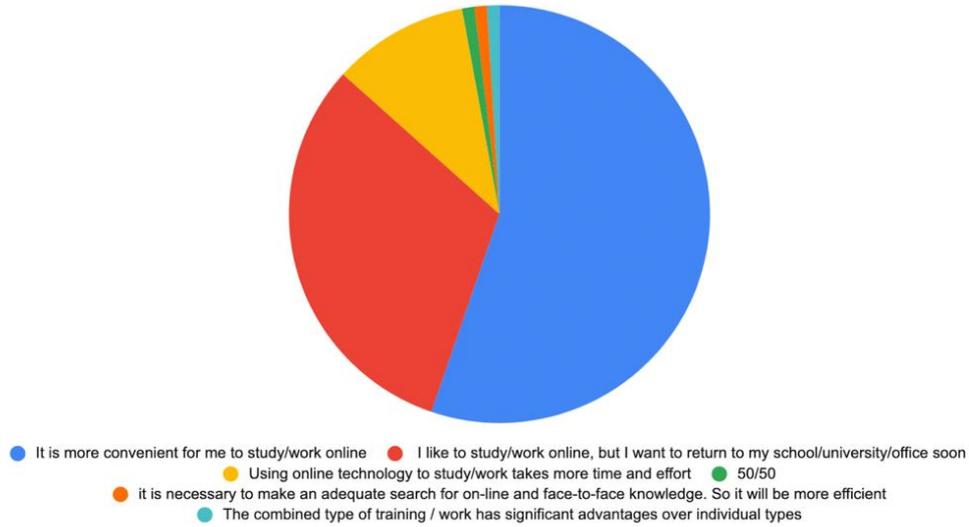
In accordance with the decision of the Organizing Committee of IGF-UA, all participants of Youth IGFUA were given the opportunity to send reports or abstracts for a printed collection of IV Youth IGF-UA reports (in accordance with MAS standards).

During the registration, participants were asked to answer some questions about the influence of the COVID-19 pandemic on their life. The questions and the results are presented below:

Чи помітили ви суттєві зміни у вашому житті після початку пандемії? | Have you noticed significant changes in your life since the beginning of the pandemic?



Особисто Ви відчуваєте переваги навчанню/роботі онлайн чи це створює вам додатковий дискомфорт? | Do you personally feel the benefits of studying/working online or does it create additional discomfort for you?



During the IV Youth IGF-UA, we discussed many important issues that require the participation of the young generation and the following messages were formed:

The online format of work and study is not a panacea for pandemic challenges. People feel discrimination against their rights and mental pressure when they can not participate in the study processes and visit events offline. The educational system needs a combination of online and offline formats.

Renewable energy is a must for Ukraine in the current circumstances. For now, the industry is quickly evolving and young people should realize their abilities in the sphere.

To aware the young generation about the possible cyber threats, we need a robust government program. But we can start with meetings with students and their parents. People should know how to identify, prevent, and where to report cybercrime.

The Game Theory is widely used in different spheres of our lives, starting from the social networks to the educational system. The gamification of the future is already in process and it can go either a digital way (eg: Metaverse) or usual offline format (Krytycotiki).

To protect your rights on internet services of high quality, you should know who is responsible for this in your country. This information should be widely spread and easily accessible.

[Videos and presentations IGF-UA-2021 are available at: https://i-ua.tv/projects/iaf-ua/28047-12-i-ukrainskyi-forum-z-upravlinnia-internetom](https://i-ua.tv/projects/iaf-ua/28047-12-i-ukrainskyi-forum-z-upravlinnia-internetom)

CONTACTS

IGF-UA Organizing Committee

www.igf-ua.org

info@igf-ua.org

tel/fax: +38 044 278-2925

15/3 Olesia Honchara street, office 22, Kyiv, 04053