**XII Український форум з управління Інтернетом IGF-UA**

**IV Молодіжний IGF-UA**

**Київ, 10-12 листопада 2021**

**Річний звіт**

**ЗМІСТ**

Вступ 1

Організаційний процес 2

Порядок денний 3

Учасники 4

Фінансування 4

Висновки 5

Звіт про підготовку та проведення Четвертого Молодіжного Українського Форуму з управління Інтернетом 13

Контакти 17

**ВСТУП**

Перший Український Форум з управління Інтернетом (IGF-UA) відбувся у вересні 2010 року в м.Києві. З того часу щорічний IGF-UA став продовженням світової серії Форумів з обговорення найбільш важливих питань розвитку інформаційного суспільства, консолідації зусиль державних органів, бізнесу, інтернет-товариства, професійних і академічних еліт для прискорення реалізації ІТ можливостей, створення умов всебічного розвитку інтернет-технологій в суспільних інтересах. IGF-UA завжди збирає учасників з різних країн світу, що представляють міжнародні організації, урядові установи, неурядові та комерційні організації в сфері ІКТ та засобів масової інформації.

**Дванадцятий Український Форум з управління Інтернетом IGF-UA** був проведений 11-12 листопада 2021 року в режимі відеоконференції. **Четвертий** **Молодіжний форум з управління Інтернетом IGF-UA** відбувся 10 листопада в режимі відеоконференції.

В 12-му IGF-UA взяли участь учасники з України та інших європейських країн, що представляють урядові установи, міжнародні організації, приватний сектор, громадянське суспільство, академічні та технічні співтовариства, засоби масової інформації.

IGF-UA продовжує бути важливим компонентом національної дискусії про майбутнє Інтернету в Україні.

**ОРГАНІЗАЦІЙНИЙ ПРОЦЕС**

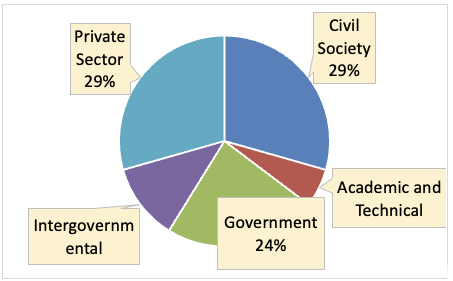
Діяльність Організаційного комітету IGF-UA базується на «Принципах щодо проведення Українського Форуму з управління Інтернетом IGF-UA (Протоколу про наміри)». Цей документ було розроблено на виконання рішень 4-го IGF-UA.

*«Принципи щодо проведення Українського Форуму з управління Інтернетом IGF-UA (Протокол про наміри)»:* [*http://igf-ua.org/docs/Principles.doc*](http://igf-ua.org/docs/Principles.doc)*.*

Всі представники інтернет-спільноти, які звернулись з пропозицією про включення своєї кандидатури до складу Оргкомітету і погодились з «Принципами…», були обрані до складу Оргкомітету. Таким чином до складу Оргкомітету увійшли 17 осіб, які збалансовано представляють різні зацікавлені групи: урядові установи, міжнародні організації, приватний сектор, громадянське суспільство, наукові і технічні співтовариства.

**Члени Оргкомітету IGF-UA**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Ім’я** | **Організація** | **Зацікавлена група** |
|  | Анісімов Міхаіл | ICANN | Міжнародні організації |
|  | Арутюнян Олександр | Інтернет Асоціація України | Приватний сектор |
|  | Баранов Олександр | НДІ інформатики і права НА правових наук України | Академічна і технічна спільнота |
|  | Звєрєв Володимир | Рада національної безпеки і оборони України | Урядові організації |
|  | Каргаполов Юрій | ГО «Українське відділення всесвітньої Інтернет-спільноти | Приватний сектор |
|  | Кохманюк Дмитро | Незалежний Експерт | Приватний сектор |
|  | Куковський Володимир | Секретар Оргкомітету | Громадянське суспільство |
|  | Мацик Юрій | Мінцифри | Урядові організації |
|  | Мороз Віталій | ГО Інтерньюз-Україна | Громадянське суспільство |
|  | Пєтухов Іван | Комісія з питань науки і ІТ УСПП | Приватний сектор |
|  | Приходько Оксана | Європейська Медіа Платформа | Громадянське суспільство |
|  | Семенченко Андрій | НКРЗІ | Урядові організації |
|  | Семеняка Олексій | RIPE NCC | Міжнародні організації |
|  | Смєлянський Юрій | ГС Комісія з питань науки та інформаційних технологій | Громадянське суспільство |
|  | Ткаченко Світлана | ТОВ «Хостмайстер» | Приватний сектор |
|  | Ткачук Анастасія | Незалежний експерт, представник спільноти з організації Молодіжного IGF-UA | Громадянське суспільство |
|  | Черняк Ігор | Служба безпеки України | Урядові організації |
|  |  |  |  |



**Участь в Оргкомітеті IGF-UA представників різних зацікавлених груп**

Організаційний комітет IGF-UA виконував роботу не лише в період безпосередньої підготовки заходів IGF, а впродовж всього періоду між 11-м та 12-м IGF-UA. За цей період відбулось сім засідань Організаційного комітету – 17.08.210.2021, 06.09.2021, 21.09.2021, 04.10.2021, 19.10.2021, 27.10.2021, 03.11.2021 (протоколи засідань українською мовою – [http://igf-ua.org](http://igf-ua.org/)).

Оргкомітет визначив склад з п’яти Організаторів IGF-UA: Інтернет Асоціація України (ІнАУ), Комісія з питань науки та ІТ Українського союзу промисловців та підприємців (УСПП), RIPE NCC (RIPE Network Coordination Centre), ГО «Інтерньюз-Україна», ТОВ «Хостмайстер».

Спонсорами IGF-UA виступили: Internet Corporation for Assigned Names and Numbers (ICANN), IGF Supporting Association (IGFSA), Internet Society.

Форум відбувся за підтримки Міністерства цифрової трансформації України, Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, Апарату Ради національної безпеки і оборони України, МГО «Європейська Медіа Платформа».

Серед організаторів IGF-UA та організацій, які підтримали Форум, збалансовано представлені різні зацікавлені групи:

* Громадянське суспільство / Приватний сектор: Інтернет Асоціація України, Комісія з питань науки та ІТ Українського союзу промисловців та підприємців;
* Громадянське суспільство: ГО «Інтерньюз-Україна», МГО Європейська медіа платформа;
* Приватний сектор: RIPE Network Coordination Centre; ТОВ «Хостмайстер»;
* Урядові організації: Міністерство цифрової трансформації України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Апарат Ради національної безпеки і оборони України;
* Міжнародні організації: Internet Society, IGF Supporting Association (IGFSA), Internet Corporation for Assigned Names and Numbers (ICANN).

Медіапартнерами виступили: I-UA.tv - генеральний інформаційний спонсор; Інтерфакс-Україна - генеральний медіапартнер; НВ – медіапартнер.

**ПОРЯДОК ДЕННИЙ**

Основна мета IGF -UA полягає в розвитку управління Інтернетом в Україні через багатосторонній діалог, а також сприяння розвитку партнерських відносин задля координації зацікавлених сторін для кращого і найбільш збалансованого розвитку Інтернету в інтересах громадян України. Ґрунтуючись на цій меті, Оргкомітет визначив перелік основних тем для обговорення на IGF-UA. На їх базі сформовано 11 секцій для обговорення та дискусій.

**Секція №1. Кібербезпека і права людини в Україні. Стандарти в сфері кібербезпеки.**

**Секція №2. Свобода інтернету та цифрові права.**

**Секція №3. Новітні технології та штучний інтелект.**

**Секція №4.  Кібербезпечні міста, смарт-міста.**

**Секція №5.  Інтернет речей і питання безпеки.**

**Секція №6. Тенденції в розвитку управління інтернетом.**

**Секція №7. Інфраструктура телекомунікацій; Впровадження ЗУ Про електронні комунікації.**

**Секція №8. Стейкхолдери інтеграції України в єдиний цифровий ринок (роль користувачів).**

**Секція №9. Covid-19 і цифрові трансформації.**

**Секція №10. Вплив політики на інтернет і на технічні рішення в сфері інтернету.**

**Секція №11. Стандарти Інтернету: звідки беруться, хто створює, як працюють, чи бере Україна участь в розробці стандартів.**

На **Заключному пленарному засіданні** підбиті підсумки Форуму.

*Повна версія програми 12-го IGF-UA – за адресою* <http://igf-ua.org/програма-igf-ua-2021>.

**УЧАСНИКИ**

В Форумі взяли безпосередню участь значна кількість учасників з України та інших європейських країн, що представляють урядові установи, міжнародні організації, приватний сектор, громадянське суспільство, академічне та технічне співтовариство, ЗМІ та молодь.

Оскільки форум відбувався в режимі відеоконференції, всі охочі могли взяти в ньому участь без реєстрації.

Учасники мали можливість зворотного зв’язку через чат та електронну пошту.

**ФІНАНСУВАННЯ**

Відповідно до Принципів щодо проведення Українського Форуму з управління Інтернетом IGF-UA (Протоколу про наміри), надання необхідних ресурсів у рамках підготовки та проведення Форуму забезпечили Організатори та Спонсори IGF-UA.

Изображение выглядит как стол

Автоматически созданное описание

Рішенням Оргкомітету схвалено формування єдиного бюджету IGF-UA і Молодіжного IGF-UA, включаючи збір і витрати коштів.

Залишкові кошти за рішенням Оргкомітету будуть направлені на проведення в Україні заходів IGF-UA у 2022 році.

**ВИСНОВКИ**

З підсумковими заявами на заключній дискусійній панелі виступили модератори панелей. Була підкреслена плідність дискусій, важливість впровадження міжнародного досвіду на теренах України та роль дискусій 11-го IGF-UA у подальшому вдосконаленні управління Інтернетом.

Секція 1. **«КІБЕРБЕЗПЕКА І ПРАВА ЛЮДИНИ В УКРАЇНІ. СТАНДАРТИ В СФЕРІ КІБЕРБЕЗПЕКИ»**

Модератором виступив І.Пєтухов (УСПП), співмодератор: О.Семеняка (RIPE NCC).

Учасники секції резюмували відповіді на ряд актуальних запитань у цій сфері:

1. Існує проблема належного розуміння ключових понять у сфері кібербезпеки, правильного їх розмежування та співвідношення, що критично для створення ефективного механізму протидії загрозам у кіберпросторі, а також дієвого механізму правового забезпечення означеної сфери.

Мають бути:

* розроблені чіткі нормативні документи;
* визначені, які саме організаційні, юридичні, технічні, освітні заходи мають проводитись відповідальними суб'єктами;
* додані до практичних заходів із забезпечення кібербезпеки людини охоронні заходи, і надано відповідне визначення.

2. Роль стандартів в сфері кібербезпеки для забезпечення кібербезпеки є надзвичайно важливою. На національному рівні необхідно постійно проводити аналіз та узагальнення досвіду таких закладів як ITU, ISO/IEC, NIST.

Потрібні:

* Розробка та прийняття національних стандартів галузі на основі міжнародних і регіональних.
* Імплементація та адаптація стандартів держав-членів відповідних організацій стандартизації, з якими є відповідні міжнародні договори

3. Обираючи модель побудови системи безпеки в кібернетичному просторі, чинна українська влада обрала хибний російський шлях: забезпечення безпеки для самої влади.

Визначені загрози та ризики:

* Не визначена та частина свободи особистості, якою вона повинна поступитися в якості плати за захист від загроз з кіберпростору.
* Ціна «відмова від свободи» для досягнення безпеки від таких загроз породжує додаткові загрози виникнення суспільно-політичної та соціально-економічної нестабільності та, як наслідок, додаткові загрози національній безпеці України.
* Жодного разу не було визначено рівня безпеки громадян, який держава може гарантувати.

Тому неможливо визначити адекватність ціни «відмова від свободи» по відношенню до рівня гарантованої владою безпеки від загроз, що виходять із кіберпростору.

Рекомендовано для української державної влади відмовитися від помилкового та небезпечного «російського» шляху формування системи безпеки в кіберпросторі.

4. Авторами Закону України «Про електронні комунікації» визначено безпеку мереж і послуг. Однак, окрім визначення поняття «безпека мереж і послуг» Закон України «Про електронні комунікації» не містить критеріїв (методології) визначення «безпечності послуги у сфері електронних комунікацій».

Потрібно затвердження на законодавчому рівні:

* чітких, зрозумілих та вимірюваних критеріїв безпечності послуг у сфері електронних комунікацій.
* основного принципу роботи в мережі Інтернет, а саме принципу відкритості.

5. При розгляді питання "Ризики та загрози безпеці об'єктам критичної інфраструктури у інформаційному просторі України" були розглянуті головні властивості критичної інфраструктури та інформаційної безпеки, розглянуті практичні питання.

Зазначено великі ризики, що несе в собі проект Закону про критичну інфраструктуру No5219 від 09.03.2021г.

Учасниками секції було пропоноване депутатам ВРУ утриматись від порушень конституційних прав громадян і приватної власності.

Секція 2. «**СВОБОДА ІНТЕРНЕТУ ТА ЦИФРОВІ ПРАВА**»

Модерував секцію Віталій Мороз, участь взяли Віта Володовська, директорка Лабораторії цифрової безпеки, Гульсанна Мамедієва, директорка Директорату з євроінтеграції Міністерства цифрової трансформації України та Ігор Розкладай, заступник директора, головний експерт з медійного права ЦЕДЕМ..

Ключові тези/висновки:

* Сьогодні концепт “безпека в інтернеті” поступово витісняє ідею “свободи інтернету”, адже інтернет стає все більш фрагментарним, країни вводять все більше регуляцій, й це може загрожувати звуженню таких цілої низки цифрових прав, зокрема права на анонімність.
* Ключовий виклик для українського уряду в захисті персональних даних – це реалізація (enforcement) дій та кроки аби відновити порушені права користувачів.
* Приватний сектор не завжди розуміє цінність захисту персональних даних, зрідка оперує категорією “цифрові права”, а на сайтах провайдерів часто замість політики конфідеційності – тільки лиш положення про надання телекомунікаційних послуг. Разом з тим, лідери ринку усвідомлюють необхідність прописувати політики конфіденційності та захисту персональних даних.
* Ефективність захисту персональних даних для урядових інституцій (Мінцифри) – це не кількість виписаних штрафів, а зміни в політиках конфідеційності приватного сектору. Урядовий сектор зацікавлений в роз’ясненні, роботі з приватним сектором, щоб компанії навчились правильно застосовувати закон.
* Приватному сектору в Україні потрібно буде готуватися до впровадження положень нового закону про захист персональних даних. Водночас, схвалення закону «Про захист персональних даних» містить потенційні ризики для приватного сектору. По-перше, брак часу в приватного сектору на втілення нових практик. По-друге, брак чітких визначень в законі, що стосується відповідальності компаній та можливих санкцій.

Секція 3. «**НОВІТНІ ТЕХНОЛОГІЇ ТА ШТУЧНИЙ ІНТЕЛЕКТ»**

Модерував секцію Віталій Мороз, участь взяли Тетяна Авдєєва, юристка ЦЕДЕМ, Володимир Хильчук, Менеджер з інновацій Into-sana, COO Lab24.com.ua, Олександр Баранов, доктор юридичних наук, Керівник Наукового центру цифрової трансформації і права Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України».

Ключові тези/висновки:

* Зміни в суспільстві з впровадження штучного інтелекту (ШІ) настануть набаго швидше, аніж ми очікуємо. Моделі розвитку штучного інтелекту можуть призвести нас до антиутопій на зразок Орвелла чи Бредбері або ж навпаки – до функціонування smart-міст, що відповідає на потреби жителів
* Існує велика ймовірність класового поділу в майбутньому, повязана з доступом до даних, неусвідомлення цінності цих даних з боку користувачів може сприяти поглибленню цього поділу. Роль великих компаній буде зростати.
* У всьому світі ШІ має широке застосування в сфері охорони здоров'я, однак для України ШІ ще не використовуються активно й тут менший обсяг даних. При цьому, в IT-секторі швидко розвиваються стартапи, що акцентують на застосуванні ШІ.
* Сертифікація ШІ стала одним з ключових питань під час дискусії – встановлення базових вимог безпечності використання технологій для людини. Сертифікація може мати кілька способів, в тому числі самостійно з боку компаній.

Секція 4. **«КІБЕРБЕЗПЕЧНІ МІСТА, СМАРТ-МІСТА»**

Модератор Світлана Ткаченко, Спікери: Олена Гунько, начальник управління інформаційних технологій Львівської міської ради; Соломія Паславська, проектна менеджерка Міністерства цифрової трансформації України, Володимир Кондзьолка, Директор "Інституту міста Дрогобича”, Роман Хіміч, експерт, Роман Чорненький, ELKO Україна, Максим Благонравін, ТОВ “Хостмайстер”.

Ключові тези/висновки:

* розумні міста побудовані на основі інтернету речей, великих даних, хмарних обчислень, штучного інтелекту тощо, де інтернет стає їх основною техелогією
* застосування концепції смарт-міста та управління на основі даних допомагає зробити не тільки більш комфортним життя мешканців міста і оптимізувати управління інфраструктурою міста, але аналізувати і скорочувати непродуктивні видатки миського бюджету
* без підвищення цифрової грамотності неможливо забезпечити рівні можливості і однаковий рівень доступу до сервісів, співпрацю з різними підрозділами міста.
* наявність в громаді "цифрового лідера" сприяє залученню груп зацікавлених сторін для підготовки, прийняття та впровадження рішень щодо використання, розгортання та підзвітності цифрових технологій у містах. Завданням відповідних міністерств є допомога цифровим лідерам в отриманні необхідні знання з міського управління та цифрової трансформації
* впровадження нових технологій несе з собою й ризики та вразливості з точки зору кібербезпеки. Необхідно приділяти особливу увагу безпечному використанню даних, забезпечити цілісність і якість надання основних послуг, надійність інформаційних систем.

Секція **5. «ІНТЕРНЕТ РЕЧЕЙ І ПИТАННЯ БЕЗПЕКИ»**

Модератор: Ю.Каргаполов (ГО "Українське відділення всесвітньої Інтернет-спільноти").

У роботі сесії брали участь Wout de Natris - відомий світовий експерт в галузі безпеки, голова Робочої групи з кіберзлочинності в RIPE NCC, голова робочої групи IGF Dynamic Coalition for Internet Standards, Safety and Security; Баранов О.А. - д.ю.н., керівник Науково-дослідного центру цифрових трансформацій і права Науково-дослідного інституту інформатики і права Національної академії правових наук України; Peter Waher - відомий світовий експерт в галузі кібербезпеки IoT, розробник IoT систем, консультант з питань імплементації IoT, автор книжок про IoT; Mark Carvell – відомий світовий експерт з питань Internet Governance, який має багатий досвід державної служби у Великобританії, координує підтримку уряду Великобританії для IGF і є членом IGF Steering Committee Великобританії, а також представляє Великобританію в ITU та інших багатосторонніх форумах з питань Internet Governance

Робота секції «Інтернет речей і питання безпеки» розпочалася з представлення учасників, які є широко відомими міжнародними фахівцями у галузі розвитку технологій IoT та протидії кіберзлочинам. Було окреслено коло питань, довкола яких відбулася дискусія. Сесія була у порядку денному підготовки до проведення IGF 2021 у Катовицях та мала розповісти у тому числі про роботу DC-ISSS (https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-internet-standards-security-and-safety-DC-ISSS). Тому питання, що розглядалися на сесії, були актуальними для світового порядку денного та включали рамкові аспекти, технічні, технологічні, організаційні, аспекти стандартизації та закупівлі.

Спочатку на сесії було розглянуто питання, які можна віднести до рамкових у діяльності DC-ISSS. Wout de Natris розповів про цілі та завдання, а також про результати отриманих під час першого року роботи Коаліції. Були представлені результати дослідження, які характеризували найбільш проблемні питання в галузі безпеки IoT з погляду опитаних фахівців по всьому світу та різних стейкхолдерів. Наголошено, що завдання Коаліції полягає не в тому, щоб розробити конкретні засоби протидії шкідливим діям, а визначити напрямки, на яких необхідно зосередити зусилля різних стейкхолдерів для запобігання виникненню загроз.

Про досвід впровадження проектів, політик технічного регулювання та стандартизації розповів Peter Waher, який звернув увагу, що практика реагування на несанкціоновані впровадження в IoT системи припадає переважно на реактивне реагування на ті загрози, які вже були. Дуже мало засобів, які б могли протистояти новим загрозам. Велика проблема щодо безпеки існує на контурі завдань аутентифікації та авторизації прав доступу до обʼєктів IoT систем.

Mark Carvell розповів про підхід до створення регуляторних правил, за рахунок яких можна побудувати комплексну систему підтримки безпечного середовища IoT. Mark Carvell розкрив тезу «безпека за умовчанням» та комплекс дій, які мають виконати всі стейкхолдери, залучені до роботи із забезпечення безпеки IoT.

Однією з пропозицій, що прозвучали під час обговорення, було створення національного постійно діючого комітету з проблем Internet Governance (National Internet Governance Steering Committee), до складу якого на принципах мультистейкхолдеризму входили б різні актори. Рішення такого комітету мають укладатися за принципом консенсусу. До завдань такого комітету можуть входити розробка та впровадження гармонізованих конкретних політик Internet Governance, вивчення та адаптація в країні кращих практик застосування політик Internet Governance.

Wout de Natris закликав українських розробників та користувачів IoT систем приєднуватися до DC-ISSS, наголосивши, що така робота дозволить бути залученим до найсучасніших трендів та збагатить матеріали, які готує Коаліція.

Секція **6. «ТЕНДЕНЦІЇ В РОЗВИТКУ УПРАВЛІННЯ ІНТЕРНЕТОМ»**

Модератор: Ю.Каргаполов (ГО "Українське відділення всесвітньої Інтернет-спільноти").

У роботі сесії брали участь: Сагіян Григорій - відомий експерт з питань Internet Governance, заступник голови НВО «Інтернет-спільнота Вірменії»; Пазюк Андрій - д.ю.н., відомий фахівець у галузі міжнародного інформаційного права і комунікаційного право, кіберправа, управління інтернетом; Філінович Валерія– к.ю.н., відомий український експерт в галузі Internet Governance, авторського права, права промислової власності, Інтернет-права, кібербезпеки, інформаційного права; Перун Роман – засновник і директор національного оператора мережевого слайсінгу «IT-KARKAS», засновник Міжнародного IT-Форуму «IT-KARKAS», Всеукраїнського IT-Форуму системних адміністраторів.

На сесії обговорювались питання, що визначають архітектуру Інтернет та виклики, які залишають простір невирішених проблем Інтернет, правові питання Інтернету, нові концепції Internet Governance, питання, повʼязані з ринком доступу в частині технічних та технологічних рішень та як вони впливають на організаційні та адміністративні процеси регулювання доступу та розвитку технологій доступу до послуг Інтернет.

Про досвід впровадження принципів та політик Internet Governance у Вірменії розповів Григорій Сагіян, котрий надав інформацію відносно процесу створення у країни постійно діючою комісії з питань Інтернет, яка була створена за ініціативою ISOC Chapter Armenia шляхом розпорядження Кабінету Міністрів. У склад комісії включені різні стейкхолдери, баланс інтересів підтримується за рахунок делегування пропорційної кількості представників державних органів, бізнесу, академічних кіл тощо, рішення приймаються консенсусом.

Андрій Пазюк розповів про моделі створення національного центру кібербезпеки. У Великобританії до учасників входять як великі гравці ринку, але малі і середні учасники ринку. Держава у своїй веде роз'яснювальну роботу. Політики таких центрів, до яких входять і бізнес та освітні установи, спрямовані не на блокування ресурсів, а на розвиток контенту. В Україні тренд спрямований на монополізацію державою зусиль щодо кібербезпеки. Найкращі практики Європи, Америки, Азії полягають у тому, що держава реалізує модель «кібербезпека як послуга», яка виходить від описаних центрів. Прозвучала пропозиція відобразити таку концепцію у проекті закону про кібербезпеку.

Обговорення такої моделі на прикладі атаки вірусу Petya показало, що така існуюча в Україні модель протидії загрозам є неефективною і спрямована не на формування механізмів розробки та оперативного захисту від нових загроз, а на блокування вже відомих. Учасники зазначили, що після атаки вірусу Petya державні органи не змінили підходи до організації схем протидії.

Валерія Філінович розповіла про захист персональних даних та тенденції, які характерні для сучасного розвитку ринку.

Було дано аналіз існуючої ситуації у сфері захисту персональних даних, зокрема, відсутності у чинному законодавстві України ефективних норм протидії витіканню персональних даних, зловживанням та маніпуляціям з персональними даними; про невідповідність українських норм положенням GDPR, відсутність права на довіру, чітких визначень контролера та оператора персональних даних тощо. Тенденція у розвитку Інтернету полягає у тому, що мають бути захищені права споживачів послуг на національному, а також й на міжнародному рівні.

Прозвучала пропозиція підтримки положень проекту закону щодо внесення змін до діючих норм стосовно захисту персональних даних.

Як і раніше, залишається головним трендом створення ефективної системи Internet Governance створення системи довіри на національному рівні – Trust’s Ecosystem.

Роман Перун звернув увагу, що сучасний ринок Інтернет послуг з одного боку зупинився у своєму зростанні, а з іншого боку характерний відсутністю нових проривних ідей. Тому з практичного боку роботи Інтернет оператора тенденції в галузі управління Інтернет полягають у створенні механізмів нових ринків та подальшому їх розвитку. Практичним прикладом є проект створення інфраструктурного оператора на ринку надання послуг кінцевому споживачеві. Досвід показує, що це може бути новою тенденцією у побудові системи взаємин між операторами на основі реалізацій стратегій win-win. Було наголошено, що створення такого ринку буде відображено у створенні нових фінансово-економічних моделей взаємовідносин с великою кількістю ОСББ.

Учасники сесії зазначили, що відсутній майданчик постійного діалогу між державними органами та рештою стейкхолдерів і це є небажаною тенденцією в розвитку ринка Інтернет в Україні.

Секція **7. «ІНФРАСТРУКТУРА ТЕЛЕКОМУНІКАЦІЙ; ВПРОВАДЖЕННЯ ЗУ ПРО ЕЛЕКТРОННІ КОМУНІКАЦІЇ»**

Модератор: О.Арутюнян (Інтернет Асоціація України).

У роботі сесії брали участь: Федієнко Олександр (Заступник Голови Комітету ВРУ з питань цифрової трансформації); Семенченко Андрій (член НКРЗі); Трощенко Вікторія (член НКРЗі); Ткаченко Микола (член НКРЗі); Мацик Юрій (Директор директорату розвитку цифрової інфраструктури Міністерства цифрової трансформації), Савчук Олександр (Голова Правління ІнАУ); Сергута Гнат (керівник департаменту регуляторних відносин та стратегії LIFECELL).

На сесії обговорювались питання в контексті впровадження ЗУ Про електронні комунікації та прийняття ЗУ Про Регулятора:

* як буде діяти шерінг (сумісне використання) мереж
* порядок ідентифікації та визначення ринків
* захист малого та середнього бізнесу і економічна конкуренція,
* методи протидії витісненню малих гравців з ринку,
* врегулювання спорів між постачальниками електронних послуг та мереж в сфері доступу до інфраструктури телекомунікацій (НКРЗІ у ролі третейського судді),

Були обговорені також шляхи вдосконалення правової бази у сфері доступу до інфраструктури телекомунікацій, зокрема необхідність внесення змін до Закону України У Про доступ до об’єктів будівництва, транспорту, електроенергетики з метою розвитку телекомунікаційних мереж.

Було наголошено про загрози реалізації державних програм діджиталізації та інтернетизації сіл в контексті рішення Окружного адміністративного суду Києва про фактичне впровадження неринкового мита на провідниково-кабельну продукцію понад 20% шляхом судового скасування рішення Міжвідомчої комісії з міжнародної торгівлі щодо недоцільності впровадження мита на кабелі.

Також було зазначено, що підняттю тарифів на доступ кабельну каналізацію електрозв’язку АТ Укртелеком має передувати економічне обгрунтування та відповідні розрахунки.

Секція **8. «СТЕЙКХОЛДЕРИ ІНТЕГРАЦІЇ УКРАЇНИ В ЄДИНИЙ ЦИФРОВИЙ РИНОК (РОЛЬ КОРИСТУВАЧІВ)»**

Модератор: О.Приходько (МГО Європейська Медіа Платформа).

У роботі сесії брали участь: Федієнко Олександр (Заступник Голови Комітету ВРУ з питань цифрової трансформації); Юлія Гаряча (Міністерство цифрової трансформації), Ольга Квашук (Міжнародний Фонд "Відродження"), Девід Фрочі (Director for European Government and Regulatory Affairs, Internet Society), Олексій Семеняка (RIPE NCC), Міхаіл Анісімов (ICANN), Ольга Большакова (НАМ), Александр Ісавнін (Вільний Московський Університет).

Зазначено, що Україна досягла значних успіхів на шляху до Єдиного цифрового ринку ЄС і має шанси стати першою з третіх країн, що отримає режим доступу до внутрішнього цифрового ринку ЄС. Для цього ще потрібно докласти дуже багато зусиль, і рівень прогресу за різними напрямками є дуже різним (найбільший прогрес досягнуто в сфері довірчих послуг, найменший - в сфері аудіовізуальних послуг).

Вирішення проблеми аудіовізуальних послуг можливо тільки політичним рішенням парламенту щодо імплементації європейських норм в українське законодавство, за іншими напрямками більш актуальними проблемами є інтерпретація вже ухваленого законодавства, співпраця в мультистейкхолдерному середовищі з урахуванням точок зору усіх зацікавлених сторін.

В цьому середовищі рішення ухвалюються за допомогою різноманітних механізмів, і в роботі з великою спільнотою необхідно приділяти достатньо уваги механізмам bottom-up і більш активно залучати українських стейкхолдерів в процеси ухвалення рішень на європейському та міжнародному рівнях (в тому числі за рахунок більш активної співпраці з Європейською Комісією, Internet Society, спільнотами ICANN, RIPE NCC, Міжнародним Фондом "Відродження" тощо).

Такі рішення, в свою чергу, мають чітко розрізняти контентний та інфраструктурний рівні кіберпростору.

Секція **9. «COVID-19 ТА ЦИФРОВІ ТРАНСФОРМАЦІЇ»**

Модератор: О.Приходько (МГО Європейська Медіа Платформа), Д.Кохманюк (Хостмайстер).

У роботі сесії брали участь: Шон Брайан Таунсенд (Український Кібер Альянс); Лілія Олексюк, (позаштатний радник Комітету ВРУ з питань цифрової трансформації); Анастасія Ткачук (модераторка IV Youth IGF-UA).

Пандемія COVID-19 значно прискорила темпи цифровізації нашого життя, і до цього виявились не готовими ані уряди (яким не вистачає розуміння загроз кібербезпеки та необхідності захисту персональних даних), ані населення (якому бракує цифрової грамотності та навичок кібергігієни).

Подальша цифровізація має враховувати ризики дискримінації певних верств населення та унеможливлювати безальтернативність державних цифрових рішень. Цифрові рішення мають бути спрямованими на уникнення небезпеки централізації інформації та на розподілення ризиків та враховувати кращі світові практики.

Секція 10. «**ВПЛИВ ПОЛІТИКИ НА ІНТЕРНЕТ І НА ТЕХНІЧНІ РІШЕННЯ В СФЕРІ ІНТЕРНЕТУ**»

Модератор Світлана Ткаченко (Хостмайстер), співмодератор Олексій Семеняка (RIPE NCC).

У секції взяли участь Менді Карвер (старший віце-президент по взаємодії з урядами та міжурядовими організаціями ICANN); Вені Марковські (віце-президент ICANN); Михайло Анісімов (старший менеджер ICANN у Східній Європі та Центральній Азії), Vesna Manojlovic (Community Builder RIPE NCC), Олександр Ісавнін (Вільний Московський Університет).

Висновки секції:

* Держави підвищують свою активність в інтернеті, запроваджуючи нові регуляції.
* Далеко не завжди ці регуляції сприяють розвитку інтернету, іноді суттєво заважають його роботі, а зрідка виявляються малореалізовними або взагалі нереалізовними на сучасному рівні розвитку технологій.
* У цій ситуації відсутність діалогу з іншими зацікавленими сторонами (насамперед технічною спільнотою) веде до фатальних наслідків для "мережі мереж", якою є Інтернет. Процес розробки політик та регуляцій має бути вкрай акуратним і врахувати технічні принципи функціонування інфраструктури Інтернету.
* Водночас Інтернет не може бути "диктатурою інженерів".
* Справжнім бенефіціаром мають бути кінцеві користувачі. При цьому процеси облаштування Інтернету повинні виявляти дискриміновані групи користувачів та викорінювати виявлену дискримінацію.
* I\*-організації беруть активну участь у цій діяльності в рамках тих мандатів, які вони отримали від Інтернет-спільноти. Таким чином, саме громадянська активність інтернет-спільноти є наріжним каменем системи підтримки балансу в Інтернеті.

Секція 11. «**СТАНДАРТИ ІНТЕРНЕТУ: ЗВІДКИ БЕРУТЬСЯ, ХТО СТВОРЮЄ, ЯК ПРАЦЮЮТЬ, ЧИ БЕРЕ УКРАЇНА УЧАСТЬ В РОЗРОБЦІ СТАНДАРТІВ**»

Модератор Олексій Семеняка (RIPE NCC), співмодератор Світлана Ткаченко (Хостмайстер)

В секції брали участь: Олег Муравський (RIPE NCC), Дмитро Белявський (Red Hat) та Марія Плескач (інтернет-спільнота, кандидат технічних наук).

Експерти детально обговорили, як створюются стандарти Інтернет в:

* Інженерній раді Інтернету (IETF)
* спільноті RIPE
* організаціях, що відповідають за розробку кібербезпеки.

Були представлені останні результати деяких груп з розробки стандарту TLS и ESNI і з'ясовано, які цілі та завдання цих органів, як відбувається обговорення та затвердження стандартів.

Групи розробки стандартів відкриті для участі і співпраці. Технічному співтовариству України необхідно активніше брати участь у всіх процесах розробки, обговорення, затвердження стандартів IETF та полісі RIPE. З боку держави очікуємо підтримку та конкретні кроки щодо стимуляції цієї участі, наприклад, шляхом видачі цільових грантів.

Важлива участь не тільки інженерів та технічних спеціалістів, а й представників законодавчої влади та органів стандартизації у роботі. Розробка національних стандартів на базі та з урахуванням напрацювань міжнародних комітетів дозволить забезпечити сумісність та розвиток національної системи. Невідповідність та неузгодженість національної системи стандартизації із міжнародними системами стає фактором, який стримує її розвиток.

Важливо також зазначити, що основна робоча мова - англійська. Це мова міжнародного співробітництва, а для розробки стандартів майже єдина можливість співпрацювати. Тому необхідні кроки з боку держави та бізнесу щодо покращення навчання фахівців англійської мови з метою зменшення мовного бар'єру.

**ЗВІТ ПРО ПІДГОТОВКУ ТА ПРОВЕДЕННЯ ЧЕТВЕРТОГО МОЛОДІЖНОГО УКРАЇНСЬКОГО ФОРУМУ З УПРАВЛІННЯ ІНТЕРНЕТОМ**

**Вступ**

Четвертий Український молодіжний форум з управління Інтернетом (Youth  
IGF-UA) відбувся в режимі онлайн 10 листопада 2021 року в Києві. Основною місією конференції було залучити молодь до розробки рішень актуальних проблем управління Інтернетом – від розуміння ключових питань до планування заходів та активної участі.

Участь у 4-му Молодіжному IGF-UA, взяли близько 60 учасників, які представляли державні установи, міжнародні організації, приватний сектор, громадянське суспільство, наукову та технічну спільноти та ЗМІ. Молоді українці отримали можливість дізнатися про молодіжні проєкти від авторитетних організацій, таких як RIPE NCC, Internet Society, ICANN, а також поділитися своїм досвідом участі в цих програмах. Серед інших тем ми також обговорили розвиток «зеленого» Інтернету в Україні, гейміфікацію майбутнього з точки зору цифрового та реального життя, а також те, хто відповідає за надання високоякісних інтернет-послуг у різних регіонах.

**Організаційний процес**

Діяльність Ініціативної групи здійснюється на основі «Кодексу поведінки Молодіжної коаліції з питань управління Інтернетом (YCIG)».

«Кодекс поведінки Молодіжної коаліції з питань управління Інтернетом (YCIG)»: <https://ycigweb.wordpress.com/code-of-conduct/>

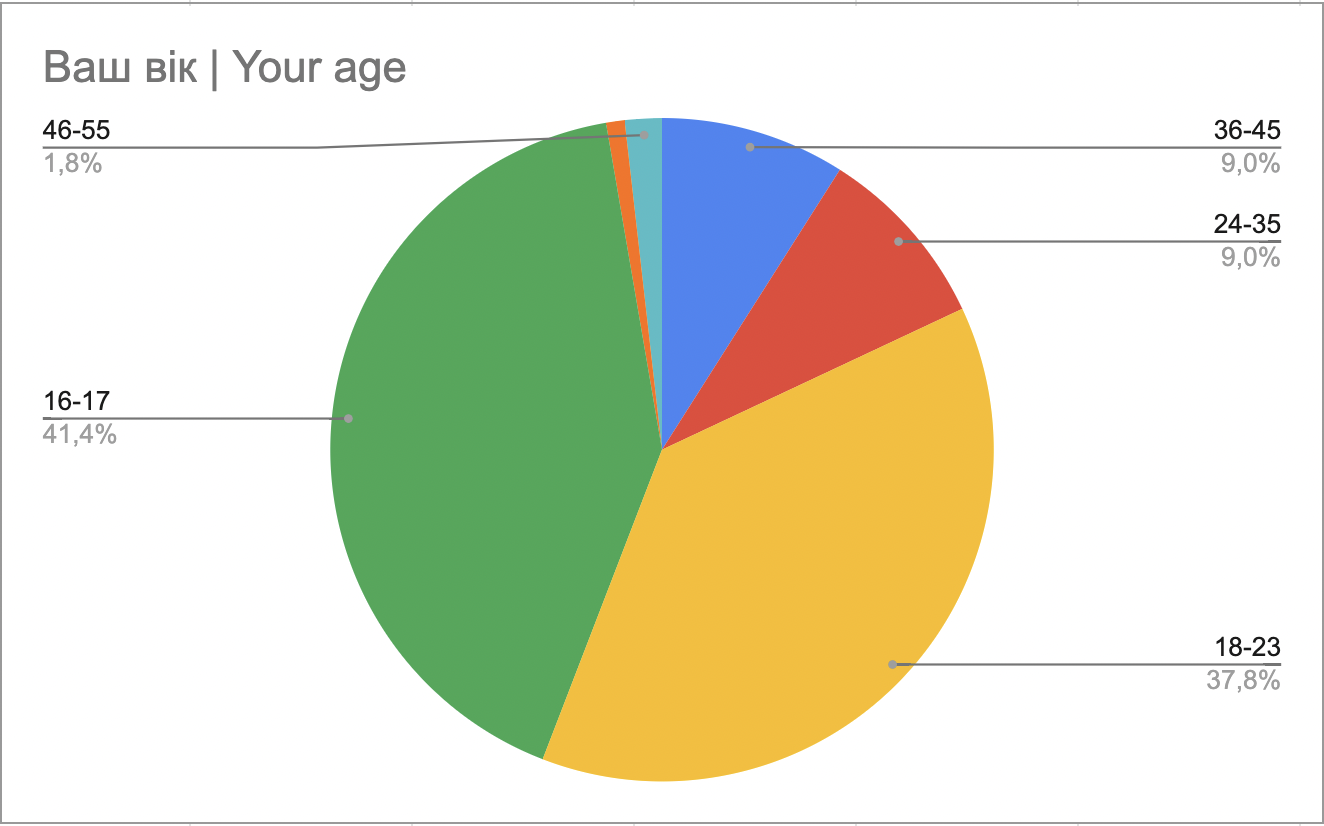
Ініціативна група Українського молодіжного форуму з управління Інтернетом була створена в лютому 2018 року в результаті досягнення консенсусу між учасниками та меценатами Молодіжного IGF-UA Pro, який відбувся 5 жовтня 2017 року в Києві. Під час заходу експерти обговорили створення нової платформи для залучення молоді до управління Інтернетом. Для цього на Молодіжному IGF-UA (лютий 2018 р.) Валерія Дубицька (Європейська Медіа Платформа) ініціювала створення багатосторонньої організаційної групи Молодіжного IGF-UA. Повідомлення про цю ініціативу надіслано до VIII IGF-UA (6 жовтня, igf-ua.org), Секретаріату IGF, EuroDIG, SEEDIG.

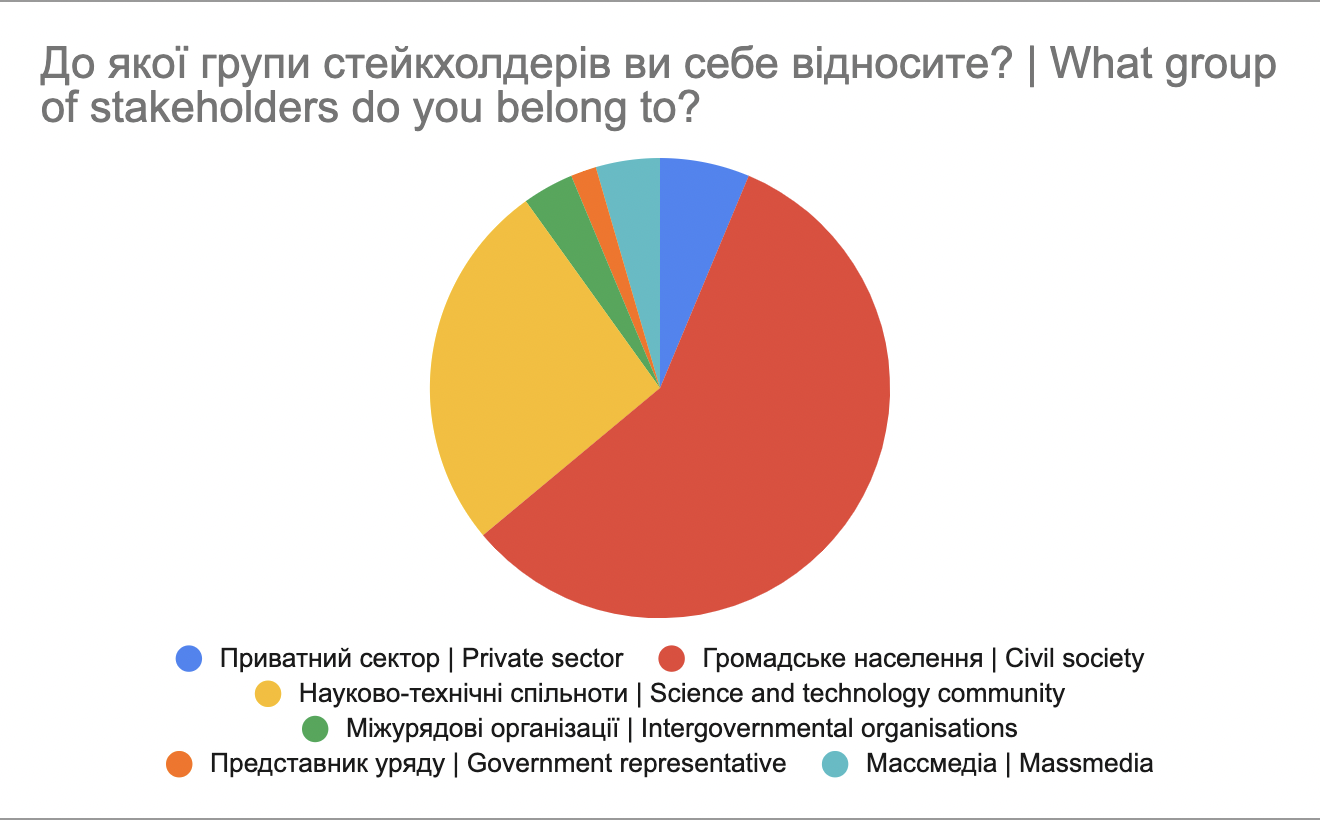
27 жовтня 2021 року на підставі рішення Оргкомітету Українського форуму з управління Інтернетом IGF-UA розпочалося створення Четвертого Українського молодіжного Інтернет-форуму (IV Молодіжний IGF-UA). Модератором заходу була призначена Анастасія Ткачук, незалежний експерт, представник Ініціативної групи Молодіжного IGF-UA, член Оргкомітету Українського форуму з управління Інтернетом.

**Учасники**

Оскільки IV Молодіжний IGF-UA проходив в режимі онлайн у форматі відео конференції, учасники могли приєднатися або через платформу Adamant, або переглянувши пряму трансляцію на YouTube.

Для того, щоб взяти участь в обговоренні та поставити запитання, учасник повинен був зареєструватися через онлайн-форму. На заході зареєструвалися 111 учасників та 62 гостей. Багато зареєстрованих учасників не змогли приєднатися до нас через платформу Adamant через технічні проблеми. Вони стежили за форумом через пряму трансляцію на YouTube.





Організатори та спонсори IV Молодіжного IGF-UA надали необхідні ресурси в рамках підготовки та проведення Форуму.

**Висновки**

Інформація про дату заходу, теми та умови участі поширювалася на офіційному сайті Молодіжного IGF-UA (https://youth-igf-ua.org), на сторінці у Facebook (https://www.facebook.com/YouthIGFUA), а також через інформаційні канали Малої академії наук України, Київського національного торговельно-економічного університету та інші канали поширення інформації.

Умови участі в Молодіжному IGF-UA виконано відповідно до Основних принципів Молодіжної коаліції з питань управління Інтернетом (прописані в Статуті та Кодексі етичних норм).

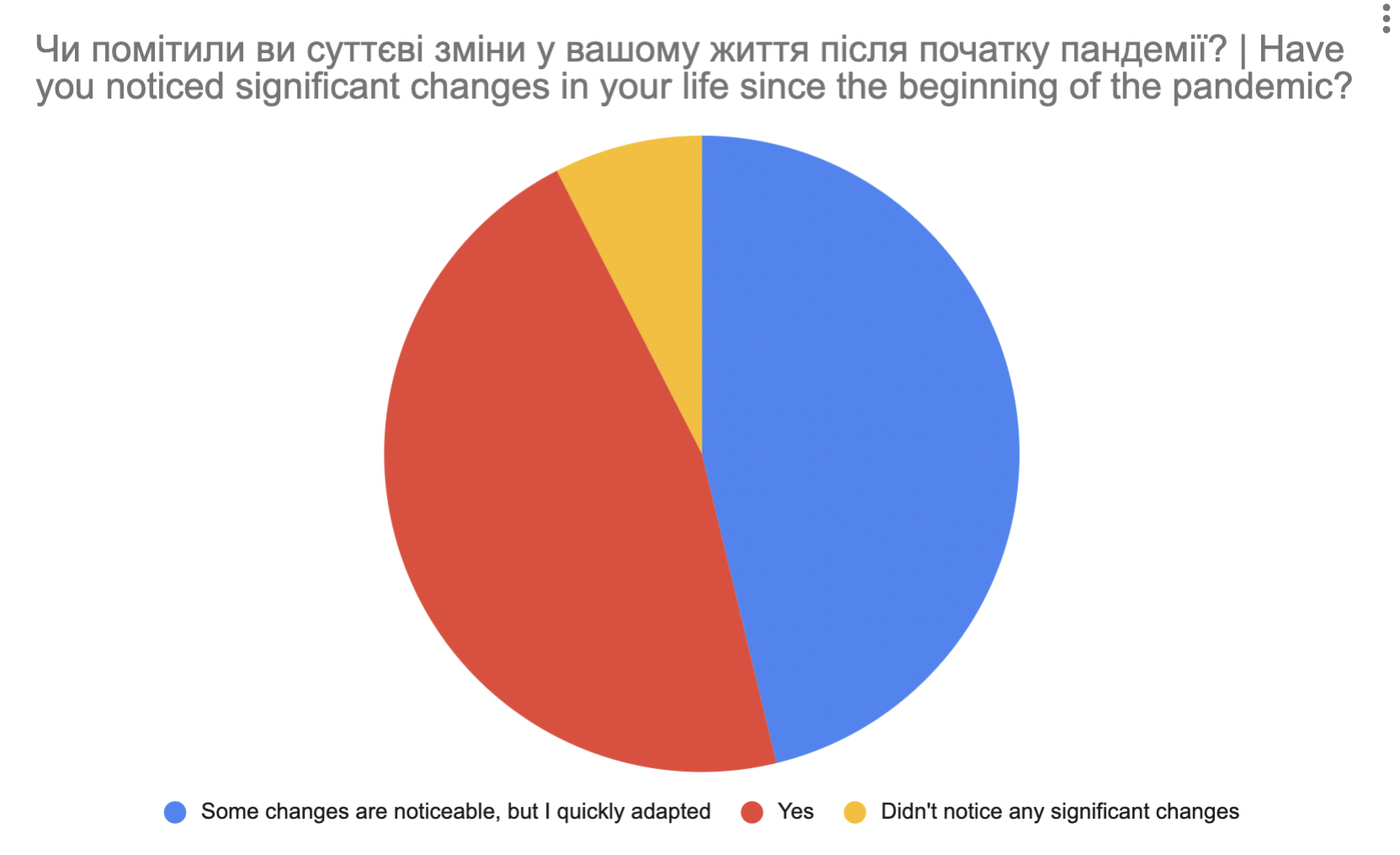
Ініціативна група отримала 12 пропозицій щодо тем для обговорення. На основі отриманих заявок була сформована наступна програма:

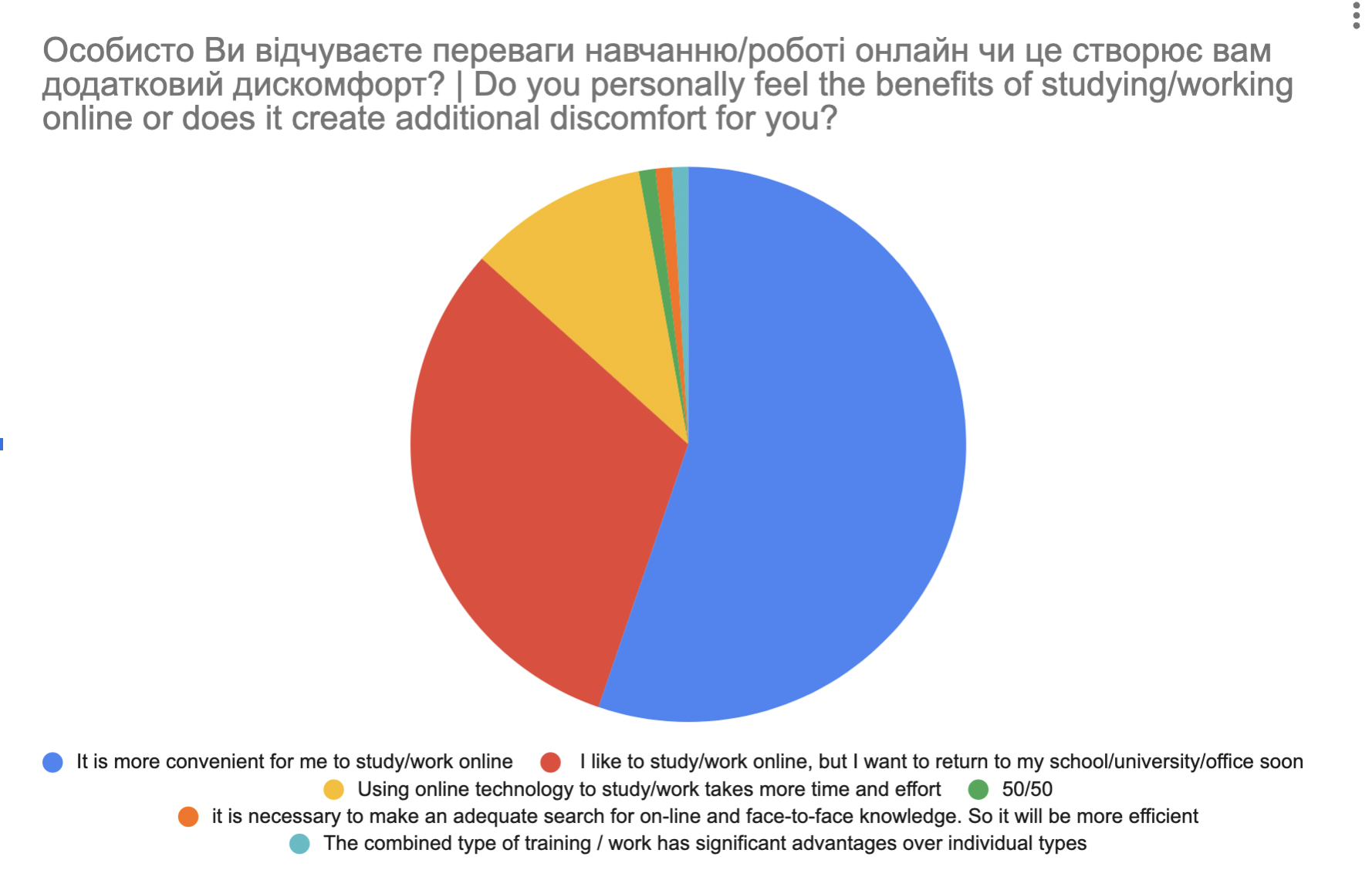
1. Вітальне слово від організаторів та спонсорів (Олексій Семеняка, Михайло Анісімов, Віталій Мороз, Валентин Протопопов, Алехандра Прієто)
2. Секція 1: Молодіжні програми Internet Society (Алехандра Прієто), RIPE NCC (Олексій Семеняка), ICANN (Михайло Анісімов).
3. Секція 2: «Зелений» Інтернет (Валентин Протопопов)
4. Секція 3: Кібербезпека з точки зору української молоді (Ілля Правосуд)
5. Секція 4: Досвід участі в міжнародних молодіжних програмах (Валерія Дубицька, Ейлін Квіпонія, Ліза Куковська)
6. Секція 5: Гейміфікація майбутнього (Павло Кравченко, Наталія Каташинська)
7. Секція 6: Інтернет 101 (Ваан Овсепян)
8. Підведення підсумків (Анастасія Ткачук, Оксана Приходько)

Модератором заходу була Анастасія Ткачук, незалежний експерт, представник Ініціативної групи Молодіжного IGF-UA, член оргкомітету Українського форуму з управління Інтернетом.

Відповідно до рішення Оргкомітету IGF-UA всім учасникам Молодіжного IGFUA була надана можливість надіслати доповіді або тези для друкованого збірника IV Молодіжного IGF-UA (за стандартами MAS).

Під час реєстрації учасникам було запропоновано відповісти на деякі запитання щодо впливу пандемії COVID-19 на їхнє життя. Запитання та результати опитування наведені нижче:





Під час IV Молодіжного IGF-UA ми обговорили багато важливих питань, які потребують участі молодого покоління та сформували наступні меседжі:

1. Онлайн-формат роботи та навчання не є панацеєю від викликів пандемії. Люди відчувають дискримінацію своїх прав і моральний тиск, коли не можуть брати участь у процесах навчання та відвідувати заходи офлайн. Освітня система потребує поєднання онлайн- та офлайн-форматів.
2. Відновлювальні джерела енергії є необхідністю для України в нинішніх умовах. На теперішній час галузь швидко розвивається, і молодь повинна реалізувати свої здібності в цій сфері.
3. Щоб інформувати молоде покоління про можливі кіберзагрози, нам потрібна потужна державна програма. Можна розпочати із зустрічей з учнями та їхніми батьками. Люди повинні знати, як виявляти, запобігати кіберзлочинності та куди повідомляти про неї.
4. Теорія ігор широко використовується в різних сферах нашого життя, починаючи від соціальних мереж і закінчуючи освітньою системою. Гейміфікація майбутнього вже триває, і вона може здійснюватися в цифровому (наприклад, Metaverse) або в звичайному офлайн-форматі (Критикотики).
5. Щоб захистити свої права на якісні інтернет-послуги, варто знати, хто несе відповідальність за це у Вашій країні. Ця інформація має бути широко розповсюдженою та легкою в доступі.

*Відеоматеріали та презентації IGF-UA-2021 – див.* [*https://i-ua.tv/projects/igf-ua/28047-12-i-ukrainskyi-forum-z-upravlinnia-internetom*](https://i-ua.tv/projects/igf-ua/28047-12-i-ukrainskyi-forum-z-upravlinnia-internetom)

**КОНТАКТИ**

Організаційний комітет IGF-UA

[www.igf-ua.org](http://www.igf-ua.org)

[info@igf-ua.org](mailto:info@igf-ua.org)

tel/fax: +38 044 278-2925

04053, м. Київ, вул. Олеся Гончара, 15/3, офіс 22