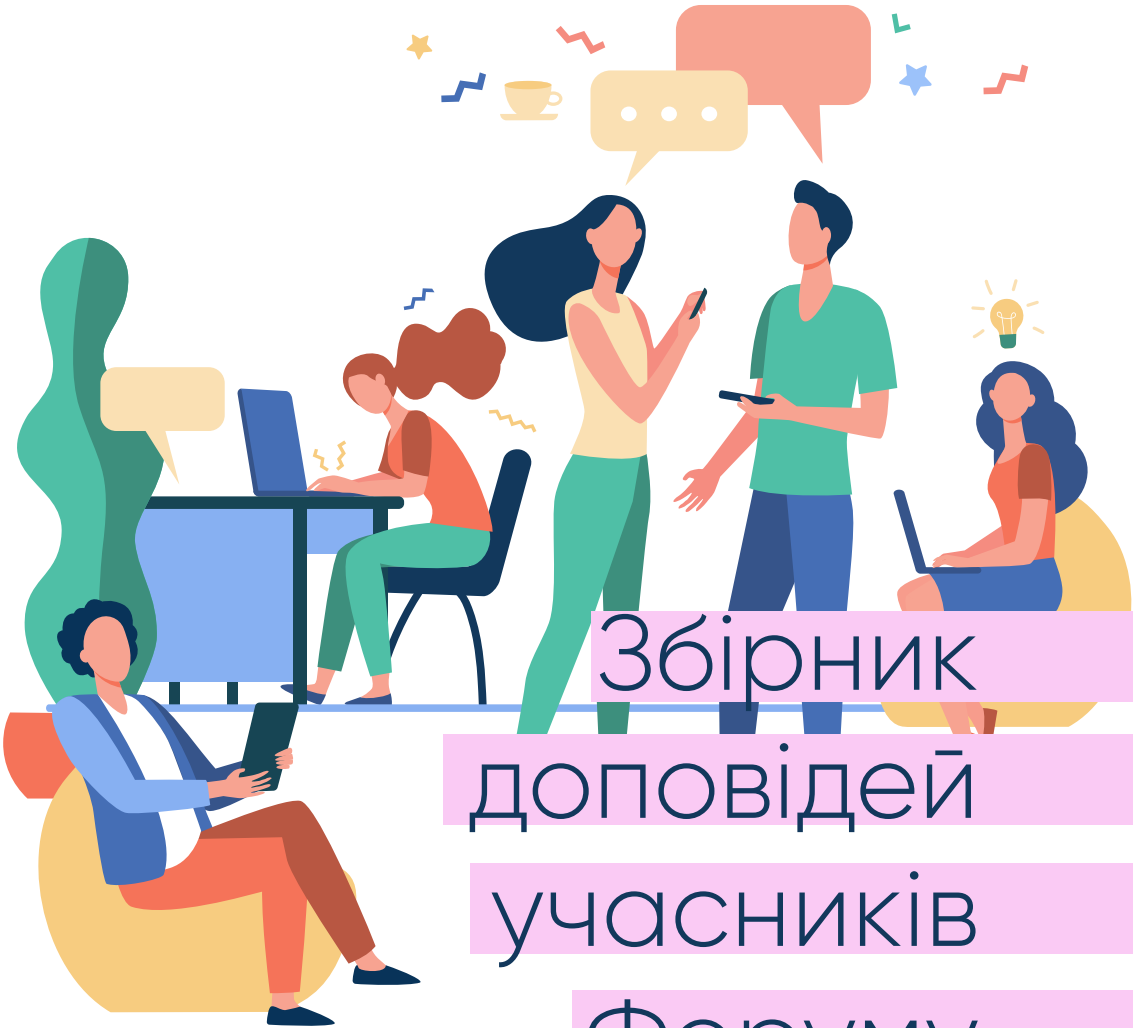
III Youth Internet Governance Forum Ukraine



Збірник доповідей учасників Форуму

SOCIAL NETWORK

Зміст

Розділ І.
Організатори, спонсори та організації, що підтримали Третій Молодіжний Український Форум з управління Інтернетом (Youth IGF-UA)

ІНТЕРНЕТ АСОЦІАЦІЯ УКРАЇНИ (ІНАУ)

- найбільше об'єднання на телеком-ринку, понад 220 членів із всіх регіонів України: оператори, провайдери, постачальники інтернет-послуг та обладнання, медіа, вузи;
- 20 років досвіду відстоювання інтересів учасників ІКТ-ринку;
- представництво в органах влади через участь в Громадських радах, заходах і нарадах;
- міднародні комунікації: участь в EURALO, Cybercrime@EAP, IGF, міжнародних заходах;
- 10 Комітетів, що охоплюють основні сегменти ІКТ, і ряд робочих груп;
- ряд щорічних Конференцій та Форумів, які проводить ІнАУ;
- власні проекти, в т.ч. Дочірнє підприємство UA-IX, щорічний Конкурс шкільних сайтів, Дослідження інтернет-аудиторії, Дослідження ринку доступу до Інтернету, Реєстр викраденого обладнання, Проект «Провайдер SOS», Гаряча лінія Skarga.ua

4 КРОКИ ДЛЯ ВСТУПУ В ІНАУ:

- заповніть заяву про вступ до ІнАУ (http://inau.ua, пункт головного меню «Вступ»);
- отримайте 2 рекомендації Дійсних членів ІнАУ (прямо на заяві підпис керівника і печатку);

- надішліть заяву в офіс ІнАУ і отримайте статус Кандидата в члени ІнАУ;
- рішення про вступ до ІнАУ приймає З'їзд ІнАУ (скликається щорічно).

ЩО ОТРИМУЮТЬ ЧЛЕНИ ІНАУ

- захист при незаконних діях відносно члена ІнАУ з боку органів влади або третіх сторін;
- інформаційну підтримку, включаючи моніторинг законодавства;
- PR-підтримку членів ІнАУ інформаційними засобами Асоціації;
- запрошення до безкоштовної або пільгової участі у ключових заходах сфери ІКТ;
- можливість врахування пропозицій при підготовці змін до нормативних актів у сфері ІКТ;
- можливість впливу на розвиток мережі UA-IX;
- знижки на послуги мережі обміну трафіком UA-IX;
- можливість необмеженого користування Реєстром викраденого обладнання;
- отримання даних досліджень: дослідження ринку доступу до Інтернету, показники розвитку сегментів інтернет-реклами, тощо;
- комунікацію з колегами під час конференцій, з'їздів, неформальних заходів, використання робочої розсилки ІнАУ members для знайомства, обміну досвідом та розвитку бізнесу.
- необтяжливі членські внески: Дійсний член 5 тис грн, Асоційований – 2,5 тис грн/рік.

ЗВЕРТАЙТЕСЬ В ІНАУ

- secretary@inau.ua
- *www.inau.ua*; www.facebook.com/inau.org.ua/
- 04053, м Київ, вул. О. Гончара,15/3,офіс 22,
  тел./факс: +38 (044) 278-2925

ГРОМАДСЬКА СПІЛКА “КОМІСІЯ З ПИТАНЬ НАУКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ” (ГС КПНІТ)

ГС КПНІТ ставить собі на меті створення сприятливих умов для розвитку суб’єктів малого та середнього підприємництва, що беруть участь у розбудові інформаційного суспільства та електронних комунікацій.

Одним із головних напрямів роботи ГС КПНІТ є налагодження системної роботи з органами державної влади, сприяння взаємовідповідальним стосункам між бізнесом і владою та відстоювання і захист прав своїх членів.

Основними завданнями ГС КПНІТ є:

- участь у законотворчій діяльності з питань розвитку електронних комунікацій, користування радіочастотним ресурсом, з питань телебачення та радіомовлення, розвитку мережі Інтернет, вільного доступу громадян до інформації;
- сприяння та консолідації зусиль державних установ та представників бізнесу щодо:
  - дерегуляції та державний нагляд (контроль) у сфері господарської діяльності;
  - оптимізації нормативного-правового врегулювання дозвільно-погоджувальних процедур, створення умов для інтеграції у світовий інформаційний простір;
  - питань інформатизації, науково-технічного та інноваційного розвитку;

- розвитку сучасних електронних банківських технологій, електронного документообігу, електронного цифрового підпису та захисту інформації;
- протидії кіберзлочинності та забезпечення інформаційної безпеки;
- доступу до інфраструктури будинкової розподільної мережі та до інфраструктури об'єкта будівництва;
- тощо.

Для виконання статутних завдань представники ГС КПНІТ беруть участь в організації та проведенні різноманітних заходів, зокрема:

- у роботі Комітетів Верховної Ради України;
- у робочих засіданнях центральних органів виконавчої влади та регуляторних органів;
- у засіданнях Робочих груп (міжвідомчих робочих (координаційних) груп (рад);
- у різноманітних нарадах та зустрічах;
- у засіданнях Громадських рад;
- заходах інститутів громадянського суспільства;
- у міжнародних конференціях, Форумах, симпозіумах, засіданнях міжнародних організацій, круглих столах, прес-конференцій, семінарах та презентаціях, тощо.

RIPE NCC - некомерційна асоціація, яка об'єднує своїх членів, і виконує функції регіональної Інтернет-реєстратури (RIR). Вона уповноважена Інтернет-спільнотою розподіляти IP-адреси (IPv4 і IPv6) і привласнювати номери автономних систем (AS) в межах свого регіону обслуговування (76 країн Європи, Центральної Азії та Близького Сходу). Крім цього, RIPE NCC проводить наукові дослідження, займається підтриманням проектів, важливих для функціонування мережі Інтернет як в регіоні, так і в усьому світі, а також є секретаріатом широкого співтовариства RIPE.

Взаємодія з навчальними та науковими інститутами є важливим напрямком діяльності організації. Так, RIPE NCC проводить «академічні дні» з різних тем, таких як: основи Інтернету; маршрутизація; використання бази даних RIPE; протокол IPv6; RPKI; управління інтернетом. Вони проводяться як в очній формі, так і онлайн. RIPE NCC готовий співпрацювати з усіма навчальними та науковими установами, зацікавленими у цих заходах. Організовуються вони досить швидко: достатньо зв'язатися з RIPE NCC для узгодження точної тематики зустрічі, після чого поширити інформацію про неї і зібрати учасників, а RIPE NCC надасть контент.

Іншим важливим починанням є RIPE Academic Cooperation Initiative (RACI). RACI пов'язує академічні кола зі спільнотою RIPE. Це дозволяє вченим ділитися своїми дослідженнями з провідними технічними діячами в світі Інтернету і отримувати ідеї про їх розвиток.

RIPE NCC зацікавлений у дослідженнях в наступних областях:

- Мережеві вимірювання та аналіз
- Впровадження IPv6
- Маршрутизація на основі протоколу BGP
- Безпека мереж
- Управління інтернетом
- Пірінг і міжмережева взаємодія
- Інтернет речей (IoT)
- Сталий розвиток ІКТ

Студенти та дослідники, відібрані в рамках RACI, отримують:

- Безкоштовні квитки на одну з майбутніх зустрічей (RIPE Meeting, MENOG, ENOG, SEE або RIPE NCC Day), включаючи урочисті вечері,
- Фінансову допомогу, що покриває супутні переміщення та проживання.

Крім того, відібрані кандидати матимуть можливість:

- Представити свої факультети та інститути на одному з міжнародних відкритих форумів, серед учасників яких є представники світових технологічних лідерів,
- Зробити доповідь про свої результати на одній з майбутніх зустрічей (RIPE Meeting, MENOG, ENOG, SEE або RIPE NCC Day),
- Отримати як цінні відгуки, так і можливі зауваження щодо їх робіт з боку галузевих експертів та учасників,
- Ознайомитися з середовищем професійного спілкування з учасниками з різних країн і організацій, а також дізнатися їх точку зору на актуальні теми,
- Зав'язати контакти з тими, хто рухає і розвиває інфраструктуру та управління Інтернетом, поліпшивши свої перспективи кар'єрного росту і розвитку,
- Опублікувати свою роботу для технічної спільноти чи Інтернет-спільноти в цілому на платформі RIPE Labs.

Всі новини щодо RACI публикуються в тематичному списці розсилки (https://www.ripe.net/mailman/listinfo/raci-list).

Internet Governance Forum Support Association

The IGF and IGFSA

The Internet Governance Forum (IGF) has proven its worth to the international community and to all those who are committed to an open, thriving, and accessible Internet. The open and inclusive dialogue and debate that it provides is critical to the Internet's continued evolution. The IGF by now is the major annual event for all stakeholders to gather as equals and discuss Internet policy related issues. In 2015 the United Nations General Assembly recognized the value of the IGF and extended its mandate for another 10 years. Part of the IGF success story is the growth of National and Regional IGF Initiatives (NRIs) in all continents, triggered off by the global IGF.

The IGF is funded through voluntary contributions and therefore in constant need of funding. IGFSA's purpose is to promote and support the global IGF as well as NRIs. It is a not-for-profit association incorporated in Switzerland created to broaden the donor base and to provide stable and predictable funding from individuals and entities who want to support the IGF as well as the NRIs. IGFSA aims to build on and complement existing funding sources and strengthen the linkages between the global IGF and the NRIs and provides financial support for the IGF Secretariat through contributions to the UN IGF Trust Fund.

IGFSA's role as a channel for additional funding for the IGF Trust Fund has been recognized by the UN through an exchange of letters. To date, IGFSA has contributed USD 280,000 to the UN IGF Trust Fund and USD 429,500 to the NRIs.

WSIS 2016 – Photo credit: ITU Pictures (Flickr)

Membership

Join us now to become a member! By joining IGFSA you show your support for the IGF and help keep the IGF the go-to event for everyone who is interested in the Internet and its governance.

Individuals, organizations and companies are encouraged to sign up for IGFSA membership to show their support for the growth and success of the IGF and the growth and increased role of the NRIs. To become a member of the IGFSA, please visit www.igfsa.org to complete the membership sign up process and to pay your annual membership dues online.

Membership fees are:
Individuals: USD 25 -- Companies/Organizations: USD 100

The IGFSA's core mission is to raise funds to support the IGF and the NRIs. Members are encouraged to contribute above the minimum membership fees. Contact IGFSA, at info@igfsa.org to become a member or funding partner.

Reinforcing the NRI Landscape

National and Regional IGF Initiatives (NRIs) are a major outcome of the IGF. They were not planned, but emerged spontaneously on all continents. What they have in common with the global IGF is their multistakeholder, bottom-up, open and inclusive character. Good Internet governance starts at the national and regional levels and the NRIs can thus provide feedback from the grassroots and provide input into the program for the annual Global IGF in a true bottom-up process. Strengthening the linkages between the NRIs and the global IGF is part of the core IGFSA mission.

Since its inception in 2014 the IGFSA was able to make 40 financial contributions to Regional and Sub-Regional and 135 contributions to National IGF Initiatives. NRIs require significant support in the form of human and financial resources. IGFSA will continue to provide support to NRIs, providing USD 3500 for Regional and Sub-Regional and USD 2000 USD for National IGF Initiatives. (The list of the NRIs who benefited from IGFSA sponsorship is available on page 2).

IGFSA works closely with the IGF Secretariat to promote and identify Initiatives that would benefit from our support.

"We are grateful to the IGFSA for supporting the logistics of the first national IGF in the English speaking Caribbean. To ensure the broadest participation, we innovated with a YouTube Live channel to stream the event beyond the confines of the physical location, and support remote participants with full participation. This TTIGF was extremely well received, and has been recognized as a leading IG event in the entire English speaking Caribbean. We are already planning the 2018 TTIGF, and are working with other countries in the region to share our IGF planning process." -T&T IGF

Above: Representatives of NRIs who benefited from IGFSA funding at the African IGF 2018 in Khartoum.

NRI Map

Map courtesy of IGF Secretariat

List of IGFSA sponsored NRIs: National NRIs

- Afghanistan IGF
- Albania IGF
- Argentina Internet Dialogues
- Armenia IGF
- Barbados IGF
- Belarus IGF
- Benin IGF
- Bolivia IGF
- Bosnia and Herzegovina IGF
- Chad IGF
- Colombia IGF
- DR Congo IGF
- Costa Rica IGF
- Croatia IGF
- Dominican Republic IGF
- Ecuador IGF
- El Salvador IGF
- Ghana IGF
- Georgia IGF
- Guatemala IGF
- Haiti IGF
- Indonesia IGF
- Kenya IGF Week
- Malawi IGF
- Mauritius IGF
- Namibia IGF
- Nepal IGF
- Nigeria IGF
- North Macedonia IG
- Panama IGF
- Paraguay IGF
- Rwanda IGF
- San Salvador IGF
- Senegal IGF
- Slovenia IGF
- Sri Lanka IGF
- St. Vincent and the Grenadines IGF
- Tanzania IGF
- The Gambia IGF
- Trinidad & Tobago IGF
- Tunisia IGF
- Ukraine IGF
- Uganda IGF
- Vanuatu IGF
- Venezuela IGF

Regional & Sub-Regional NRIs

- African IGF
- Asia Pacific Regional IGF
- Caribbean IGF
- Central Africa IGF
- Central Asia IGF
- East Africa IGF
- EuroDIG
- LACIGF
- North Africa IGF
- Pacific IGF
- SEEDIG
- Southern Africa IGF
- West Africa IGF

The General Assembly and the Executive Committee

The General Assembly is the supreme governing body of the Association. The Executive Committee is the decision-making body of the Association which manages IGFSA's activities. Its tasks include preparation of the annual budget for approval by the General Assembly, engaging in fundraising and outreach to build awareness of the IGF and the importance of supporting the IGF. The Executive Committee is currently composed as follows:

Marilyn Cade
Edmon Chung
Avri Doria
Makane Faye
Nigel Hickson
Markus Kummer
Jimson Olufuye
Nilmini Rubin
Eduardo Santoyo

The Executive Committee is chaired by Markus Kummer. Jennifer Chung serves as the Secretary .

Become Part of the ICANN Community

The Internet continues to shape our lives every day. You can be part of the community that helps shaping the future of the Internet and its system of unique identifies. There really is no better time to the diverse ICANN community. We are using robust remote participation tools to ensure the policy development process moves forward in a meaningful way, especially during the COVID-19 pandemic.

There's a wealth of information available to help you learn and come up to speed, including the ICANN Learn platform. If you're interested in participating, there are two programs that are aimed at helping you join the community:

- Fellowship Program
- NextGen Program

The goal of the ICANN Fellowship Program is to strengthen the diversity of the multistakeholder model by fostering opportunities for individuals from underserved and underrepresented communities to become active participants in the ICANN community.

Fellows are exposed to the workings of the ICANN community, are assigned a mentor, and receive training across different areas of knowledge and skill building before, during, and after an ICANN Public Meeting. Travel assistance to attend the meeting is also provided.

Fellowship participants come from a variety of backgrounds, providing a gateway for people around the world to become equipped in shaping the future of the Internet tomorrow. There are certain eligibility criteria for the Fellowship Program, and those can all be found on our fellowship web page, (https://www.icann.org/fellowshipprogram) but the main one is that the applicant should be at least 21 years old.

Another initative aimed at increasing involvement in ICANN is the NextGen@ICANN program; which looks for the next generation of individuals who are interested in becoming actively engaged in their regional communities and in shaping the future of global Internet policy.

Through the NextGen program, ICANN provides coaching and travel assistance to students from the regions where the ICANN meeting is taking place. It does so through broadening participation in ICANN by providing opportunities for university students to attend ICANN Public Meetings. It is intended for undergraduate and graduate students aged 18-30 studying in the region where the ICANN Public Meeting is taking place.

More information on the criteria can be found here: https://www.icann.org/public-responsibility-support/nextgen

Visit our website, icann.org, to learn more. If you are interested in one of these program and want to participate, please contact Mikhail Anisimov, Global Stakeholder Engagement manager for Eastern Europe and Central Asia by mikhail.anisimov@icann.org for any further questions.

IGF Youth Ambassadors Program

The main goal of the IGF Youth Ambassadors Program is to empower young adults from all around
the world by:

- Building their capacity through training.
- Fostering a new cadre of young Internet leaders who are motivated to learn, engage, and act within their region and beyond.
- Partnering with organizations to broaden the depth and breadth of the program.
- Reinforcing the importance of multi-disciplinary leaders in fostering the sustainability, robustness, security, stability and development of the Internet.
- Promoting youth citizenship, diplomacy, volunteerism and community service as key aspects of next generation leadership.
- Broadening their experience and enabling their participation in public policy debates.
- Providing them with opportunities to participate in the global Internet ecosystem and to interact and engage with the broader Internet Governance community.
- Increasing their visibility and preparing them to deliver more meaningful impacts at the local, regional and global levels.
- Mobilizing youth beyond IG-specific topics.

Program Components

A. 3-phase Selection Process

1. Online Applications

   The first phase of the selection process is based on Online Applications.

   The selection committee attempts to achieve professional, geographical, and gender diversity in the overall selections.

2. 4-week Online Internet Governance Course

   Those selected at phase 1 (up to 150 individuals) take a 4-week online course on Internet Governance.

   All participants are grouped into classes, each with a dedicated expert moderator to facilitate the learning process. The top ones (up to 50) proceed to the next phase.

3. Paper Writing

   The top performers during the online course phase will be required to write a paper on an existing or emerging area in Internet governance, leveraging the learnings from to course. The individuals submitting the best papers will be selected as IGF Youth Ambassadors (up to 30).

B. Webinar Series

Those selected as IGF Youth Ambassadors (up to 30) participate to Webinar Series led by global Internet Governance experts to deepen their knowledge, present their projects/ideas and be prepared for the IGF.

C. Attending the IGF

IGF Youth Ambassadors receive support to attend the Global Internet Governance Forum.

D. Collaborative Leadership Exchange

IGF Youth Ambassadors will attend a dynamic leadership session with Internet Society community members, youth representatives from other programs, Internet Society staff and other IGF attendees. This session takes the form of an unconference, with the agenda being crowdsourced by attendees, and breakout groups facilitated to create

pockets of common interest and interaction. The goal here is to build/deepen relationships and foster community around youth engagement.

Continued Success

The Internet Society's IGF Youth Programs have provided opportunities for leadership capacity building for the participants (meet 2019 and 2020 IGF Youth Ambassadors!). They concretely used their synergies to build projects by their own efforts:

- The Internet Society Youth Special Interest Group (SIG)/Youth Observatory was created to use the power of the Internet to develop abilities in young adults and encourage them to participate in the development of the Internet environment and its governance.
- Youth contribution to regional meetings increased, such as the African Internet Summit, EuroDIG, NRIs...
- Many Youth become Internet Society Chapter Delegates, SIG Leaders and/or eLearning Expert Tutors.
- New civil society organizations were created, such as Digital Grassroots, an initiative that aims at increasing digital literacy amongst the young population globally in order to promote their activity as stakeholders in the Internet ecosystem at the most basic levels.
- Several are now leading the Youth Coalition on Internet Governance.
- Youth Declarations and Recommendations created by ISOC Youth have been read and supported during the IGF.
- Some IGF Youth Ambassadors have been invited to participate to high-level panels at the IGF meetings.

Компанія «Адамант»

«Адамант» є однією з перших Інтернет-компаній в Україні. Ще наприкінці 90-х років компанія «Адамант» започаткувала масову трансляцію телевізійних та радіопрограм у мережі Інтернет, відкрила власний супутниковий телепорт Стокгольм-Київ, ввела пакетні послуги на доступ до Інтернету, розпочала комплектацію власних сертифікованих серверів і персональних комп'ютерів.

Спільно з головним редактором об'єднаного прес-центру «Вибори-99» журналістом Сергієм Набокою реалізувала перший в Україні Інтернет-проект обговорення виборів в Інтернеті - «Elections 99». В чаті (форумі) цього проекту приймали участь перші особи держави та кандидати у Президенти України.

Компанія «Адамант» разом з іншими операторами та провайдерами телекомунікацій стала ініціатором створення Української точки обміну Інтернет-трафіком (UA-IX) у 2000 році.

За 29 років діяльності компанією було реалізовано чимало цікавих проектів національного масштабу і зараз вона впевнено підкорює майбутнє!

Канал I-UA.TV

Креативний україноцентричний незалежний інформаційно-аналітичний волонтерський майданчик громадської спілки Національна Асамблея України, створений безпосередньо зусиллями її учасників. Ми забезпечуємо інформаційну онлайн підтримку багатьох міжнародних заходів в галузях культури, політики, науки та технологій та інших, що допомагають розвитку України.

Ми працюємо з листопада 2016 року створюючи правдивий і якісний контент якій можна побачити як на просторах інтернету так і в форматі OTT для кабельного мовлення. Канал виступає партнером багатьох цікавих вітчизняних і міжнародних конференцій і форумів, зокрема:

1. Український форум з управління Інтернетом IGF-UA - *https://i-ua.tv/stream/27189-11-i-ukrainskyi-forum-z-upravlinnia-internetom-igf-ua*
2. Дні електронних комунікацій - *https://i-ua.tv/tech/27719-dni-elektronnykh-komunikatsii-2021*
3. Global Cybersecurity Summit (GCS) - *https://i-ua.tv/stream/25462-global-cybersecurity-summit-day-1-original-audio*
4. RIPE NCC Days - *https://i-ua.tv/stream/25717-ripe-ncc-days-kyiv-day-1-ukrainska-mova*
5. UADOM - *https://i-ua.tv/stream/26023-konferentsiia-domennoi-industrii-uadom2019*
6. UAMobile - *https://i-ua.tv/stream/25519-ua-mobile-2017*
7. PKI Forum UA - *https://i-ua.tv/stream/26153-zakhyst-personalnykh-danykh-u-sferi-tsyfrovoi-ekonomiky-2*

8. Horasis China Meeting - *https://i-ua.tv/stream/25560-horasis-china-meeting-14-october-2018-english*
9. Міжнародний конкурс молодих піаністів пам'яті Володимира Горовиця - *https://i-ua.tv/stream/25527-khii-mizhnarodnyi-konkurs-molodykh-pianistiv-pam-iati-volodymyra-horovytsia-24-kvitnia-2019r*
10. Міжнародний Гранд Форум BIT&BIS-2021- *https://i-ua.tv/stream/27528-mizhnarodnyi-hrand-forum-bit-bis-2021*

Та дуже багато інших - *https://i-ua.tv/stream*

Міжнародна громадська організація
“Європейська Медіа Платформа” *eump.org*

Міжнародна громадська організація **“Європейська Медіа Платформа” (ЄМП)** була зареєстрована Міністерством юстиції України 19 квітня 2010 року.

Задекларована місія ЄМП – просування європейських стандартів в сфері медіа та інфомаційного суспільства в Європі, в першу чергу на пострадянському просторі.

Пріоритет ЄМП – (згідно з рішенням Генеральної Асамблеї ЄМП 2015 року) – адвокація мультистейхолдерного підходу до процесу ухвалення законодавчих, регуляторних та інших рішень в цифровій сфері, сфері електронних (теле) коммунікацій, кібербезпеки, захисту персональних даних, цифрової освіти тощо.

Проєкти ЄМП (реалізовані та ті, що реалізуються саме зараз):

- “Налагодження співпраці стейкхолдерів в процесі інтеграції України в Єдиний цифровий ринок ЄС” (що реалізується за підтримки Європейського Союзу та Міжнародного Фонду «Відродження» в межах грантового компоненту проекту EU4USociety) – в процесі реалізації – *http://eump.org/2021-April-21/*
- “Інтеграція України до Єдиного цифрового ринку Європи: перетворення перешкод на вікна можливостей” – *http://eump.org/round-table-2019-06-07-uk/index.html*
- щорічне опитування на тему “Кібербезпека очима української молоді” – *http://eump.org/youth-and-cybersecurity/index.html*
- підтримка Yoth IGF-UA – *http://eump.org/youth-in-internet-governance/index.html*

Сьогодні Київська Мала академія наук – це близько 9000 школярів м. Києва, які займаються науково-дослідницькою діяльністю, це 36 колективних членів, десятки партнерів – закладів вищої освіти та науково-дослідницьких інститутів, а також 120 педагогів, серед яких 41 науковець, у тому числі – 1 член-кореспондент АПН України. 39 – мають державні нагороди та нагороди МОН України та Департаменту освіти і науки КМДА.

Варто зазначити, що унікальність діяльності Київської МАН полягає у тому, що саме тут, завдяки науково-дослідницькій діяльності в секціях академії, лабораторіях закладів вищої освіти та науково-дослідницьких установ, учні можуть отримати знання й можливість створювати наукові проєкти, публікації у наукових виданнях та отримувати патенти у таких галузях науки, які взагалі не представлені в шкільній програмі: мистецтвознавство, археологія, етнологія, медицина, теологія, соціологія, філософія, педагогіка, астрофізика, медіапсихологія, гідрологія, матеріалознавство, архітектура та дизайн та багатьох інших. За останні 3 роки у Київській МАН було створено нові відділення – суспільних комунікацій, «Київ-столиця» та відділення безпеки й оборони.

Завдяки постійній підтримці виконавчого органу Київської міської ради (Київської міської державної адміністрації) Департаменту освіти і науки м. Києва вихованці Київської МАН мають змогу займатися науковими розвідками на сучасному обладнанні, котре дозволяє «крокувати в ногу» з інноваційними досягненнями сьогодення.

Наукове кураторство діяльністю Київської Малої академії наук здійснює Національна академія наук України через президію Київської МАН, до складу якої входять 15 та член-кореспондентів академіків НАН України.

Київська МАН сьогодні – це стартовий майданчик для тих, хто прагне змінити на краще світ та своє життя за допомогою науки. Ми вчимо робити відкриття!

Розділ ІІ.
Доповіді та тези учасників Третього Молодіжного Українського Форуму з управління Інтернетом (Youth IGF-UA)

Роль молоді в питаннях управління Інтернетом – досвід України

Дубицька Валерія
мНУО «Європейська Медіа Платформа», Київ
vsd2007@gmail.com

Both the world community and Ukraine still need to take certain steps towards full and comprehensive involvement of young people in Internet governance. The voice, opinion and experience of young people should not just be considered, but also perceived at the same level as all other stakeholders. At the same time, it is important to note that there are already best practices that should be taken into account when building a youth community in Ukraine. Only through joint efforts this process will be organically implemented in the overall development of Internet governance.

В останні роки в глобальній екосистемі управління Інтернетом спостерігається збільшення кількості молоді (студентів і молодих фахівців). Крім того, молодь становить значний відсоток користувачів Інтернету в усьому світі. Не можна не погодитися, що молодь відіграє надзвичайно важливу роль у формуванні нашого цифрового майбутнього. Саме тому її потрібно включати в визначення процесів, принципів і політики, що регулюють питання управління Інтернетом.

Варто відмітити, що світовій спільноті, і Україні зокрема, потрібно зробити більше щодо включення молоді до управління Інтернетом. Окрім обізнаності з проблемами, варто відповісти на питання, а як саме молодь може насправді впливати на рішення у своїх громадах? Молодь потребує підтримки та заохочення з боку всіх стейкхолдерів.

Всі групи стейкхолдерів у сфері управління Інтернетом повинні мати можливість забезпечити інтеграцію молоді до плану глобальної сталості за допомогою цифрових технологій.

Необхідно відмітити, що помітну роль в залученні молоді відіграє Форум з управління Інтернетом (IGF), що був створений на Всесвітньому саміті з питань інформаційного суспільства в Тунісі у 2005 році як відповідь на заклики до створення міжнародної платформи, де можуть обговорюватися питання управління Інтернетом [3]. Форум з управління Інтернетом IGF, який відбувається на щорічній основі, є відкритим для всіх: урядів, громадянського суспільства, міжнародних організацій, викладачів та науковців, організацій приватного сектору, молоді та інших. Метою Форуму є вивчення питань, що стосуються Інтернету з найрізноманітніших точок зору: вони варіюються від суто технічних аспектів до питань прав людини. Всі учасники можуть вільно виступати та ділитися своїм досвідом. На відміну від багатьох інших форумів, IGF не має законодавчих чи виконавчих повноважень.

Хоча вплив Інтернету на молодь вже давно обговорюється на щорічних засіданнях Форуму з управління Інтернетом (IGF), де також брала участь молодь, молоді люди лише порівняно нещодавно в історії IGF взяли участь у реальних робочих процесах. Громада IGF дедалі більше визнає важливість залучення молоді до її робочих процесів – від розуміння ключових питань до планування заходів та активної участі. Більше того, було застосовано різноманітні підходи для включення поглядів та голосів молоді в обговорення політики Інтернету на щорічних засіданнях IGF та під час підготовчого процесу [6].

Найбільш помітне та постійне залучення молоді відбувається на національному, субрегіональному та регіональному рівнях, де молодіжні ініціативи IGF зосереджуються на об'єднанні молоді для обговорення питань управління Інтернетом та політики. Окрім цих видів практики, співтовариство IGF доклало багато зусиль для підтримки молоді для участі у щорічних засіданнях IGF, а також для створення різноманітних програм на національному, регіональному або міжнародному рівнях з метою підготовки, навчання та інформування молоді про процеси управління Інтернетом та основні теми [9].

Молодіжні ініціативи IGF створюються з метою заохочення та залучення молоді до предметної дискусії з питань управління Інтернетом. Очікується, що ці форми, а також національні, субрегіональні та регіональні IGF (NRI) [1] відповідають основним принципам IGF – бути відкритими, інклюзивними, некомерційними, мультистейкхолдерними впродовж усього підготовчого етапу та самого заходу, - відповідно до процесу прийняття рішень знизу вгору.

Окрім щорічних зустрічей IGF, однією з найпомітніших молодіжних ініціатив є Youth Coalition on Internet Governance (YCIG) [5]. Молодіжна коаліція з управління Інтернетом (YCIG) – це відкрита група для організацій та приватних осіб, яка представляє всі стейкхолдерні групи, готових співпрацювати задля заохочення та збагачення участі молоді у місцевих, регіональних та міжнародних дискусіях та процесах управління Інтернетом [2].

YCIG була створена для захисту прав дітей, молоді та молодих спеціалістів під час форумів та процесів управління Інтернетом. YCIG відкрита для всіх молодих людей та інших стейкхолдерів, що цікавляться проблемами управління Інтернетом. Як зареєстрована динамічна коаліція IGF, YCIG має місце для зустрічей на кожному форумі і об'єднує молодь з усього IGF для виявлення та обговорення відповідних питань, а також з метою об'єднати мережі для посилення голосу молоді у процесах управління Інтернетом.

Варто підкреслити, що молоді люди – це часта тема обговорень під час IGF, але на сьогоднішній день все ще недостатньо молодих голосів було почуто. Молоді люди не знаходять постійного місця за столом, щоб вільно і на одному рівні обговорювати всі питання управління Інтернетом.

Аналогічна ситуація стосується і України. Саме з метою об'єднати молодих людей, створити спільноту та просунути голоси молоді було започатковано проведення Youth IGF-UA в Україні. Для обговорення майбутнього Інтернету щодо таких питань, як відкритість, різноманітність, доступність, безпека та особиста недоторканність, і не в останню чергу , права людини.

Хоча процес становлення сталих процесів залучення молоді до управління все ще триває, важливо зазначити, що певні кроки були вже зроблені.

Так, 5 жовтня 2017 року мНУО «Європейська Медіа Платформа» (мНУО «ЄМП») (у партнерстві з America House Kyiv, IGF Support Association, Урядовим офісом з питань європейської та євроатлантичної інтеграції, Інститутом модернізації змісту освіти) організувала Youth IGF-UA Pro (в приміщенні America House Kyiv) напередодні VIII IGF-UA (6 жовтня 2017 р., Nivki-hall) [7].

Експерти та молодь обговорили питання створення нової платформи для участі молоді в управлінні Інтернетом. В ході дискусії було згадано про роль різних стейкхолдерів у процесі забезпечення кібербезпеки, розширення громадського доступу до високошвидкісного Інтернету, розвитку електронної комерції, можливостей для молоді, українського законодавства про телекомунікації щодо узгодження із законодавством ЄС.

Валерія Дубицька та інші члени команди мНУО «ЄМП» представили російський переклад набору інструментів NRI та основні принципи IGF [11]:

- Відкритість і прозорість;
- Інклюзивність;
- Підхід «знизу вгору»;
- Некомерційність;
- Мультистейкхолдеризм.

Для реалізації Молодіжного Форуму IGF-UA Валерія Дубицька (мНУО «ЄМП») ініціювала створення Молодіжної мультистейкхолдерної організаційної групи IGF-UA (лютий 2018 р.). Цю ініціативу підтримали Гліб Стригуненко (Урядовий офіс з питань європейської та євроатлантичної інтеграції) та Єгор Аушев (CyberGuard / приватний сектор), а також інші учасники Youth IGF-UA Pro. Повідомлення про цю ініціативу надходили до VIII IGF-UA (6 жовтня, igf-ua.org), Секретаріату IGF, EuroDIG, SEEDIG. З цими повідомленнями Молодіжна

мультистейкхолдерна організаційна група IGF-UA звернулась до Секретаріату IGF, VIII IGF-UA, EuroDIG та спільноти SEEDIG, щоб бути формально визнаними як Youth IGF-UA. Координатором Youth IGF-UA є Валері Дубицька, Європейська Медіа Платформа iNGO (valerie@eump.org).

Youth IGF-UA Pro відвідало 46 учасників, а 7 – взяли віддалену участь. Всі учасники представляють різні вікові групи, але 69,6% представляють вікові групи 15-25 та 25-35 років.

Щодо мультистейкхолдерного представництва, слід зазначити, що на основі проведених опитувань можна зробити висновок, що учасники Молодіжного IGF-UA Pro не мали повного розуміння поняття мультистейкхолдеризму. Наприклад, студенти приватних коледжів ідентифікують себе як приватний сектор, а студенти державних установ – як уряд.

22 травня 2018 року було організовано парламентську конференцію «Українська молодь та управління Інтернетом в контексті євроінтеграції» за підтримки голови комітету ВРУ Марії Іонової та депутата Європейського парламенту Міхала Боні. Більше 85 учасників взяли участь в заході, щоб обговорити роль української молоді в управлінні Інтернетом.

Наступним кроком залучення молоді і розвитку спільноти стало проведення Першого Youth IGF-UA. Youth IGF-UA відбувся 27 вересня 2018 року в Києві в бізнес-центрі UBI Hall і став першим заходом в рамках Днів Інтернету в Україні [8]. Під час Youth IGF-UA 2018 більше 100 молодих людей та представників різних стейкхолдерних груп відвідали захід.

Співорганізаторами заходів, за рішенням Оргкомітету, стали Інтернет асоціація України, Комісія з питань науки та інформаційних технологій Української ліги промисловців та підприємців, RIPE NCC, ISOC, IGFSA, Громадська організація «Інтерньюз-Україна», ICANN. Заходи пройшли за підтримки Комітету з питань інформатизації та комунікацій з громадськістю Верховної Ради України, Офісу програми з питань кіберзлочинності (Рада Європи), мНУО «ЄМП».

Для координації фінансових, матеріально-технічних та будь-яких інших цілей в рамках Організаційного комітету IGF-UA була створена Робоча група (РГ) з питань Youth IGF-UA. Оскільки на цей момент Youth IGF-UA не мала жодного статутного документа, того року було вирішено слідувати Принципам Українського форуму з управління Інтернетом IGF-UA (Протокол про наміри).

Незвичним, але вдалим досвідом стало проведення Форуму в різних форматах. Так, було проведено 6 різних секцій, кожна з яких мала свій формат і здобутки.

Впродовж секції «Моделі кіберризиків української молоді» (модератори: Олексій Барановський, Андрій Перцух, формат: World café) аудиторія поділилась на дві команди для визначення моделей кібер-ризиків, що зараз виникають перед молоддю. В результаті плідної роботи обидві команди прийшли до висновку, що головними ризиками, з якими молодь зустрічається в Інтернеті є:

- Віруси
- Хакерство
- Шахрайство
- Фішинг
- Спам
- Секстінг

Андрій Манкіш, представник CERT-UA і Уве Расмунсен підсумували результати обговорень молоді, зазначивши, що дуже важливим є сам факт того, що такі питання виходять за рамки індивідуального сприйняття, коли молодь опиняється один-на-один з ризиками в Інтернеті. Перехід від стану індивідуального до спільного є визначним моментом, що є відправною точкою для створення якісно нового підходу до розвитку моделей кібер-ризиків.

Впродовж секції «Соціальні мережі. Безпека дитини онлайн» (модератор: Тетяна Харківська, Ла Страда, формат: тренінг) були підняті такі важливі питання, як захист прав дітей онлайн і правила поведінки молоді онлайн. Вирішення проблем, з якими стикаються молоді

люди в Інтернеті в сучасному світі, є вкрай важливими як для поточної безпеки молоді, так і для розуміння кроків для подальшого покращення ситуації. Однак, і на поточному етапі вже можна говорити про вдосконалення, адже спеціальні гарячі лінії вже не тільки створюються, а й отримують активну підтримку з боку різних стейкхолдерів. Саме розуміння і сприйняття молоддю своїх прав і обов'язків в Інтернеті вийшли на новий рівень, що є характерною рисою розвитку онлайн безпеки сучасного світу.

Секція «Збери собі робота» (модератор: Валентин Протопопов, формат: майстер-клас) мала практичний характер, адже молоді було запропоновано не просто подивитись, як виглядають роботи, а стати частиною цього процесу і відкрити питання Інтернету речей з нового боку. Молодь активно залучалась до процесу збору машин, що самостійно їздять по заданій траєкторії, а також збору та керуванням дрону, що був повністю самостійно зібраний представниками Державного навчального закладу «Київський професійний коледж з посиленою військовою та фізичною підготовкою». В результаті цієї секції учасники отримали як теоретичне, так і практичне розуміння своєї участі в глобальних системах управління Інтернетом.

На секції «Блокчейн» (модератор: Анастасія Андрійчук, формат: імітація) молоді була представлена коротка інформація про технологію блокчейн, а також його зв'язку з криптовалютою. Біткоїн – питання, що є достатньо спірним в сучасному світі. Водночас, це питання, яке набуло надзвичайної популярності , в тому числі серед молоді. На секції були підняті питання, наскільки блокчейн і біткоїн змінюють життя, перетворюючись на потенціальні сфери. Учасникам також було запропоновано відчути себе «крипто-трейдером» та самостійно відчути процес «здобуття» критовалюти. Учасники повинні були знайти слова в картках, які були надані всім, а знайдені слова обміняти на смачні подарунки.

Впродовж секції «Цифрова безпека для молоді» (модератор: Ірина Чулівська, Лабораторія Цифрової Безпеки, формат: майстер-клас) розглядались такі питання, як захистити свої акаунти соцмереж, ме-

сенджери від того, що хтось отримає доступ до переписки і особистих даних. Учасники отримали розуміння, як працюють соцмережі і месенджери, на яких етапах можуть бути проблеми з приватністю і безпекою, і що вони можуть зробити, щоб краще захистити свої комунікації.

Темою останньої секцію стала «Мережевий нейтралітет», а її модераторами стали Фарид Нахлі (координатор програм регіонального відділення МСЕ), Юрій Каргополов (ІнАУ). Під час дискусії були розглянуті проблеми, які становлять, на думку учасників, «філософську основу» процесів, пов'язаних з управлінням Інтернетом. Оскільки поняття «Мережевий нейтралітет» впливає на фундаментальну основу побудови фінансово-економічних відносин між учасниками ринку, які представляють і зацікавлені у досягненні різних цілей. Ставлення до «нейтральної мережі» створює передумови для формування системи координат сприйняття процесів управління Інтернетом. «Мережевий нейтралітет» – це не лише протистояння між тими, хто генерує вміст, власником прав інтелектуальної власності та тими, хто постачає цей цифровий вміст користувачам. Це дуже складна сукупність організаційних, адміністративних, технічних і технологічних моделей та умов їх реалізації, яка включає всіх стейкхолдерів, що беруть участь у процесі управління Інтернетом. Модератори продемонстрували складність взаємозв'язку, що виникає при вирішенні проблеми «мережевого нейтралітету» на прикладах різних країн та глобальної взаємодії структурних елементів Інтернету. В ході дискусії зазначено, що кожна країна в рамках системи управління Інтернетом може сама визначити принципи та підходи, які мають значення для поточної ситуації на ринку. Це пов'язано з різним рівнем розвитку та кон'юнктурою ринку різних країн. Але принципи, на яких приймаються рішення про «мережевий нейтралітет», є загальними та універсальними. Огляди після обговорення показують цікавий та глибокий пізнавальний характер для учасників.

Також відмінністю, а згодом і традицією стало представлення меседжів, що були розроблені під час Youth IGF-UA, на заключному засіданні IGF-UA.

Для підготовки та проведення наступного Youth IGF-UA 2019 було створено ініціативну групу у складі Андрійчук Анастасії, Дубицької Валерії, Куковської Єлизавети, Марчука Валерія, Похабової Ірини, Правосуда Іллі. Участь в ній була добровільна, обмеження були виключно за віком (особи віком до 13 та від 35 років брали участь в роботі Youth IGF-UA лише в якості спостерігачів). Для участі в цій групі було достатньо надіслати листа з конкретними пропозиціями.

Другий Молодіжний Український Форум з управління Інтернетом відбувся 26 вересня 2019 року в приміщенні вченої ради Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» [4].

В ньому взяли участь 68 осіб:

- 12 школярів (віком до 16 років)
- 33 студентів (віком від 17 до 24 років),
- 13 інших осіб (віком від 25 до 35 років, в тому числі викладачів, а також представників міжнародних організацій)
- 10 інших осіб (віком від 36 років, в тому числі викладачів і представників міжнародних організацій).

Питання, що розглядались під час Youth IGF-UA, були дуже різноманітними - від питань про права і свободи молоді в Інтернеті до сфери технологій блокчейну. Але особлива увага цього Форуму була зосереджена на одному з фундаментальних принципів NRI's - інклюзивність. До вивчення питання підійшли особливо ретельно і різнобічно. Так, була особливо глибоко розглянута тема технічного забезпечення сайтів для людей з вадами зору. Представниками молоді були запропоновані технічні характеристики для сайту, які мають бути враховані при розробці. Крім того, був представлений макет такого сайту, який потенційно буде використовуватись для сайту Українського молодіжного Форуму з управління Інтернетом.

Молоддю піднімались важливі питання, що стоять перед всім світом сьогодні – як впливають Інтернет та соціальні мережі зокрема на особистість, чи не перебуваємо ми в ув'язненні Інтернетом, більше негативу чи позитиву привносить Інтернет в життя підростаючого

покоління. Дуже різнобічно ці теми розкрили Марія Іващенко, Оксана Самчинська та Дмитро Фарадж.

Крім того, учасники особливо ретельно підійшли до питань прав і свобод молоді в Інтернеті. Так, були висвітлені питання законодавчого захисту дітей працівників Інтернет-професій (Ярина Мамчур), питання розширення ролі Інтернету як засобу маніпулювання суспільством (Микола Мнишенко).

Цього року особлива увага приділялась питанням доступу до Інтернету. Питання було розглянуто з різних аспектів – як з точки зору фізичної наявності Інтернету у віддалених від центру районах, зокрема в селах (Яким Єрмак), так і з точки зору наявності доступу в Інтернет людям з особливими потребами (Кароліна Харкевич).

Другу половину заходу відкрила Ірина Похабова, яка зосередила свою увагу на ролі академічної спільноти і університетів в сфері Інтернету для розвитку. Надзвичайно популярну нині тему Інтернету речей та її технічну сторону розкрила в своїй презентації Єлизавета Куковська.

Ваган Говсепян, член RIPE NCC, познайомив молодь із тими можливостями залучення до процесу управління Інтернетом, які постають перед юнацтвом сьогодні.

Окремий блок був повністю присвячений системі G Suite for Education, який розкривався безпосередніми користувачами системою – школярами з Білої Церкви під керівництвом Антоніни Букач, Google for Education Certified Trainer. Крім того, саме юними учасниками був представлений сайт для Youth IGF-UA (зокрема участь брали такі учасники: Марчук Валерій, Ямпольська Даніела, Кобулей Анна, Кириченко Діана).

Крім того, кожному з учасників пропонувалось подати свої ідеї і пропозиції щодо тих тем, що висвітлювались під час події. Прозвучало багато практичних пропозицій. Але головною ідеєю виступила думка про те, що майбутнє зосереджено в руках молоді, адже саме молодь є рушієм всього.

Результати II Youth IGF-UA 2019 року були представлені у Берліні на глобальному IGF Валерією Дубицькою, модератором II Youth IGF-UA.

Підготовку до організації та проведення Третього Молодіжного Українського Форуму з управління Інтернетом (III Youth IGF-UA) було розпочато 12 серпня 2020 року, на підставі рішення ОргКомітету Українського Форуму з управління Інтернетом, членом якого є Валерія Дубицька, модератор Youth IGF-UA, делегат Youth IGF Summit 2019 року в Берліні, спікер vIGF Youth Summit 2020 року.

Роботу з організації та проведення III Youth IGF-UA продовжила ініціативна група у складі Валерії Дубицької, Єлизавети Куковської, Анастасії Ткачук, Іллі Правосуда, які працювали над організацією та проведенням попереднього, II Youth IGF-UA. Цього року до складу ініціативної групи долучився Валентин Протопопов, керівник Навчально-практичного Центру відновлювальної енергетики ДНЗ «Київський професійний коледж з посиленою військовою та фізичною підготовкою». Також інформаційну та організаційну підтримку заходу надала Мала Академія Наук України (МАН).

Інформація про умови участі у заході та заклик надсилати теми до обговорення розповсюджувалась через вебсайт https://youth-igf-ua.org, сторінку Facebook https://www.facebook.com/YouthIGFUA, через інформаційні канали МАН, Інституту телекомунікацій України, Київського Національного торговельно-економічного університету та інші канали інформації. Умови участі в Youth IGF-UA відповідали основоположним принципам Всесвітньої Молодіжної коаліції з управління Інтернетом (прописаним в Статуті та Кодексу етики).

Третій Молодіжний Український Форум з управління Інтернетом відбувся 28 жовтня 2020 року. Через ситуацію, що склалась через пандемію коронавірусу в світі, Форум відбувся онлайн на платформі Адамант [10].

Загалом на адресу info@youth-igf-ua.org надійшло 12 пропозицій тем до обговорення та 5 пропозицій доповідей або організації тематичних секцій.

У відповідності до рішення ОргКомітету IGF-UA усім учасникам Youth IGF-UA було надано можливість надіслати доповіді (спікерам) або тези доповідей (учасникам) для друку збірки доповідей III Youth IGF-UA (у відповідності до стандартів МАН).

Під час Форуму було обговорено багато питань, на основі яких сформовано такі повідомлення:

1. На жаль, не всі усвідомлюють, яким чином могли бути порушені особисті права під час пандемії, та які наслідки це може мати. Також були розглянуті кейси порушення прав онлайн в Україні та юридичний бекграунд, який за цим стоїть.

2. Tracking untracked - все частіше ми опиняємось в середовищі нових гаджетів і пристроїв, що вимагають ділитись особистими даними. Ми маємо обачливо до цього ставитись і пам'ятати про можливі наслідки використання особистих даних.

3. Популярність криптовалюти набирає обертів. Разом із цим ми стикаємось все з більшою кількістю загроз і шахраїв, які намагаються «відмивати» електронні гроші. При цьому Україна вже почала шлях щодо запобіганню цього.

4. Кібербезпека серед української молоді не втрачає актуальності. Дослідження, що проводяться серед молоді, показують, що мають бути проведені заходи для підняття рівня цифрової грамотності молоді.

5. Відновлювальна енергетика – це не альтернатива, а головний напрям подальшого розвитку всієї енергетики. Енергоефективність має безпосередній вплив на смарт технології і ми маємо брати це до уваги.

6. Старше покоління повинно мати такий самий доступ до Інтернету та можливості, які він надає, як молоді люди. Це молодь повинна допомагати та сприяти цьому.

Варто підсумувати, що як світовій спільноті, так і Україні зокрема ще варто зробити певні кроки до повноцінного і різнобічного залучення

молоді до питань управління Інтернетом. Голос, думка і досвід молоді варто не просто брати до уваги, але і сприймати на аналогічному рівні, як і всіх інших стейкхолдерів. При цьому, важливо відмітити, що вже існують кращі практики, які варто брати до уваги при розбудові молодіжної спільноти в Україні. Саме завдяки спільним зусиллям цей процес буде органічно імплементований в загальний розвиток сфери управління Інтернетом.

Список використаних джерел:

1. Frequently Asked Questions about the NRIs [Електронний ресурс] – Режим доступу до ресурсу: https://www.intgovforum.org/multilingual/content/frequently-asked-questions-about-the-nris
2. How to get involved, EuroDIG [Електронний ресурс] – Режим доступу до ресурсу: https://eurodigwiki.org/wiki/How_to_get_involved
3. Report of the Working Group on Internet Governance, Château de Bossey, June 2005 [Електронний ресурс] – Режим доступу до ресурсу: https://www.wgig.org/docs/WGIGREPORT.pdf
4. X Ukrainian Internet Governance Forum IGF-UA and II Youth Ukrainian Internet Governance Forum Youth IGF-UA Kyiv, September 23 and September 26, 2019 Annual report [Електронний ресурс] – Режим доступу до ресурсу: https://youth-igf-ua.org/about/
5. Youth Coalition on Internet Governance [Електронний ресурс] – Режим доступу до ресурсу: https://ycigweb.wordpress.com/
6. YOUTH ENGAGEMENT AT THE IGF, LOOKING AT EXISTING EXAMPLES OF PRACTICES, [Електронний ресурс] // IGF Secretariat in collaboration with the NRI communities – Режим доступу до ресурсу: https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4874/800
7. Youth IGF-UA Pro Kyiv, 5 October 2017 [Електронний ресурс] – Режим доступу до ресурсу: https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/3568/807
8. Youth IGF-UA, Report, 27 September 2018 Kyiv [Електронний ресурс] – Режим доступу до ресурсу: http://igf-ua.org/wp-content/uploads/2019/07/Youth-IGF-UA-eng.pdf
9. Youth Initiatives, THE IGF [Електронний ресурс] – Режим доступу до ресурсу: https://www.intgovforum.org/multilingual/content/youth-initiatives
10. III Youth Ukrainian Internet Governance Forum Youth IGF-UA Kyiv, 28 October 2020 Annual report [Електронний ресурс] – Режим доступу до ресурсу: https://youth-igf-ua.org/media/2020/Ukrainian-Youth_IGF-UA_2020_Annual_Report_ENG.pdf
11. Руководство в помощь национальным, субрегиональным, региональным и молодежным инициативам (NRIs) [Електронний ресурс] – Режим доступу до ресурсу: http://eump.org/nris-toolkit-in-russian

The role of youth in Internet governance – the experience of Ukraine

Dubytska Valeriia
iNGO European Media Platform, Kyiv
vsd2007@gmail.com

In recent years, there has been an increase in the number of young people (students and young professionals) in the global Internet governance ecosystem. In addition, young people make up a significant percentage of Internet users worldwide. One cannot but agree that young people play a vital role in shaping our digital future. That is why youth should be included in the definition of processes, principles and policies of Internet governance.

It is worth noting that the world community, and Ukraine in particular, needs to do more to involve young people in Internet governance. In addition to the awareness of the problems, it is worth answering the question, how exactly can young people influence decisions in their communities? Young people need to receive support and encouragement from all stakeholders. All stakeholder groups in the field of Internet governance should be able to integrate young people into the global sustainability agenda through digital technologies.

It should be noted that the Internet Governance Forum (IGF), established at the World Summit on the Information Society in Tunisia in 2005 in response to calls for an international platform to discuss Internet governance, plays a significant role in engaging young people [3]. The annual Internet Governance Forum (IGF) is open to everyone: governments, civil society, international organizations, educators and

academics, private sector organizations, youth and others. The purpose of the IGF is to examine issues related to the Internet from a variety of perspectives: they range from technical aspects to human rights issues. All participants are free to speak and share their experiences. Unlike many other forums, the IGF has no legislative or executive powers.

Although the impact of the Internet on young people has long been discussed at the annual meetings of the Internet Governance Forum (IGF), which also involves young people, youth has only recently in the history of the IGF participated in real work processes. The IGF community increasingly recognizes the importance of involving young people in their work processes, from understanding key issues to planning events and participating actively. Moreover, various approaches have been used to include the views and voices of young people in the discussion of Internet policy at the annual IGF meetings and during the preparatory process [6].

The most visible and ongoing involvement of young people is traced at the national, subregional and regional levels, where IGF youth initiatives focus on bringing young people together to discuss Internet governance and policy. In addition to these practices, the IGF community has made many efforts to support young people to participate in annual IGF meetings, as well as to create a variety of programs at national, regional or international levels to prepare, educate and inform young people about Internet governance and key topics [9].

IGF Youth Initiatives are designed to encourage and engage young people in a substantive discussion on Internet governance. These forms, as well as national, subregional and regional IGFs (NRIs) [1], are expected to be in line with IGF's core principles of being open, inclusive, non-profit, multi-stakeholder during the preparatory phase and the event itself, in line with bottom-up decision-making.

In addition to the annual IGF meetings, one of the most notable youth initiatives is the Youth Coalition on Internet Governance (YCIG) [5]. The Youth Coalition for Internet Governance (YCIG) is an open group for organizations and individuals representing all stakeholder groups willing to work together to encourage and enrich youth participation in

local, regional and international discussions and Internet governance processes [2].

YCIG was created to protect the rights of children, youth and young professionals during Internet governance forums and processes. YCIG is open to all young people and other stakeholders interested in Internet governance. As a registered dynamic coalition of the IGF, YCIG has a meeting place in each forum and brings together young people from across the IGF to identify and discuss relevant issues, as well as to bring together networks to empower young people in Internet governance.

It is worth emphasizing that youth engagement is a frequent topic of discussion during the IGF, but to date, not enough young voices have been taken into consideration. Young people do not find a permanent place at the table to discuss all issues of Internet governance freely and equally.

A similar situation can be applied to Ukrainian reality. In order to unite young people, create a community and promote the voices of young people the Youth IGF-UA was launched in Ukraine. It was done to discuss the future of the Internet on issues such as openness, diversity, accessibility, security and privacy, and last but not least, human rights.

Although the process of establishing sustainable processes for involving young people in governance is still ongoing, it is important to note that some steps have already been taken.

INGO European Media Platform (in partnership with America House Kyiv, Internet Governance Forum Support Association, Government Office for European and Euro-Atlantic Integration, Institute of education content modernization) organized Youth IGF-UA Pro (5 October 2017, America House Kyiv) as a pre-event of VIII IGF-UA (6 October 2017, Nivki-hall) [7].

Experts and youth discussed the establishment of a new platform for young people engagement in Internet Governance. During the discussion it was mentioned the role of different stakeholders in the process of ensuring cybersecurity, expanding public access to high speed Internet, development of e-commerce, opportunities for young

people, Ukrainian legislation on telecommunications to be align with EU law.

Valeriia Dubytska and other trainees of iNGO European Media Platform (EMP) presented their Russian translation of NRIs Toolkit and basic principles of IGF [11]:

- Open and Transparent;
- Inclusive;
- Bottom-Up;
- Non-commercial;
- Multistakeholder.

For that to happen at Youth IGF-UA (February 2018) Valerie Dubitskaya (EMP) initiated creation of Youth IGF-UA Multistakeholder Organizing Team. This initiative was supported by Glib Strygunenko (Government Office for European and Euro-Atlantic Integration) and Yegor Aushev (CyberGuard/ private sector), as well as other participants of Youth IGF-UA Pro. Messages about this initiative were delivered to VIII IGF-UA (October 6, igf-ua.org), IGF Secretariat, EuroDIG, SEEDIG. With this messages Youth IGF-UA Multistakeholder Organizing Team addresses IGF Secretariat, VIII IGF-UA, EuroDIG and SEEDIG community to be recognized as Youth IGF-UA in formation. Focal point of Youth IGF-UA in formation is Valerie Dubitskaya, iNGO European Media Platform (valerie@eump.org).

46 on-site and 7 remote participants represent different age groups, but 69,6% represent the age groups 15-25 and 25-35 years old.

Regarding stakeholder representation it is necessary to mention that participants of Youth IGF-UA Pro lack understanding of the concept of multistakeholderism. For example, students of private colleges identify themselves as private sector, and students of governmental institutions – as government.

On May 22, 2018, a parliamentary conference «Ukrainian Youth and Internet Governance in the Context of European Integration» was

organized with the support of the Chairman of the Verkhovna Rada Committee Maria Ionova and the Member of the European Parliament Michal Boni. More than 85 participants took part in the event to discuss the role of Ukrainian youth in Internet governance.

The next step in youth involvement and community development was the First Youth IGF-UA. Youth IGF-UA took place on September 27, 2018 in Kyiv at the UBI Hall business center and became the first event within the Internet Days in Ukraine [8]. During Youth IGF-UA 2018, more than 100 young people and representatives of various stakeholder groups attended the event.

According to the decision of the IGF-UA Organizing Committee, the Internet Association of Ukraine, the Commission on Science and Information Technologies of the Ukrainian League of Industrialists and Entrepreneurs, RIPE NCC, ISOC, IGFSA, Internews-Ukraine, ICANN were co-organized the events. The events were supported by the Committee on Informatization and Public Relations of the Verkhovna Rada of Ukraine, the Office of the Cybercrime Program (Council of Europe), and the iNGO EMP.

The IGF-UA Youth Working Group (WG) was created within the IGF-UA Organizing Committee to coordinate financial, logistical and any other objectives. As Youth IGF-UA did not have any statutory documents at that time, it was decided that year to follow the Principles of the Ukrainian Internet Governance Forum IGF-UA (Protocol of Intent).

An unusual but successful experience was holding the Forum in various formats. Thus 6 different sections were held, each of which had its own format and results.

During the section Model of cyberthreats for Ukrainian Youth (Moderators: Oleksii Baranovsky, Igor Sikorsky Kyiv Polytechnic Institute, Andrii Pertsiukh, IT lab, format – World café) the audience was divided into two teams to determine the models of cyber risks that youth is now facing. As a result of fruitful work, both teams concluded that the main risks that young people encounter on the Internet are:

- Viruses
- Hacking
- Fraud
- Phishing
- Spam
- Sexting

Andriy Mankish, CERT-UA, and Uwe Rasmussen, (Council of Europe) summarized the results of the discussion, noting that it is very important that the issues themselves go beyond individual perceptions when young people find themselves being alone in face of online risks. The transition from an individual to a group discussion is an important moment, which is the starting point for creating a new approach to the development of cyber-risk models.

During section Social networks. Child Safety Online (Moderators: Tetyana Kharkivska, La Strada, format – training) important issues were raised, such as the protection of the rights of children online and the rules of conduct of young people online. Addressing the challenges faced by young people online in the modern world is crucial both for youth's security today, and for understanding the steps to improve the situation further. However, at the current stage we can already talk about improvement, because special hotlines are not only created, but also receive active support from different stakeholders. The understanding and perception of the youth of their rights and responsibilities on the Internet reached a new level, which is characteristic of the development of the modern world online security.

The section Make yourself a robot (Valentin Protopopov, Kyiv Professional College with Enhanced Military and Physical Training, format – workshop) was practical in nature, because young people were asked not just to look at what the work looks like but to become part of this process and to take the new perspective on the Internet of Things. Young people were actively involved in the process of assembling cars that travel independently on a given trajectory, as well as assembling and managing a quadcopter that was made by the students of the

State Educational Institution «Kyiv Professional College with Enhanced Military and Physical Training». As a result of this section, participants received both theoretical and practical understanding of their role in global Internet governance systems.

In the section Blockchain (Moderator: Anastasia Andriychuk, iNGO European Media Platform, format – simulation) youth was presented with a brief information on the technology of blockchain, as well as its connection to cryptography. Bitcoin is an issue that is quite controversial in the modern world. At the same time, this is an issue that has gained enormous popularity, and it is popular among young people too. Questions like «how much Blockchain and Bitcoin influence life, potentially turning into a new sphere» were raised on the section. Participants were also offered a chance to feel like a cryptotrader and feel the process of cryptocurrency mining on their own. The participants were given cards and had to find the words in the cards. The words found were to be exchanged for delicious gifts.

During the section Digital Security for Youth (Moderator: Iryna Chulivska, Digital Security Lab Ukraine, format – workshop) issues such as protecting social network accounts and messengers from unauthorized access the personal data. Participants got an understanding of how social networks and messengers operate, at which stages there may be privacy and security issues and what they can do to better protect their communications.

The topic of the last section was Net Neutrality, and its moderators were Farid Nakhli (program coordinator of the ITU regional branch), Yuri Kargopolov (InAU). During the discussion the problems which constitute by the participants' opinion the «philosophical basis» of the processes concern with the Internet Governance were considered. Because the concept of «Net Neutrality» affects the fundamental basis of building financial and economic relations between market participants, who represent and are interested in achieving different goals. The attitude to «Net Neutrality» creates the prerequisites for the formation of the coordinate system of perception of the processes of the Internet Governance. The «Net Neutrality» is not only a confrontation between

those who generate content, the owner of intellectual property rights to the content and those who supply this digital content to users. This is a very complex set of organizational, administrative, technical and technological models and conditions of their realization, which includes all stakeholders involved in the process of the Internet Governance. The moderators demonstrated the complexity of the relationship that arises in solving the problem of the «Net Neutrality» on the examples of different countries and the global interaction of the structural elements of the Internet. During the discussion noted that each country in the framework of the Internet Governance system could itself defines the principles and approaches that are relevant for current market situation. This is due to the various levels of development and the market's conditions of different countries. But the principles on which decisions on the «Net Neutrality» are made are common and universal. The post-reviews of the discussion show the interesting and profound cognitive character for the Participants.

Another difference, and later a tradition, was the presentation of messages developed during Youth IGF-UA at the final meeting of IGF-UA.

An initiative group consisting of Anastasia Andriychuk, Valeria Dubytska, Elizaveta Kukovska, Valeriy Marchuk, Iryna Pokhabova, and Ilya Pravosud was created to prepare and hold the next Youth IGF-UA 2019. Participation was voluntary, with age restrictions only (persons under 13 and above 35 y.o. participated in Youth IGF-UA only as observers). To participate in this group, it was enough to send a letter with specific proposals.

The Academic Boardroom of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" hosted the Second Youth Ukrainian Internet Governance Forum on the 26th of September 2019 [4].

There were 68 attendees, including 12 pupils (aged under 16), 33 university students (aged 17-24), 13 attendees from other groups (aged 25-35, including instructors, as well as the representatives of international organizations), 10 people (aged over 36, including instructors, as well as the representatives of international organizations).

Event was moderated by Valeriia Dubytska. Oleksii Novikov (Kyiv Polytechnic Institute, Provost), Oksana Prykhodko (iNGO European Media Platform, Director), Oleksii Semeniaka (RIPE NCC), Markus Kummer (IGF SA, video address), Antonina Bukach (Digital Development Academy), and Massimiliano Stucchi (ISOC) delivered their opening remarks.

The agenda of Youth IGF-UA was very broad, ranging from youth rights and freedoms on the internet to blockchain technology. However, inclusivity, one of the fundamental NRI principles, was the particular focus of this Forum. This issue was meticulously studied and viewed from different angles. For example, there was a very detailed conversation about the technical capabilities of the websites for visually impaired users. The youth suggested the website features that must be noted during the website development. In addition, a website mock-up was presented, that would provisionally be used for the Youth Ukrainian Internet Governance Forum website.

Young people raised important issues that the world is facing today. For instance, how the web and social media impact personality, whether or not we are 'jailed' in the internet, whether the internet results in more pros or cons in the life of the younger generation. These topics were extensively covered by Mariia Ivashchenko, Oksana Samchynska and Dmytro Faradzh.

On top of that, the delegates looked at the youth rights and freedoms in the internet agenda with the utmost care. Yaryna Mamchur spoke about the legal protection for the children of internet-related professionals, while Mykola Mnyshenko highlighted the extensive use of the internet as a means for the manipulation of the general public.

Internet access was this years` special focus. A variety of perspectives was introduced, such as the actual connectivity of remote areas, including the rural communities (Yakym Yermak), and internet access for people with special needs (Karolina Kharkevych).

Iryna Pokhabova opened the second half of the event, addressing the role of the academia and universities in promoting internet for development. Yelyzaveta Kukovska did a presentation on a topic that

is incredibly popular these days – the internet of things, including the technical side.

Vahan Hovsepyan of RIPE NCC outlined the opportunities to become engaged in the internet governance process, available to young people today.

A separate section was entirely dedicated to G Suite for Education system under the direction of Antonina Bukach, Google for Education Certified Trainer. Presentations were made by the actual system users who were pupils from the city of Bila Tserkva. Apart from that, it was the young attendees who presented the website for Youth IGF-UA (with the participation of Valerii Marchuk, Daniela Yampolska, Anna Kobulei, Diana Kyrychenko).

Also, all attendees were invited to share their ideas and suggestions on the issues present in the event agenda. Many practical suggestions were put forward. However, the key idea was that the future lies in the hands of the young, since young people are the driving force of everything.

The results of II Youth IGF-UA 2019 were presented in Berlin at the global IGF by Valeriia Dubytska, moderator of II Youth IGF-UA.

Initiations of the Third Ukrainian Youth Internet Forum (III Youth IGF-UA) began on August 12, 2020, based on the decision of the Organizing Committee of the Ukrainian Internet Forum, IGF-UA). Valeriia Dubytska, Youth IGF-UA moderator, Youth delegate of IGF Summit 2019 in Berlin, speaker of the vIGF Youth Summit 2020, is member of the Organizing Committee of the Ukrainian Internet Forum.

The work on the organization and holding of the III Youth IGF-UA was continued by the initiative group consisting of Valeriia Dubytska, Elizaveta Kukovska, Anastasia Tkachuk, Ilya Pravosud, who worked on the organization and holding of the previous, II Youth IGF-UA. This year, Valentyn Protopopov, head of the Educational and Practical Center for Renewable Energy of the Kyiv Vocational College with Enhanced Military and Physical Training, joined the initiative group. The information and

organizational support of the event was also provided by the Small Academy of Sciences of Ukraine (SAS).

Information about the terms of references in the event and the call to send topics for discussion was disseminated through the website https://youth-igf-ua.org, Facebook page https://www.facebook.com/YouthIGFUA, through information channels of the Academy of Sciences, the Institute of Telecommunications of Ukraine, Kyiv National University of Trade and Economics and other information channels. The terms of references in the Youth IGF-UA were complied with the fundamental principles of the World Youth Coalition for Internet Governance (prescribed in the Statute and the Code of Ethics).

The III Youth IGF-UA took place on October 28, 2020. Due to the situation due to the coronavirus pandemic in the world, the Forum was held online on the Adamant platform [10].

Initiative group received 12 proposals for topics for discussion and 5 proposals for reports.

In accordance with the decision of the IGF-UA Organizing Committee, all Youth IGF-UA participants were given the opportunity to send reports (speakers) or abstracts (participants) for printing a collection of III Youth IGF-UA reports (in accordance with SAS standards).

Many issues were discussed during the Forum, on the basis of which the following messages were formed:

1. Unfortunately, not everyone is aware of how personal rights online could be violated during a pandemic, and what the consequences could be. In addition, cases of online rights violations in Ukraine and the legal background were considered.
2. Tracking untracked - more and more often we all, especially young people, find ourselves in the midst of new gadgets and devices that require the sharing of personal data. We must be careful about this and keep in mind the possible consequences of sharing personal data.

3. The popularity of cryptocurrency is gaining momentum. At the same time, we are facing more and more threats, including fraudsters trying to «launder» cyber money. It was noted that Ukraine has already begun the path in the regulatory field to prevent this.
4. Cybersecurity among Ukrainian youth is still a relevant and popular topic. Research among young people shows that measures should be taken to raise the level of digital literacy of young people with the participation of all stakeholders.
5. Renewable energy is not an alternative, but the main direction of further development of all energy. Energy efficiency has a direct impact on smart technology, and we need to take this into account.
6. The older generation should have the same access to the Internet and opportunities that it provides as young people. It is the youth who must help and promote this.

To conclude with it is worth mentioning that both the world community and Ukraine still need to take certain steps towards full and comprehensive involvement of young people in Internet governance. The voice, opinion and experience of young people should not just be considered, but also perceived at the same level as all other stakeholders. At the same time, it is important to note that there are already best practices that should be taken into account when building a youth community in Ukraine. Only through joint efforts this process will be organically implemented in the overall development of Internet governance.

ПРАВО НА ПРИВАТНІСТЬ ТА ЦИФРОВІ ІНСТРУМЕНТИ ПРОТИДІЇ COVID-19

Віта Володовська
ГО «Лабораторія цифрової безпеки», Київ
v.volodovska@gmail.com

Право на повагу до приватного життя є одним із фундаментальних прав людини, що гарантується статтею 8 Конвенції про захист прав людини та основоположних свобод [1] та статтею 17 Міжнародного пакту про громадянські та політичні права [2]. І хоча це право не є абсолютним, будь-яке втручання в його реалізацію має бути передбачене якісним та доступним законом, слугувати легітимній цілі (захист національної безпеки, громадського порядку та ін.), а також бути необхідним у демократичному суспільстві (відповідати нагальній суспільній потребі, бути пропорційним та обґрунтованим).

Коронавірусна пандемія, що охопила світ на початку 2020 року, спонукала уряди шукати ефективні способи забезпечити дотримання карантинних засобів, зокрема, із застосуванням інформаційних технологій стеження за громадянами. Такі заходи безумовно є втручанням у право на приватність, хоча і можуть бути виправданими легітимною метою захисту громадського здоров'я. На жаль, перед лицем серйозної загрози навіть демократичні держави не приділили достатньої уваги забезпеченню двох інших важливих умов обмежень прав людини – законності та пропорційності.

У квітні 2020 понад сотня міжнародних громадських та правозахисних організацій виступили із заявою [3], в якій закликали уряди держав використовувати технології цифрового стеження для боротьби

з пандемією з повагою до прав людини. Одним із ключових занепокоєнь, висловлених в заяві, є загроза розгортання масштабних заходів стеження за громадянами, які не будуть припинені навіть після завершення кризи, зважаючи на ресурси, вкладені в їх впровадження та можливості для контролю суспільства.

Правозахисники зазначили, що технології можуть та мають відігравати важливу роль спробах врятувати життя, зокрема через поширення повідомлень у сфері громадського здоров'я та підвищення доступу до медичної допомоги. Водночас, збільшення повноважень держави щодо здійснення цифрового стеження без згоди громадян, зокрема отримання доступу до даних про місцезнаходження мобільних телефонів, загрожує приватності, свободі вираження поглядів та свободі об'єднань таким чином, що може призвести до порушення прав людини та знизити довіру до органів влади, що підважить ефективність будь-яких заходів з забезпечення громадського здоров'я.

Рішення, які приймають уряди для протидії пандемії сьогодні, сформують те, як наш світ виглядатиме у майбутньому. Саме тому у своїй заяві правозахисники відзначили низку важливих принципів, яким мають відповідати заходи для протидії пандемії, а саме:

- заходи зі стеження, які були впроваджені для протидії пандемії, мають бути законними, необхідними та пропорційними. Вони мають бути передбачені законом та відповідати легітимним цілям охорони здоров'я, визначеним належними органами влади у сфері громадського здоров'я, та бути пропорційними таким потребам. Уряди мають бути відкритими щодо заходів, які вони вживають, для того, щоб їх можна було ретельно дослідити та, за потреби, у майбутньому модифікувати, відкликати або переглянути;
- посилення повноважень щодо моніторингу та стеження має бути обмеженим у часі і продовжуватися лише доки це буде необхідно для протидії пандемії;
- дані, зібрані, утримані чи агреговані з метою протидії COVID-19, мають бути обмеженими за обсягом та часом використання,

залежно від розвитку пандемії, та не повинні використовуватись для комерційної чи будь-якої іншої цілі;

- уряди мають забезпечити належний рівень безпеки будь-яких персональних даних та будь-яких технічних засобів, застосунків, мереж або сервісів, що збирають, передають, обробляють та зберігають дані. Будь-які заяви про те, що дані є анонімними, мають базуватися на доказах та підтверджуватися достатньою інформацією щодо того, як відбувалася така анонімізація;
- будь-яке використання технологій цифрового стеження для відповіді на COVID-19, включно з використанням «big data» та систем штучного інтелекту, має враховувати ризики, пов'язані з можливим впливом таких інструментів на посилення дискримінації та порушення прав расових меншин, людей, що живуть у бідності та іншого вразливого населення, чиї потреби та реалії життя можуть бути неврахованими чи некоректно представленими у великих наборах даних;
- якщо уряди укладають угоди, які передбачають передачу даних іншим установам публічного чи приватного сектору, такі договори мають базуватися на законі, а факт їх укладення та інформація, необхідна для оцінки їх впливу на приватність та права людини, мають бути оприлюднені – у письмовому вигляді, з визначеними положеннями про закінчення дії таких угод, публічним наглядом та іншими запобіжниками за замовчуванням.

Правозахисники також відзначили, що будь-який захід, спрямований на протидію пандемії, має включати елементи підзвітності та запобіжники проти зловживань. «Посилені повноваження щодо стеження, пов'язаного з COVID-19, не мають бути надані службам безпеки або розвідки та мають підлягати ефективному нагляду зі сторони відповідних незалежних органів. Понад те, особам має бути надана можливість знати про та оскаржувати будь-які заходи зі збору, агрегації, утримання та використання даних, пов'язаних з COVID-19. Особи, щодо яких було встановлено стеження, повинні мати доступ до ефективних засобів правового захисту», - йдеться у заяві.

Для повноцінного аналізу дотримання висловлених принципів при впровадженні заходів стеження, потрібен час, адже особливо показовим з точки зору прав людини буде саме згортання заходів втручання в приватність по мірі того, як пандемія відступатиме. Водночас, уже сьогодні можна відзначити надмірність державних ініціатив, яким бракує належних гарантій захисту від зловживань[4]. Так, білоруська громадська організація Human Constanta та російська Роскомсвобода навесні запустили проект Pandemic Big Brother [5], метою якого є моніторинг обмежень прав людини у цифровому середовищі, у зв'язку з пандемією. За даними моніторингу[6], друга хвиля епідемії дала поштовх впровадженню нових, ще більш серйозних обмежень права на приватність та посилення відповідальності громадян за порушення карантинних заходів.

В Україні заходи протидії коронавірусній епідемії також не оминули використання цифрових технологій та втручання в право громадян на приватність. Так, ухвалені парламентом зміни [7] до Закону України «Про захист населення від інфекційних хвороб» [8] для запобігання поширенню COVID-19, що набрали чинності у квітні 2020 року, на період карантину (виключно для здійснення протиепідемічних заходів) передбачили можливість обробки персональних даних без згоди особи. До переліку таких даних було включено: повне ім'я, стан здоров'я, місце госпіталізації або самоізоляції, дата народження, місце проживання, місце роботи (навчання). Передбачено також, що протягом 30 днів після закінчення карантину, такі дані підлягають знеособленню, а якщо це неможливо – знищенню.

Такі зміни дещо суперечать статті 7 Закону України «Про захист персональних даних», яка взагалі забороняє обробку інформації про стан здоров'я особи без її згоди, крім вичерпного переліку випадків, наведених у цій статті [9]. Запропоноване новим законом виключення можна розглядати як створення додаткової підстави для обробки такої чутливої інформації, але її формулювання не відповідає принципу визначеності, точності та не містить елементів захисту від зловживань, тоді як розголошення таких даних може мати серйозні наслідки для безпеки і прав особи.

Зокрема, закону бракує правової визначеності стосовно того, які саме державні органи отримують повноваження здійснювати обробку персональних даних без згоди особи та в якому обсязі інформація має їм передаватися. Закон України «Про захист населення від інфекційних хвороб», перелічує низку органів влади, які можуть здійснювати заходи щодо протидії епідемії: Кабінет Міністрів України, МОЗ та його установи, місцеві органи виконавчої влади та органи місцевого самоврядування. Уряд додав до цього кола також Національну поліцію та Національну гвардію. Таким чином, коло осіб, залучених до протиепідемічних заходів надзвичайно широке. Надання їм повноважень отримувати доступ до усієї переліченої вище інформації не є виправданим [10].

Яскравою ілюстрацією наслідків відсутності чітких вимог щодо захисту інформації про осіб, до яких застосовуються заходи обсервації або ізоляції, є оприлюднення Житомирською ОДА карти з позначенням вулиць, де мешкають хворі на Covid-19 (включно з інформацією про вік таких пацієнтів та статус лікування)[11]. Така інформація не лише жодним чином не сприяє захисту від пандемії, а може призвести до дискримінації та зростання соціальної напруги в громадах [10].

Для забезпечення дотримання карантинних заходів Міністерство цифрової трансформації також запустило спеціальний додаток – «Дій вдома», що має контролювати дотримання особою режиму самоізоляції. Контроль відбувається за допомогою регулярних повідомлень у застосунку в довільні проміжки часу протягом дня та перевірки відповідності фотографії обличчя особи еталонній фотографії, зробленій під час встановлення мобільного застосунку, та геолокації мобільного телефона в момент фотографування. У разі отримання повідомлення громадянину необхідно протягом 15 хвилин за допомогою застосунку зробити фото свого обличчя на фоні навколишнього середовища[12]. Встановлення додатку «Дій вдома» є добровільним. Водночас, для осіб, що повертались з-за кордону єдиною альтернативою була госпіталізація до закладів обсервації.

20 листопада Мінцифри оголосили про нові ініціативи цифрових сервісів для протидії коронавірусу. Міністерство разом з Кабміном

та МОЗ працює над цифровізацією та централізацією збору інформації щодо фактів і підозр про випадки інфекційних захворювань, а також планує оновити та вдосконалити мобільний застосунок для контролю самоізоляції "Вдома". Зокрема, впроваджуватиметься можливість передавати до Центру громадського здоров'я інформацію про симптоми, задля оперативного відстеження інформації про погіршення стану здоров'я та розвантаження сімейних лікарів. Міністерство також планує розробити та впровадити систему QR-кодів, що допомагатиме українцям зрозуміти, чи мали вони контакт з носієм коронавірусної інфекції у громадських місцях. Система QR-кодів потенційно працюватиме у громадських закладах, де епідеміологічно вищий ризик поширення COVID-19 [13].

Таким чином, нові цифрові інструменти протидії епідемії Covid-19 посилять обсяги збору та використання персональних даних громадян, у тому числі, чутливих даних про стан здоров'я. Зважаючи на це, важливо забезпечити належне дотримання стандартів прав людини при їх впровадженні. Зокрема, необхідно забезпечити прозорість обробки персональних даних в рамках взаємодії між МОЗ, Мінцифри та МВС та чітко регламентувати порядок доступу органів влади, залучених у протиепідемічні заходи, виключно до тих категорій персональних даних, які є мінімально необхідними для виконання їх повноважень, визначених законодавством.

Належне дотримання карантинних заходів населенням великою мірою залежить від довіри до органів влади та впевненості у власній захищеності від зловживань. Без дотримання принципів відкритості та прозорості у впровадженні технічних рішень протидії пандемії, зокрема, гарантій захищеності персональної інформації про особу, яка збирається в таких цілях, рівень виконання карантинних заходів може суттєво знижуватись, що, безумовно матиме, негативний ефект і для системи громадського здоров'я. Саме тому застосування цифрових технологій для подолання епідемії вимагає зважених державних рішень та широких консультацій з усіма зацікавленими сторонами, у тому числі із правозахисниками. Бо у війні з безпрецедентною загрозою національному здоров'ю важливо не перетворити демократію та верховенство права на супутні жертви.

Список використаних джерел:

1. Конвенція про захист прав людини і основоположних свобод, ратифікована Законом № 475/97-ВР від 17.07.97//База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
2. Міжнародний пакт про громадянські і політичні права, ратифікований Указом Президії Верховної Ради Української РСР N 2148-VIII (2148-08) від 19.10.73// База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text
3. Держави мають використовувати технології цифрового стеження для боротьби з пандемією з повагою до прав людини – спільна заява громадянського суспільства// Лабораторія цифрової безпеки. URL: https://dslua.org/publications/derzhavy-maiut-vykorystovuvaty-tekhnolohii-tsyfrovoho-stezhennia-dlia-borot-by-z-pandemiieiu-z-povahoiu-do-prav-liudyny-cpil-na-zaiava-hromadians-koho-suspil-stva/
4. Дворовий М. Коронавірус, трекінг інфікованих та приватність: як далеко можуть піти держава і техкомпанії та де тут права людини?//Лабораторія цифрової безпеки. URL: https://dslua.org/publications/koronavirus-trekinh-infikovanykh-ta-pryvatnist-iak-daleko-mozhut-pity-derzhava-i-tekhkompanii-ta-de-tut-prava-liudyny/
5. Pandemic Big Brother. URL: https://pandemicbigbrother.online/ru/
6. The second wave of restrictions and “coronavirus” apps. // Pandemic Big Brother Digest. URL: https://pandemicbigbrother.online/en/digest/15/
7. Закон України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)»// База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/555-20#Text
8. Закон України «Про захист населення від інфекційних хвороб»//База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1645-14#Text
9. Закон України «Про захист персональних даних»//База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
10. Володовська В. «Не час для згоди»: що не так із новим «антивірусним» законом//Лабораторія цифрової безпеки. URL: https://dslua.org/publications/ne-chas-dlia-zghody-shcho-ne-tak-iz-novym-antyvirusnym-zakonom/
11. Чумні квартали: Житомирська ОДА оприлюднила карту з позначками вулиць, де мешкають хворі на COVID-19//Детектор медіа/Media Sapiens. URL: https://ms.detector.media/zakonodavstvo/post/24517/2020-04-16-chumni-kvartali-zhitomirska-oda-oprilyudnila-kartu-z-poznachkami-vulits-de-meshkayut-khvori-na-covid-19/

12. Як працює застосунок «Дій вдома»// Урядовий портал. URL: https://www.kmu.gov.ua/news/yak-pracyuye-zastosunok-dij-vdoma

13. Мінцифра запроваджує нові цифрові рішення для протидії COVID-19 — Михайло Федоров// Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/news/mintsifra-zaprovadzhue-novi-tsifrovi-rishennya-dlya-protidii-covid-19-mikhaylo-fedorov?utm_source=newsletter&utm_medium=email&utm_campaign=mincifra_vprovadzhuye_cifrovi_instrumenti_dlya_protidiji_koronavirusu&utm_term=2020-11-30

КІБЕРБЕЗПЕКА З ТОЧКИ ЗОРУ УКРАЇНСЬКОЇ МОЛОДІ

Правосуд Ілля

Дана стаття містить результати дослідження, яке було проведене міжнародною громадською організацією "Європейська Медіа Платформа" за підтримки Counterpart International та Google for Education Certified Trainer.

Метою дослідження було виокремлення найбільш поширених кіберзагроз, на які наражаються українські підлітки. Важливим етапом було визначення наявності в молоді розуміння реальної небезпеки та інструментів протидії загрозам, з якими вони зустрічаються в Інтернеті.

Дослідження складалось з трьох етапів, в якому брали участь 1364 учні та 516 вчителів:

- опитування в трьох фокус-групах в 2017-2018 роках;
- опитування школярів-учасників онлайн курсу з кібербезпеки (січень 2019 року);
- опитування вчителів, які були учасниками вебінару, присвяченого Дню Безпечнішого Інтернету 5 лютого 2019 року.

Опитування показало наступні результати:

1. Більшість респондентів, а саме 68% учнів та 83% вчителів, мали досвід зустрічі з кіберзагрозами. Те, що відсоток вчителів більший, можна пояснити не лише їхнім більшим досвідом користування Інтернетом, але й насамперед тим, що досить часто учні навіть не усвідомлюють, що стали жертвою кіберзлочину.

2. Найпоширенішими кіберзагрозами, на які наражались учасники опитування, можна виділити віруси, піратство, спам, шахрайство, крадіжка паролів. До менш поширених належать фінансові крадіжки, злом акаунтів, DDoS атаки, жорстоке поводження з дитиною, булінг, фішинг, грумінг. У деяких випадках учасники опитування згадували, що їх комп'ютери використовували для майнінгу біткоінів і в якості частини ботнетів. Також були скарги на кібертероризм та порнографію.
3. 62%, тобто більша частина молоді, яка зазнала на собі шкоди в Інтернеті, по допомогу не звертались. Трохи більше половини вчителів (54%), які наразились на кібершахрайство, звернулись по допомогу.
4. Як показало дослідження, найчастіше підлітки звертаються по допомогу до друзів (25%), на другому місці стоять батьки (23%). Менше 10% звертались по допомогу до вчителів. Також були поодинокі випадки звернень на "гарячі" лінії та до правоохоронних структур.
5. Більше половини респондентів виявили бажання дізнатись більше інформації та засобів захисту щодо власної кібербезпеки. Серйозною проблемою виступає мала проінформованість, адже 60% опитуваних не знають, де і як їх шукати.
6. Соціальні мережі виступають першоджерелом інформації щодо питань кібербезпеки.
7. Близько половини опитуваних учнів продовжують користуватись російськими соціальними мережами.

Виходячи із вищезазначених результатів, можна сформулювати наступні висновки та рекомендації:

1. На сьогоднішній день у держави не існує власної "гарячої лінії" з питань кібербезпеки, зокрема окремої "дитячої" лінії. Можна виділити єдину Національну дитячу "гарячу" лінію, яка є лише в ГО "Ла Страда – Україна". Але слід зазначити, що вона працює лише чотири години на добу через нестачу коштів (з боку держави поки що немає жодної підтримки).

Аби покращити ситуацію з обізнаністю про Інтернет небезпеки, необхідно проінформувати підлітків про існування Національної дитячої "гарячої лінії" – 0 800 500 335 або 116 123 (короткий номер з мобільного). Але робити це потрібно використовуючи мультистейкхолдерний підхід. Тобто застосовуючи спільні зусилля Міністерства освіти і науки України, громадських організацій, правоохоронних органів, IT бізнесу, навчальних закладів, медіа, операторів і провайдерів та інших стейкхолдерних груп, які можуть мати на це вплив.

Також необхідно звернутись до міжнародних спонсорів та бізнесу за отриманням фінансування "гарячої лінії", а також щодо приєднання України до міжнародної мережі "гарячих ліній" InHope. З боку держави необхідно закласти в державний бюджет статтю витрат на фінансування кібербезпеки для молоді. Спільними зусиллями громадськості, держави та бізнесу треба розробити механізми взаємодії "гарячої лінії" з українськими правоохоронними органами.

Важливим кроком буде забезпечення підтримки з боку CERT-UA (за участі громадскості та приватного бізнесу) механізмів та стандартів захисту інформаційних ресурсів МОН та його підрозділів, а також навчальних та дитячих закладів.

2. І молоді, і фахівцям не вистачає інформації щодо видів кіберзагроз.

Так, не володіючи даними про те, як діють фішингові сайти, людина навіть не знаючи про це надає злочинцям інформацію про себе, своїх родичів та друзів. Цю інформацію злодії можуть використати для підробки документів, оформлення кредиту або крадіжки коштів.

Спільними зусиллями експертів, правоохоронних органів, громадськості, бізнесу та молоді необхідно розробити модель ризиків та алгоритм протидії кіберзагрозам для молоді.

Також треба проводити регулярні опитування молоді з врахуванням віку, освіти, засобів доступу до Інтернету та інших вагомих факторів, стосовно питань кібербезпеки. При цьому потрібно активно застосовувати ресурси фахівців МОН, кіберполіції, соціологів, громадськості, бізнесу та молоді. Необхідно аналізувати результати до-

сліджень та широко їх презентувати, а також привести українську термінологію з кібербезпеки у відповідність до європейської.

3. Варто зазначити, що молодь не розуміє всіх ризиків від користування російськими соціальними мережами та не усвідомлює всієї небезпеки, яка може йти від російського піратського програмного забезпечення (насамперед, антивірусів). Через російські соціальні мережі спецслужби отримують інформацію як про користувача, так і про його родичів та друзів. Таким чином, ці дані можуть бути використані у злочинних цілях. Крім того, завдяки геотегам, користування цими сервісами дає змогу з'ясувати місцеперебування людини.

Як показало дослідження, 71,6% підлітків продовжують користуватись російськими мережами; 23% вже не користуються, але мають акаунт; 4,3% видалили свій акаунт; 1,1% не мають (і не мали) акаунту.

Наразі необхідно розробити інформаційну кампанію, яка буде інформувати про ризики користування російськими соціальними мережами і піратським програмним забезпеченням. Це потрібно робити за участі експертів з кібербезпеки, соціологів, медійників, освітян, фахівців з PR і SMM та власне молоді, аби розуміти хід їх думок.

Також треба пропагувати відкрите програмне забезпечення; запровадити обов'язкову стандартизацію програмного забезпечення, яке застосовується в навчальних закладах, задля неприпустимості використання російського та піратського програмного забезпечення (спільними зусиллями МОН та правоохоронних органів, за участі громадських та приватних експертів); пропагувати українські інформаційні продукти й антивіруси зусиллями активістів соціальних мереж, медіа та громадських організацій.

4. Молодь не володіє даними, де можна знайти інформацію про кіберзагрози та як застерегти себе від них. Зокрема, більше половини опитуваних погоджуються, що їм не вистачає знань та потрібно більше відомостей в сфері кібербезпеки. 62% з них не знають, де їх можна знайти. Найбільш поширеним джерелом інформації з питань кібербезпеки виступають соціальні мережі.

Щоб виправити ситуацію, **необхідно:**

- регулярно інформувати молодь про нові кіберзагрози та про те, як можна убезпечитись від них. Це потрібно робити спільними зусиллями кіберполіції та CERT-UA, користуючись допомогою громадських і приватних фахівців, медіа, активістів соціальних мереж;
- просувати вже існуючі, а також створювати нові онлайн ресурси, які сприятимуть підвищенню проінформованості молоді з питань кібербезпеки та кіберзахисту;
- розробити державну просвітницьку програму з кіберзахисту, яка буде орієнтована на молодь (не лише в якості частини шкільного курсу з інформатики, а й в якості окремих курсів).

5. Справедливо буде зазначити, що супільству бракує усвідомлення ризиків, до яких призводить використання проти молоді соціальної інженерії та маніпулювання думками за допомогою соціальних мереж.

Через використання даних, які збираються про користувачів соціальних мереж, інформація подається таким чином, аби сформулювати певні "необхідні" замовнику погляди молоді.

Щоб уникати зазначених ризиків, необхідно підтримувати вже розроблені та сприяти розробці нових програм з критичного мислення, медіаграмотності та інформаційної гігієни, ввести їх в шкільну програму знову ж таки зусиллями МОН та громадських організацій. Доречно буде провести інформаційну кампанію для усвідомлення молоддю ризиків поширення інформації про себе, своїх родичів та друзів в соціальних мережах – зусиллями МОН, офісу Омбудсмена, правоохоронних органів, приватного сектору, соціологів, громадських організацій.

Отже, підсумовуючи всі вищезазначені пункти, можна сформулювати наступні загальні рекомендації для стейкхолдерних груп:

- **Парламенту** необхідно розробити та ухвалити Закон про кібербезпеку, який забезпечить створення ефективної системи кібербезпеки (беручи до уваги потреби молоді) та приведе

українську термінологію в сфері кібербезпеки у відповідність до європейської;

- **Уряду та Міністерству освіти і науки України** треба розробити комплексну державну програму просвітницьких та профілактичних заходів із кібербезпеки в навчальних закладах. Окрім цього, до розробки програми необхідно організувати залучення експертів з кібербезпеки, представників громадськості, бізнесу та молоді. Щоб контролювати процес навчання молоді у відповідній сфері, важливо запровадити регулярне опитування школярів та студентів з питань кібербезпеки, а також проводити олімпіади з питань кібербезпеки та змагання "білих хакерів".
- **Правоохоронні органи** повинні розробити стратегію інформаційної кампанії із метою: широкого інформування про те, куди може звернутися молодь у разі зіткнення з кіберзагрозами; своєчасного інформування про нові кіберзагрози та про те, як можна застерегти себе від них; обширного інформування про результати розслідування інцидентів, особливо тих, де жертвою стала молодь. При цьому важливо використовувти соціальні мережі, адже саме звідти молодь черпає найбільшу частину інформації.
- Нагальною є допомога **зі сторони бізнесу,** який повинен долучитися до: розробки інформаційної кампанії Уряду та МОН; проведення просвітницької роботи в сфері кібербезпеки в навчальних закладах; розробки онлайн-курсів та онлайн ресурсів з кібербезпеки для школярів і студентів, а також їх батьків.
- **Громадські організації** мають брати участь у розробці інформаційної кампанії з Уряду та МОН, а також ініціювати власні просвітницько-інформаційні кампанії. Вагомим внеском буде їх долучення до проведення просвітницької роботи в сфері кібербезпеки в навчальних закладах та пропагування українських інформаційних продуктів.
- **Школам** необхідно проводити факультативні позакласні навчання з кібербезпеки для учнів за участю запрошених вітчизняних експертів, а також демонструвати відеозаписи лекцій міжнародних експертів.

- І звісно ж сама **молодь** повинна брати активну участь у розробці й обговоренні законодавчих ініціатив і державних програм в сфері кібербезпеки. Їй повинна бути надана роль у підготовці та проведенні Українського Молодіжного Форуму з управління Інтернетом. Школярі та студенти повинні піклуватись про підвищення власного рівня обізнаності з питань кібербезпеки, медіаграмотності та інформаційної гігієни. Вони повинні свідомо ставитись до розповсюдження інформації про себе, своїх родичів та друзів і знати наслідки користування небезпечними інформаційними ресурсами.

Таким чином, дослідження показало значні прогалини не лише у знаннях молоді стосовно кібербезпеки, а й у самому відношенні до процесу їх інформування та навчання з боку відповідних стейкхолдерних груп. Лише використовуючи мультистейкхолдерний підхід (беручи до уваги думку молоді) вийде покращити ситуацію та протидіяти загрозам, які з Інтернету переходять у реальний світ та можуть мати серйозні наслідки. Адже тільки комплексний підхід має реальний шанс на подолання та попередження кіберзагроз, які у наш час стали вже звичайною справою.

ЕНЕРГОЕФЕКТИВНІСТЬ ТА SMART-ТЕХНОЛОГІЇ

Протопопов Валентин Володимирович

Завідуючий Навчально-практичним Центром відновлювальної енергетики ДНЗ «Київський професійний коледж з посиленою військовою та фізичною підготовкою»

Голова міської методичної секції педагогічних працівників енергетичних, радіотехнічних і професій радіоелектроніки та зв'язку закладів професійної (професійно-технічної) освіти м. Києва

Керівник Навчально-наукової лабораторії «Noosphere Engineering School - KNU» при Київському національному університеті імені Тараса Шевченко

Керівник Секції «Київ розумне місто – безпечне для життя» Відділення «КИЇВ-СТОЛИЦЯ» КПНЗ «Київська мала академія наук учнівської молоді»

Розумне та автономне місто яке комфортне та безпечне для своїх мешканців. Реалізації цієї концепції напряму залежить від енергопостачання та відповідно автономності роботи всіх ключових елементів забезпечення життєдіяльності міста. Оскільки всі ключові системи комунікації потребують електричного живлення та забезпечення теплопостачання. Системи відновлювальної енергетики є необхідним ланцюгом який забезпечує збереження екології міста, енергоефективність, автономність та невичерпність ресурсів великого міста. Сучасний глобальний світ демонструю високі тенденції створення ризиків різних видів та типів, в результаті яких створюються виклики на які не завжди спроможна реагувати та усувати людина. Тому суспільство потребує таких систем та технологічних рішень які не залежали від наявності людини та її повсякчасного втручання для їх обслуговування.

Пандемія короновірусної хвороби COVID-19 наочно продемонструвала що наявні теплові та атомні станції Україні напряму залежать від присутності на них людини, що в свою чергу несе пряму загрожу життю та здоров'ю цієї самої людини. Тому забезпечення атомності та енергонезалежності забезпечення міста та його функціонування є пріоритетом розвитку сучасних міст. Важливим елементом розумних (smart) технологій є забезпечення підключення до мережі інтернет. І саме забезпечення постійного функціонування цієї мережі є фактором який би впливав на координацію та управління розумними системами. Зелений інтернет – це система забезпечення автономності та енергонезалежності функціонування технологічної інфраструктури мережі інтернет.

На сьогодні в Україні активно використовуються системи відновлювальної енергетики джерелами для яких використовуються енергію: сонця, вітру, біомаси. Ці системи мають високу ефективність та можуть слугувати понад 25 років без втрат потужності та з мінімальним втручанням людини та поточного обслуговування та майже виключним для ремонту. Поєднання систем відновлювальної енергетик різного типу є можливістю для забезпечення роботи самих систем та створення умов для їх автономності. Окупність таких систем складає від 5-6 років в залежності від конфігурації та потужності. На сьогодні ці системи є актуальними для України.

Електрогенерація країни на 53-56% за різними оцінками, залежить від атомної енергетики. Хочу за останні часи ці системи і стали більш безпечними але сам факт існування прецедентів в сучасній історії України доводить , що помилки в цих системах коштують надвеликої та неприпустимої кількості людських життів. Важливим є і те що функціонування енергоблоків атомних реакторів зупиниться для України через 17 років, та вартуватиме для її бюджету понад 15 мільярдів доларів США. В ц вартість включається виведення їх з експлуатації, утилізація ядерного палива та інших технологічних елементів згідно аналітичних даних наведених у *малюнку 1.* Відповідно інформації Державного науково-технічного центру з ядерної та радіаційної безпеки.

Враховуючи вище зазначене сьогодні надважливо створювати технологічну інфраструктуру для забезпечення автономного функціонування ключових систем життєзабезпечення великих міст України. Для цього необхідно використовувати системи відновлювальної енергетики та конфігурувати їх між собою для досягнення необхідних результатів. В свою чергу це забезпечить зелений інтернет, а також комфортне та безпечне життя мешканців великих міст та буде елементом захисту їх від нових глобальних загроз.

Малюнок 1 – Карта атомних електростанцій України.

Теоретичний аналіз і дослідження технологій майбутнього

Крижановська Діана Олександрівна
Студентка 1 курсу
Київський національний торговельно-економічний університет,
diana.krizhanovskaya@gmail.com

Волошина Аріана Русланівна
Студентка 1 курсу
Київський національний торговельно-економічний університет,
arianna.voloshina.nyc15@gmail.com

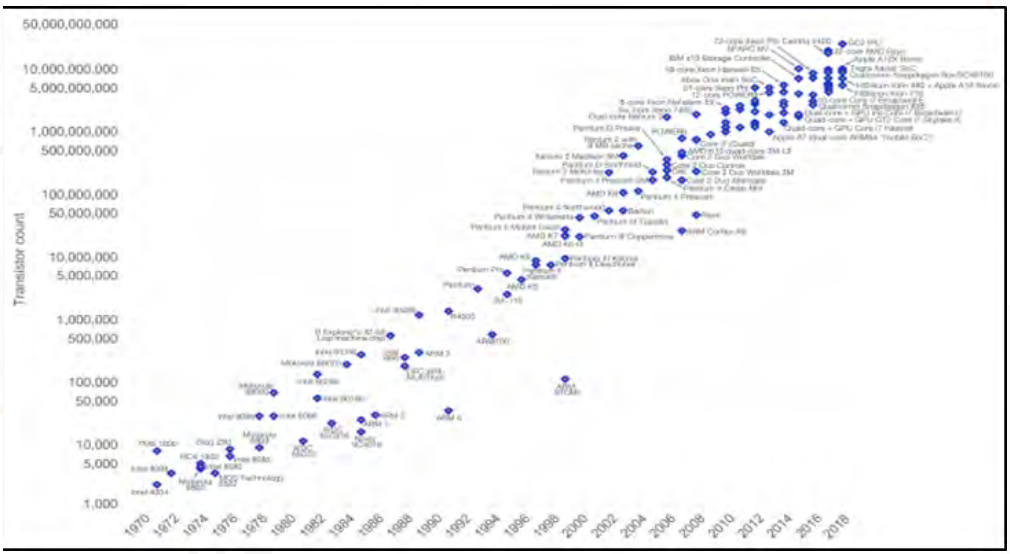
За останні роки сучасні технології настільки змінили життя практично кожної людини, що стає непомітним факт, як швидко людство звикає до їх використання та ,безперечно,відчуває в тій чи іншій мірі залежність від них. Спочатку розглянемо, що таке технології в загальному значенні:

Технології — знання про методи здійснення виробничих процесів та наукова дисципліна, що описує, розробляє і вдосконалює способи забезпечення потреб людства шляхом застосування технічних засобів, процеси та порядок їх здійснення. Як наукова дисципліна технології сприяють впровадженню найефективніших і найекономічніших виробничих процесів, що потребують найменших затрат часу і матеріальних ресурсів[1]. Не викликає жодних сумнівів те, що люди завжди прагнули зазирнути в майбутнє, але й водночас з острахом сприймали його. Розгляньмо такі випадки, як-от технології майбутнього, які навіть існують на даний момент,але в певній формі

з різними функціональними можливостями. Технологічні винаходи,певна річ, займають особливе значення у різних сферах діяльності людини,наприклад, особливо вираженими є медицина,наука та освіта. У результаті цього ми живемо у часи, коли розвиток технологій став настільки швидким, що ми як суспільство вже не встигаємо їх зрозуміти. За судженнями авторів книги «Передбачення:що нам готує найближче майбутнє», людство сприймає новітні технології за допомогою системи переконань, уявлень, вірувань, принципів, які вже є застарілими,технологічно ми вже живемо у майбутньому, а от світоглядно – ще десь в епоху вугілля і сталі[8]. Завдяки цьому тотальне переведення інформації та речей в цифрову форму дозволить виявляти закономірності, які ми пояснити не буде можливо.

Таким чином з'являться знання, що знаходяться поза межею людської свідомості. Цифри їх пояснюють, а людський мозок не розуміє. Дослідження технологічного прогресу демонструють потужну аналітику коливань розвитку та вдосконалення за останні роки в цілому, у тому числі різних корпорацій, які є провідними у цьому питанні *(Рис.1)*. Необхідно сказати, що саме завдяки технологіям все, що ми робимо, завжди перебуває у стані становлення.

Рис. 1



Необхідно зупинитися на такому понятті, як «generation gap»,яке в перекладі з англійської означає « конфлікт поколінь». Напевне, приводячи в приклад сьогодення, можна сміливо стверджувати, що технологічні тренди 2020 року розуміють зовсім не всі, а лише в більшій мірі наше покоління молоді (покоління Z). Саме наше покоління тісно пов'язане із сучасними та майбутніми технологіями, здатне критичним мисленням та ідеями створити таке, що для звичайної людини буде незрозумілим,викликатиме безліч питань та сумнівів. У випадку конфлікту поколінь можна образно виділити відмінності, які пов'язані із впливом технологій. Нарешті, перейдімо до таких сфер майбутніх технологій, які ми б хотіли прослідити на основі власних переконань та міркувань: медицина та освіта. Нові технології потрібно розробити, створити, втілити в реальність[5]. Деякі технології, які розробляються вже зараз, дозволяють зазирнути в майбутнє і уявити, чого від нього можна очікувати.

Технології у медицині

Щороку понад 25 % пацієнтів помирають через нестачу донорських органів. Ця проблема стала глобальною у світі медицини, оскільки наявність необхідних біоматеріалів та відсутність бюрократичних проблем могли б урятувати сотні життів. Розглянемо один із новітніх винаходів людства – 3D-друк медичних імплантів. У дослідних центрах і лікарнях по всьому світу досягнення в області 3D-друку і біопринтінгу надають нові можливості для лікування людей і наукових досліджень. У найближчі десятиліття біопринтінг може стати наступною важливою віхою в охороні здоров'я і персоналізованої медицини.

Принцип роботи 3D-принтера. Традиційні принтери, такі як у вас удома чи в офісі, працюють у двох вимірах. Вони можуть друкувати текст чи зображення на папері, використовуючи певний розмір в довжину та ширину. 3D принтери додають ще один вимір – глибину. Під час друку головка принтеру рухається уверх та вниз, вліво та вправо. Замість того, аби доставляти чорнила на папір, 3D принтери розподіляють різні матеріали – пластик, метал, кераміку, шоколад, тощо — до друку цілісного, об'ємного предмета, шар за

шаром в процесі відомого як «адитивне виробництво»,аби створити 3D-об'єкт, потрібен план – цифровий файл, що створений за допомогою програмного забезпечення для моделювання. Після створення згенерована модель відправляється до принтера[4]. Матеріал завантажений у пристрій та готовий до нагріву, аби легко витікати з принтера. Головка пристрою переміщується, вносячи шари обраного вами матеріалу для створення кінцевого продукту. При друкуванні кожен нанесений шар перетворюється у тверду форму або шляхом охолодження, або при змішуванні двох різних розчинів, які подаються через сопло принтера. Нові шари ідеально лягають на попередні, аби отримати стійкий елемент. Таким способом можна створити практично будь-яку форму.

Біопринтери працюють ідентично 3D-принтерам. Але є одна суттєва різниця – вони наносять шари біоматеріалу, які містять в собі живі клітини для створення складних структур, на кшталт кровоносних судин або шкіри.

Медицина – консервативна і дуже наукомістка індустрія, яка з великою пересторогою ставиться до будь-яких інновацій. Розробка нових формул лікарських речовин коштує сотні мільйонів доларів США, випробування нових ліків можуть проводитися роками і навіть десятками років[3]. Нарешті перейдемо до прикладів досягнень у біо-розробці на сьогоднішній день *(Табл.1)*.

Кістки	Команда дослідників Університету Суонсі у 2014 році розробила технологію біологічного друку, що дозволяє створювати штучний кістковий протез у такій же формі, який потрібен. Над такими ж дослідженнями водночас працювали й вчені з Ноттінгемського університету в Англії.
Хрящі	Ще у 2015 році вчені з Цюриха розробили технологію, котра дозволить лікарням друкувати повноцінний імплантат людського носа менше як за 20 хвилин. Вони вважають, що будь-який хрящовий імплантат може бути виготовлений за їх методою.
Шкіра	Вчені медичної школи Уейк Форест успішно розробили, побудували та протестували принтер, що може друкувати клітини людської шкіри безпосередньо на рані з опіком. Сканер точно визначає розмір та глибину пошкоджень. Ця інформація передається на принтер після чого шкіра друкується безпосередньо на рані.

Кровоносні судини	Інженер-біомеханік Моніка Мойя з Ліверморської національної лабораторії ім. Лоуренса використовує біодрук для створення кровоносних судин. Матеріали, створені її біопринтером, спроектовані таким чином, щоб дозволити маленьким кровоносним судинам розвиватися самостійно.
Сечовий міхур	У 2013 році в Університеті Уейк Форест у США дослідники успішно взяли клітини з хворого сечового міхура пацієнта, культивували їх додавши додаткові корисні речовини. Потім була надрукована трьохвимірна форма сечового міхура пацієнта. Форма була поміщена в інкубатор та коли вона досягла потрібної кондиції її пересадили у тіло пацієнта. Форма з часом зруйнується, залишивши лише органічний матеріал. Та ж команда успішно створила життєздатну уретру.
Нирки	Австралійські вчені займаються подібними дослідженнями. Вони використовували людські стовбурні клітини для вирощування ниркового органу, котрий має всі необхідні типи клітин для нирок. Такі клітини можуть слугувати цінним джерелом для біодруку складнішої структури нирок.
Серце	У квітні 2019 року ізраїльські вчені надрукували перше у світі трьохвимірне серце. Воно ще дуже маленьке, розміром як вишня, але здатне виконувати свою функцію. Трьохвимірне серце з кров'яними судинами використовує персоналізовані «чорнила» з колагену.

Технології у освіті

Нові технології стрімко проникають у навчальний процес, тому перейдемо до перспектив їх розвитку та використання у майбутньому.

Біометрія. У майбутньому комп'ютери розумітимуть наш фізичний та емоційний стан. Роботи зможуть реагувати на вираз обличчя, голос, пульс і навіть запах учня. Вони будуть слідкувати за ритмом та швидкістю, з якими студент набирає текст. Все це допоможе роботам розуміти, наскільки добре засвоюється інформація. І в разі необхідності пояснити матеріал студенту ще раз, але з використанням індивідуальної методики, яка найбільш підходить конкретному учню.

Нейростимуляція. Сучасні вчені зайшли значно далі: розробили спеціальний пристрій, що нагадує шапку. Він здатний наповнюва-

ти людський мозок потрібною інформацією за допомогою струму. Стимулятор створили аби «годувати» наш мозок і дати людям можливість покращити вже набуті знання. Вперше апарат протестували на пілотах-початківцях.[7] Результати показали, що ті пілоти, які використовували стимулятор – засвоїли на 33% більше знань, ніж ті, хто ним не користувався.

Лінзи «Додаткова реальність». Google вже застосовує окуляри доповненої реальності. Але вчені запевняють, що це тільки початок. Наступний крок – створення лінз, які матимуть тонкий вбудований екран. Ми отримаємо легкий доступ до інформації, котра з'являтиметься прямо перед очима. Розробники запевняють, що лінзи доповненої реальності дозволять шукати інформацію в Інтернеті без використання інших гаджетів[6]. Викладачі та студенти зможуть відправляти е-мейли з необхідним матеріалом для навчання. За допомогою лінз студенти робитимуть спільні проекти, що займатиме менше часу.

Ручка, що копіює реальність. Творчі та неординарні особистості можуть радіти. Вчені працюють над створенням ручки, яка копіюватиме реальний колір речей, що нас оточують. Тож студентам не потрібно більше жодних пеналів, а художникам – фарб. Достатньо доторкнутися ручкою до потрібного кольору і продовжити писати чи малювати.

Поверхні multi-touch. Сенсорні екрани вже давно звичне явище. Але такі корпорації як Microsoft не зупиняються на подібних досягненнях. Вони вже певний час працюють над створенням поверхонь із технологією мультитач. Вчені запевняють – одного дня університетські аудиторії повністю зміняться завдяки цій технології. Зошити та ручки залишаться у далекому минулому. Увімкнув парту – і пишеш конспект, робиш лабу або створюєш проект разом зі своїми одногрупниками. Завдяки одному лише дотику до такої парти, студентам будуть доступні мільйони онлайн-ресурсів.

Висновок

Отже, поява технологій, що дозволяють машинам вчитися, мислити та приймати рішення, має величезне значення для працівників найрізноманітніших напрямків, а також приватних і державних підприємств, бізнесу, всіх галузей і економіки в цілому[5]. Нині ми є свідками революції, яка змінить не тільки світ, в якому ми живемо, а й саму людину. Вже звичними стають речі, які лише десять років тому видавалися далекою фантастикою.

Список використаних джерел:

1. «Технологія» // Українська радянська енциклопедія : у 12 т. / гол. ред. М. П. Бажан ; редкол.: О. К. Антонов та ін. — 2-ге вид. — К. : Головна редакція УРЕ, 1974–1985.
2. Тетяна Колісник, «Ваше здоров'я» / 5 лют 2018
3. https://www.imena.ua/blog/3d-bioprint-part-1/
4. https://community.com.ua/ru/statti/3d-biodruk-meditsina-maybutnogo/
5. https://blog.lavkababuin.com/ukr/zazyraiemo-v-maibutnie-iak-tekhnolohii-zminiuiut-nas-i-nashe-zhyttia-chastyna-1/
6. https://studway.com.ua/tekhnologii-zminyat-vishi/
7. Naked Science, British American Tobaco, The Ohio State University.
8. «Передбачення: що нам готує найближче майбутнє Джефф Хоу, Джой Ітo.

Безпека баз даних

Івкіна Ірина Миколаївна
КНТЕУ, м. Київ, Україна
ivkina.irina02@gmail.com

Матвієнко Іван Олександрович
КНТЕУ, м. Київ, Україна
proffzip2@gmail.com

Вступ

Атаки на сховища і бази даних є одними з найнебезпечніших для підприємств і організацій. В останні роки кількість витоків даних в світі неухильно зростає, при цьому на 2015 рік понад тридцять відсотків з них припадають на зовнішніх порушників і більше шістдесяти виконано за участю співробітників організації. Навіть якщо припустити, що в ряді випадків витік включала дані, до яких співробітник має легальний доступ, кожен третій випадок припадав на зовнішню атаку. Також потрібно відзначити, що на зовнішні атаки припадають сім з восьми витоків обсягом понад десяти мільйонів записів.

Зловмисників цікавлять такі види інформації, як внутрішня операційна інформація, персональні дані співробітників, фінансова інформація, інформація про замовників / клієнтів, інтелектуальна власність, дослідження ринку / аналіз діяльності конкурентів, платіжна інформація . Ці відомості в результаті зберігаються в корпоративних сховищах і базах даних різного об'єму.

Все це призводить до необхідності забезпечення захисту не тільки комунікацій, операційних систем та інших елементів інфраструктури, а й сховищ даних як ще одного бар'єра на шляху зловмисника. Однак на сьогоднішній день роботи в галузі забезпечення безпеки баз даних спрямовані в основному на подолання існуючих і вже відомих вразливостей, реалізацію основних моделей доступу і розгляд питань, специфічних для конкретної системи управління базами даних.

Метою даної роботи є комплексний розгляд і систематизація питань безпеки різних баз даних в світлі нових загроз, загальних тенденцій розвитку інформаційної безпеки і зростання ролі і різноманітності сховищ даних.

Поняття баз даних

Під базою даних розуміється не просто оброблена інформація, що зберігається в файлі або групи файлів, а правильно організована і підготовлена для користувача. Для роботи з базами використовуються програмні засоби захисту і управління - системи управління базами даних (СКБД), які передбачають застосування мов програмування, що забезпечують єдині принципи опису, зберігання і обробки інформації.

Як програмна оболонки для баз даних найчастіше використовуються Oracle Database, MS SQL Server, MySQL (MariaDB) і ACCESS.

На практиці використовуються наступні типи баз даних: фактографічна, документальна, розподілена, централізована, неструктурована.

Загрози безпеки баз даних

Вибудовування ефективної системи безпеки баз даних потребує оцінки загроз з опорою на цінність інформації і на практику злочинного посягання на дані. Основними загрозами є:

- несанкціоноване використання інформації в БД системними адміністраторами, користувачами, хакерами;

- вірусні атаки з різними наслідками;
- SQL-ін'єкції, довільно змінюють код або переформатують бази;
- технічні проблеми, зниження продуктивності, відмова в доступі, що виключають можливість використання інформації;
- фізичний збиток, нанесений обладнанню або каналам зв'язку;
- помилки, недоробки, несанкціоновані можливості в програмах, які керують базами, і іншому ПО, найбільш уразливі операційні системи.

Захист баз даних

Основні поради щодо захисту баз даних підприємств:

1. Контролюйте доступ до бази даних.

Запобігти атакам кіберзлочинців допоможуть обмеження дозволів та привілеїв. Крім базових системних дозволів, слід застосувати:

- Обмеження доступу до конфіденційних даних для певних користувачів і процедур, які можуть робити запити, пов'язані з конфіденційною інформацією.
- Обмеження використання основних процедур тільки певними користувачами.
- Уникнення використання і доступу до баз даних в неробочий час.

Також для запобігання атакам зловмисників рекомендують вимкнути всі служби і процедури, які не використовуються. Крім того, базу даних слід розміщувати на сервері, недоступному безпосередньо через мережу Інтернет, щоб запобігти віддаленому доступу зловмисників до корпоративної інформації.

2. Визначте критично важливі дані.

Першим кроком має стати аналіз важливості захисту для конкретної інформації. Для полегшення визначення місця та способу збереження

конфіденційних даних слід зрозуміти логіку і архітектуру бази даних. Не всі дані є критично важливими або потребують захисту, тому на них немає сенсу витрачати час і ресурси.

Спеціалісти також рекомендують провести інвентаризацію баз даних компанії, обов'язково врахувавши всі відділи. Ефективним способом для запобігання втраті інформації може бути фіксація всіх копій і баз даних компанії. Інвентаризація особливо важлива під час виконання резервного копіювання інформації для врахування всіх критично важливих даних.

3. Шифруйте інформацію.

Після ідентифікації критично важливих даних потрібно застосувати надійні алгоритми шифрування конфіденційної інформації. У разі використання уразливості або отримання доступу до сервера або системи, зловмисники в першу чергу спробують викрасти бази даних, які, зазвичай, містять багато цінної інформації. Кращий спосіб захистити базу даних — зашифрувати її для осіб, які намагаються отримати доступ без авторизації.

4. Зробіть анонімними непродуктивні бази даних.

Багато компаній інвестують час та ресурси у захист своїх продуктивних баз даних, але при розробці проекту або створення тестового середовища вони просто роблять копію вихідної бази даних і починають використовувати її в середовищах з менш жорстким контролем, тим самим розкриваючи всю конфіденційну інформацію.

За допомогою маскування та анонімізації можна створити аналогічну версію з тією ж структурою, що і оригінал, але із зміненими конфіденційними даними для їх захисту. За допомогою цієї технології значення змінюються за умови збереження формату. Дані можуть бути змінені шляхом змішування, шифрування, переставляння символів або заміни слів. Конкретний метод, правила і формати, залежать від вибору адміністратора, але незалежно від вибору, метод повинен забезпечити неможливість отримати вихідні дані за допомогою зворотньої інженерії.

Цей метод рекомендовано використовувати для баз даних, які є частиною середовища тестування і розробки, оскільки він дозволяє зберегти логічну структуру даних, забезпечуючи відсутність доступу до конфіденційної інформації поза виробничим середовищем.

5. Проводьте моніторинг активності бази даних.

Аудит і відстеження дій всередині бази даних передбачає знання про те, яка інформація була оброблена, коли, як і ким. Володіння повною історією транзакцій дозволяє зрозуміти шаблони доступу до даних і модифікацій і, таким чином, допомагає уникати витоку інформації, контролювати небезпечні зміни і виявляти підозрілу активність в режимі реального часу.

Висновки

Отже, в даній статті проаналізовано основні загрози для баз даних та поради щодо їх уникнення. Проаналізувавши всі існуючі методи захисту інформації баз даних, можна зробити висновок, що використання лише якогось певного методу не може гарантувати повного зберігання даних. Тому для підвищення рівня безпеки інформації в базах даних рекомендовано використання комплексних заходів. Підсумовуючи, можна зробити висновок, що розробки в даній галузі є досить актуальними та вартими подальшої підтримки. Бази даних мають досить високий попит у сучасному світі, саме тому їх захист потребуватиме постійного вдосконалення.

Список використаних джерел

1. http://swsys.ru/index.php?page=article&id=4175&lang
2. https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-baz-dannykh/
3. https://eset.ua/ua/blog/view/14/-
4. https://ru.wikipedia.org/wiki/Database_security

ПРОБЛЕМИ РОЗВИТКУ ІНТЕРНЕТУ РЕЧЕЙ

Костюк Юлія Володимирівна

Костюк Кирил Ігорович

Київський національний торговельно-економічний університет, Україна

Економіко-правовий ліцей, Україна

kostyuk_yu@knute.edu.ua

Якщо подивитися навколо, то побачимо себе оточеними розумними гаджетами. Навіть у багатьох новинах, пов'язаних з такими розумними девайсами досить часто чуємо словосполучення «інтернет речей». А ви маєте пристрій, що відправляє дані на ваш смартфон? Як, знаходячись в дорозі, за допомогою лише девайсу і мобільного інтернету, зберігати своє помешкання в безпеці? Так ось, за цим стоїть Інтернет речей - технологія, що набирає популярності у світі. Квартири, будинки та цілі міста все активніше використовують цю технологію в реальному житті.

Вперше термін "Інтернет речей" (Internet of Things, IoT) запропонував один з трьох засновників центру автоматичної ідентифікації Масачусетського університету Кевін Ештон в 1999 році. А першою інтернет річчю вважається тостер Джона Ромки, одного з засновників протоколу TCP/IP, якого в 1990 році Джон підключив до інтернету та змусив дистанційно включатись та вимикатись. За оцінкою корпорації Cisco кількість пристроїв, які підключені до інтернету вже в 2009 році перевищила кількість людей на нашій планеті. А в 2020 році кількість речей підключених до інтернету сягнула відмітки в 30 млрд.

Така велика кількість пристроїв, підключених до інтернету, висвітила і технологічні проблеми розвитку цієї галузі. По-перше, виникає питання ідентифікації кожного пристрою, що пов'язано з тим, що кожен

пристрій в інтернеті повинен мати свій унікальний ідентифікатор. Цю задачу вирішує протокол IP. Але протокол IP версії IPv4 дозволяв присвоїти всього лише 4,22 мільярда адрес. Саме тому розробники вимушені були створити версію IPv6, яка вирішила дану проблему.

По-друге, виникла задача обробки і зберігання великої кількості інформації, яка виробляється пристроями IoT. За даним аналітиків в 2020 році ця кількість складає десятки мільярдів терабайт даних. Тому в компанії Microsoft вважають, що головна частина Інтернету речей - це не датчики і засоби передачі даних, а хмарні системи, що забезпечують високу пропускну здатність і здатні швидко реагувати на певні ситуації (наприклад, вміти за показаннями датчиків з'ясувати, що в будинку вже п'ять хвилин нікого немає, а вхідні двері залишилася відкритими) [1].

Третя проблема пов'язана з високою швидкістю розвитку цього ринку та великою кількістю виробників. Виникла необхідність створити єдині стандарти в цій галузі. Цю проблему взявся вирішити глобальний партнерський проект oneM2M, заснований в 2012 році та який складається з 8 провідних світових організацій з розробки стандартів, зокрема: ARIB (Японія), ATIS (США), CCSA (Китай), ETSI (Європа), TIA (США), TSDSI (Індія), TTA (Корея) и TTC (Японія).

Використання IoT в багатьох галузях обмежено проблемою в забезпеченні інформаційної безпеки, конфіденційності та безпеки інформації. Найбільшою проблемою IoT є низький рівень захищеності системи. Пристрої не мають жодних антивірусів або навіть систем ідентифікації користувача. А коли вони ще й під'єднуються до інтернету, хакери спокійно можуть викрасти будь-яку інформацію. До загроз відносяться: несанкціонований доступ, перехоплення даних користувача, порушення конфіденційності, цілісності інформації, DoS-атаки, віруси, експлойтери, мережеві черв'яки, тощо [2,3,4].

Іноземні фахівці приділяють велику увагу науковим і експериментальним дослідженням в забезпеченні інформаційної безпеки Інтернету речей. Прийняття обґрунтованих заходів безпеки, що протистоять виявленим недолікам, а також впровадження різних систем виявлення вторгнень, криптографічних заходів безпеки в процесі обміну інформацією та використання ефективних методів комуніка-

ції призведе до створення більш безпечної і надійної інфраструктури Інтернету речей, що зможе гарантувати безпеку інформації та майна користувача.

Список використаних джерел

1. Петруня А., Інтернет речей. Новомодне захоплення чи технологія, що змінює світ? [Електронний ресурс] / Петруня А. // Економічна правда – 2015.
2. Наконечний А. Й. Інтернет речей і сучасні технології / А. Й. Наконечний, З. Є. Верес // Вісник Національного університету «Львівська політехніка». Серія: Автоматика, вимірювання та керування. – 2016. – № 852. – С. 3–9.
3. Соколов М.Н., Смолянинова К.А., Якушина Н.А. Проблемы безопасности интернета вещей: обзор. — Вопросы кибербезопасности : журнал. — 2015. — № 5(13). — 34с.
4. Лукацкий А.С. Криптография в «Интернете вещей» // www.slideshare.net : сайт. — 2016. — 23 марта

РОЗУМНИЙ БУДИНОК ЯК ПРОДУКТ ВПРОВАДЖЕННЯ КОНЦЕПЦІЇ ІНТЕРНЕТУ РЕЧЕЙ

Сітало Максим Сергійович
ліцеїст 9-Б класу
Криворізького природничо-наукового ліцею,
м. Кривий Ріг,
sitalomasim8@gmail.com

Неочікувана поява вірусу COVID-19 викликала глобальну пандемію на території всієї планети. Передбачуваною реакцією голів держав на масову захворюваність та смертельні випадки стало обмеження або, навіть, повна заборона на переміщення людських мас територіями держав, континентів. Вимушена ізоляція поставила питання перед соціумом щодо організації повсякденного життя наближено до комфортних умов існування. Зважаючи на те, що протягом трьох-шести місяців, люди повинні бути виключеними із звичного середовища, ключовим об'єктом побудови мережі спілкування, замовлення необхідних для життя товарів, застосування та використання систем життєзабезпечення, стала мережа Інтернет.

Протягом майже тридцяти років, починаючи з моменту як один із творців протоколу TCP/IP Джон Ромки підключив до мережі свій тостер, сучасне суспільство ознаменувало початок епохи Інтернет-речей. Експертна оцінка визначає справжніми початком ери технології IoT у 2013 році, однак цей момент не викликав у громадськості сплеску інтересу, оскільки спочатку IoT стартувала як технологія взаємодії машин без участі людини (machine-to-machine, M2M) для бездротових систем моніторингу.

На сьогодні вже важко знайти людину, що хоча б раз у житті не скористалась можливостями IoT, основи її розробки були включені до курсу вивчення інформатики у середній школі.

Насамперед, зауважимо, що IoT не можна визначити технологією у певному значенні цієї дефініції. IoT – це концепція, ідея створення обчислювальної мережі фізичних об'єктів, що містять у собі технології для взаємодії один з одним та (або) із зовнішнім простором. Якщо звичайний Інтернет – лише спосіб поєднання комп'ютерів, то «Інтернет речей» це - спроба вийти за його межі. Отже, IoT може стати наступним кроком у розвитку «фізичного» інтернету, метою якого буде поєднання всіх систем заради забезпечення комфортного існування соціуму.

Поширеним прикладом Інтернету речей є технологія «Розумний будинок». Розумними, наразі, називають будинки, у яких за безпекою, енергозбереженням і комфортом стежить програмне забезпечення, що поєднує побутові прилади в єдину систему за допомогою технології передавання даних. Такий будинок самостійно керує освітленням і може вимикає світло в кімнаті, відслідковуючи місцезнаходження людини, стежить за споживанням води, станом стічних труб якості повітря, попереджає про можливість загоряння, автоматично поливає домашні рослини і годує домашніх вихованців, тощо. З такою системою можна не тільки бути впевненим у безпеці будинку, а й взагалі не відволікатись на побутові проблеми.

На ринку Інтернету речей представлено безліч систем, що працюють з відповідним програмним забезпеченням, у тому числі й мобільним. Проте їх встановлення потребує додаткового обсягу пам'яті, відповідності програмного забезпечення, нарешті, рівня обізнаності користувача у питаннях застосування й використання комп'ютерних технологій. Тому, ми вбачаємо можливість підключення всіх пристроїв через сайт, який поєднає в собі доступ до застосунків та пристроїв вимірювання, контролю і їх доцільного використання.

Представлений макет сайту дозволяє споживачу дізнатися про переваги розумного будинку та смарт-систем, порівняти їх енергоефективність і практичність зі звичайними електроприладами, а

також в режимі он-лайн перейти на сайти надавачів комунальних послуг задля моніторингу вартості спожитого продукту, вчасно обрахувати і здійснити оплату. Таким чином, споживач не буде самостійно здійснювати пошук окремих сайтів компаній-постачальників, а безпосередньо з основного здійснюватиме необхідні операції.

Передбачено також можливість купити на сайтах провідних інтернет-магазинів відповідні продукти для організації розумного будинку. Така гіперлокація дозволить користувачу підібрати компоненти, замовити їх доставку та провести оплату, не лишаючи безпечного середовища будинку.

Список використаних джерел

1. Електронний ресурс - https://www.everest.ua/iot-vse-shho-potribno-znaty-pro-internet-rechej-i-pro-majbutnye-suchasnoyi-czyvilizacziyi/
2. Бехман Г. Современное общество: общество риска, информационное общество, общество знаний. М:Логос, 2010.-248 с.
3. Труханенко Г. М. Інформаційний простір ліцею як умова творчого зростання вчителя / Г. М. Труханенко // Вища освіта України. – 2012. – № 3. – С. 555-562.

НОВИЙ СВІТ – НОВІ ПРОФЕСІЇ

Труханенко Марія Олексіївна
студентка Ужгородського національного університету,
факультет фізики,
stenberglev@gmail.com

Із широким розповсюдженням мережі Інтернет виникла можливість поєднати людей з різних країн, континентів, з різними думками та бажаннями. Вибуховим контентом стала поява такого комп'ютерного феномену як соціальні мережі. З плином часу, широкий спектр різних платформ для спілкування перестав бути лише «сучасним телефоном». Можливості поєднувати однодумців за різними запитами або потрібностями почали використовуватись для пропозиції різного роду товарів, тобто з'явився Інтернет речей.

Та як ефективно продавати в соціальній мережі, як правильно визначати коло осіб, які будуть зацікавлені саме у вашому ресурсі? Є виклик - з'являється і пропозиція.

Відповіддю на запити суспільства з'являється новий спеціаліст – таргетолог. На теренах українських інтернет - видань не міститься науково обґрунтованого терміну, що відповідає самому змісту даного соціального явища. Спробуємо, використовуючи доступні ресурси, виявити основі концептуальні поняття даного феномену.

Таргетолог - це фахівець, який займається налаштуванням таргетованої реклами у соціальних мережах. Слово «таргет» з англійської перекладається як «мета», тому таргетована реклама - це реклама, налаштована на певну цільову аудиторію. Таргетолог - перспективна спеціальність. Таргетована реклама займає друге місце

за популярністю у рекламодавців, а компанії планують збільшувати бюджети на таргетовану рекламу.

Фахівець, який займається рекламою в соціальних мережах, налаштовує рекламу таким чином, щоб вона була доступною не всім підряд, а тільки певній групи людей - цільової аудиторії. Цільова аудиторія формується за профілем в соціальних мережах. Ми стаємо частиною певної аудиторії, коли заповнюємо профіль: вказуємо стать, вік, інтереси, групи, місце розташування. Завдання таргетолога – визначити основні запити і інтереси відповідної категорії користувачів мереж та налаштувати рекламу під потрібну аудиторію. Щоб визначити цільову аудиторію, потрібно бути трохи психологом, аналітиком і навіть детективом. Працювати таргетологом буде простіше, якщо вам вдається: мислити аналітично; мати стратегічне бачення проблеми; працювати в режимі багатозадачності і вести кілька проектів одночасно; експериментувати і брати відповідальність за виконання проекту; постійно вчитися і освоювати нові способи ведення рекламних кампаній.

Враховуючи той аспект, що в соціальних мережах панує неформальне спілкування, необхідно щоб і реклама може бути творчою і неформальною. Роботодавці цінують нестандартний підхід і почуття гумору. Також треба мати розуміння і принципи мислення людей нового покоління, яке називають «кліповим», а саме: прихильники спілкування в соціальних мережах усвідомлюють інформацію за короткий проміжок часу, показують зацікавленість у товарі лише декілька секунд. Тому, таргетолог повинен уміти багато: вибирати майданчик під рекламу, відстежувати рекламні кампанії, визначати коефіцієнт конверсії по кожному каналу, працювати з інструментами автоматичного парсинга, володіти веб-аналітикою, знати Excel.

Визначення цільової аудиторії - одна з основних задач таргетолога. Професійний таргетолог повинен вміти спілкуватися з замовником, аналізувати пропозиції конкурентів і самостійно визначати портрет цільової аудиторії, її інтереси і «болю». Чим точніше буде складено портрет цільової аудиторії, тим більша ймовірність того, що рекламу побачить потенційний клієнт.

Отже, можемо визначити, що з однієї позиції таргетолог - вузькопрофільний фахівець з просування реклами в соціальних мережах, навіть існує і більш вузька спеціалізація: деякі таргетологі працюють тільки з однією соціальною мережею і її рекламним кабінетом. Разом з тим такий спеціаліст повинен володіти широкими знаннями у сфері психології, маркетингу, логістики, мати уявлення про аналітику, вільно володіти комп'ютерними технологіями для роботи з базами даних. Вважаємо, що даний феномен потребує подальшого вивчення та усвідомлення впливу глобальної мережі Інтернет на життя людини.

Список використаних джерел

1. Електронний ресурс : https://johar.ru/en/disasters/targetolog-eto-chto-za-professiya-obuchenie-sostavlenie-rezyume-poisk-raboty-i/
2. Електронний ресурс : https://myacademy.ru/baza-znanii/stati/kto-takoi-targetolog

LIKE
SHARE