Cybersecurity from the point of view of Ukrainian Youth
(draft report)

The aim of the research is to analyze the role of Internet users (especially young) in Internet Governance and cybersecurity in Ukraine (from the point of view of different stakeholders), to analyze relevant Ukrainian policy landscape.

1. Cybersecurity landscape in Ukraine

Legislative level:

- Council of Europe Convention on cybercrime (signed by Ukraine in 2001, entered in force in 2006 – not in full, until now);

- Law on basis of cyberserity in Ukraine (2017);

- Strategy on cybersecurity (2016);

- Ukrainian President's Decree №133/2017 (on blocking access to a number of Russian websites in Ukraine, such as Yandex, Vkontakte and Odnoklassniki).

Institutional level:

There is no one coordination center for cybersecurity in Ukraine.

We have governmental stakeholders, such as:

- National Security and Defense Counsel of Ukraine;

- State Service of Special Communications and Information Protection of Ukraine (CERT-UA);

- cyberpolice;

- Security Service of Ukraine

and a lot of others.

Private stakeholders:

- Zillya (Ukrainian antivirus);

- Deloitte, ISSP, Berezha Security.

- Cisco, Cognitix.

Civil society:

- La Strada;

- European Media Platform;

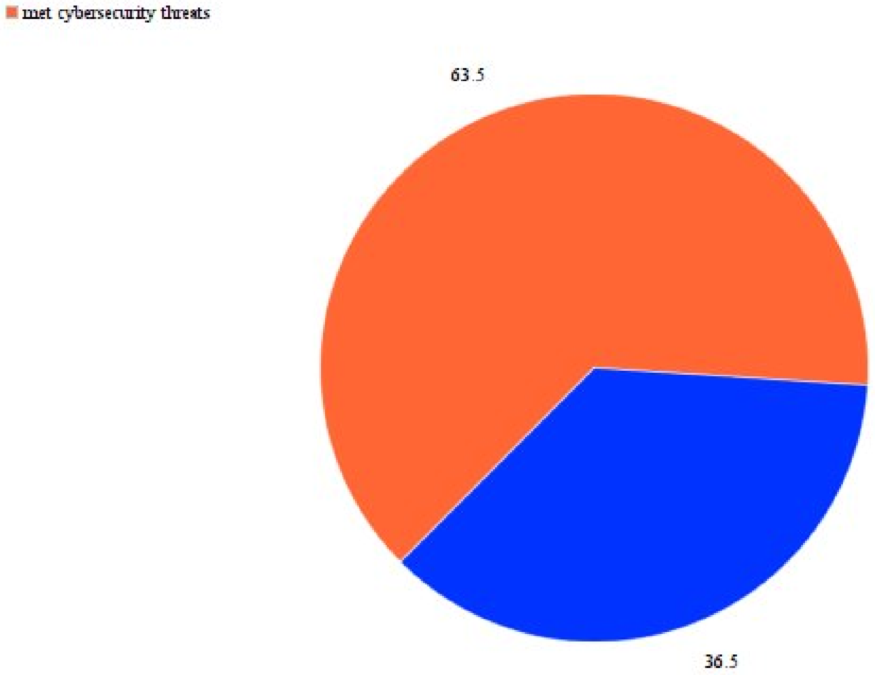
- Internews

Youth organizations:

Minor Academy of Sciences of Ukraine.

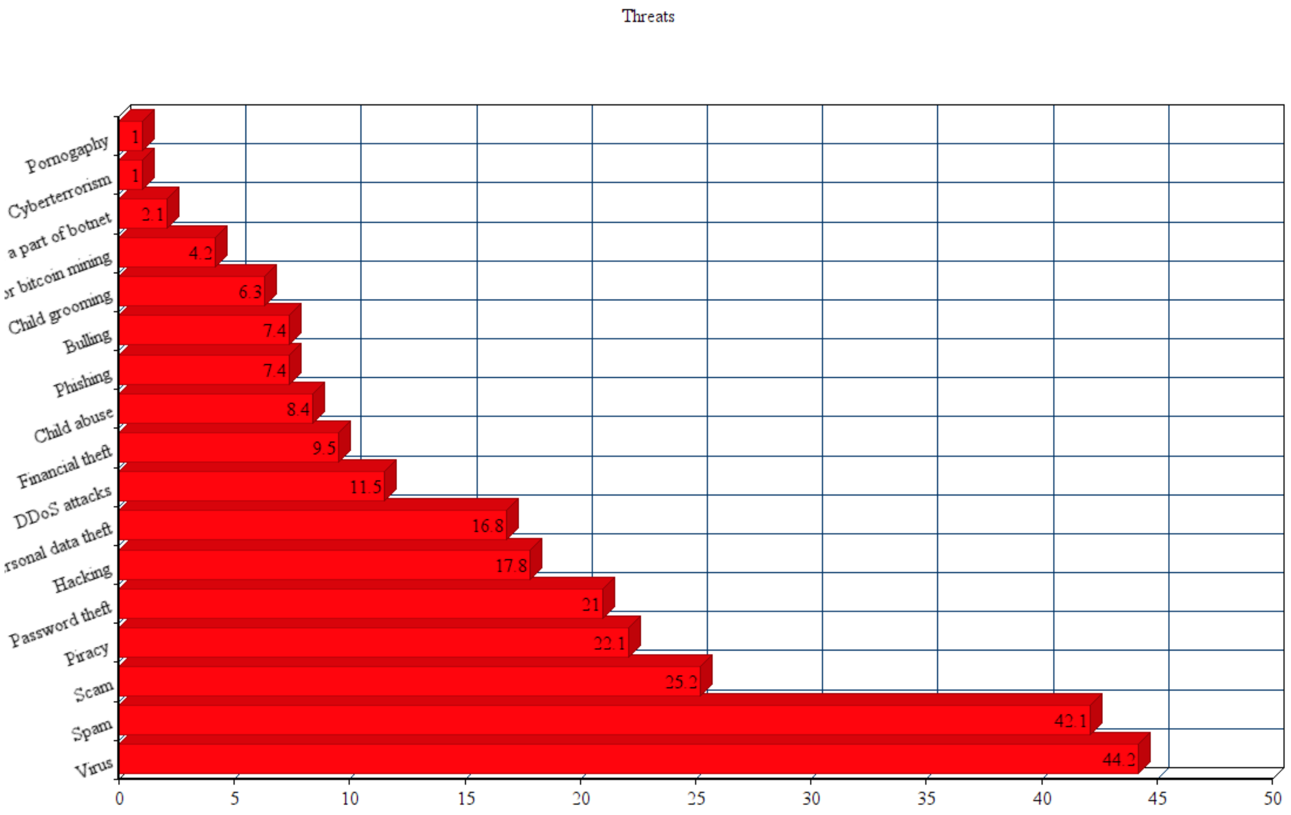
2. Within the framework of the Counterpart International project iNGO European Media Platform conducted opinion poll in focus-groups (students of one Kyiv school, one Kyiv college, one Kyiv university). The text of questionnaire is attached as AnnexA.

Results of this opinion-poll:
63,5% respondents (14-20 years old) met cybersecurity threats.

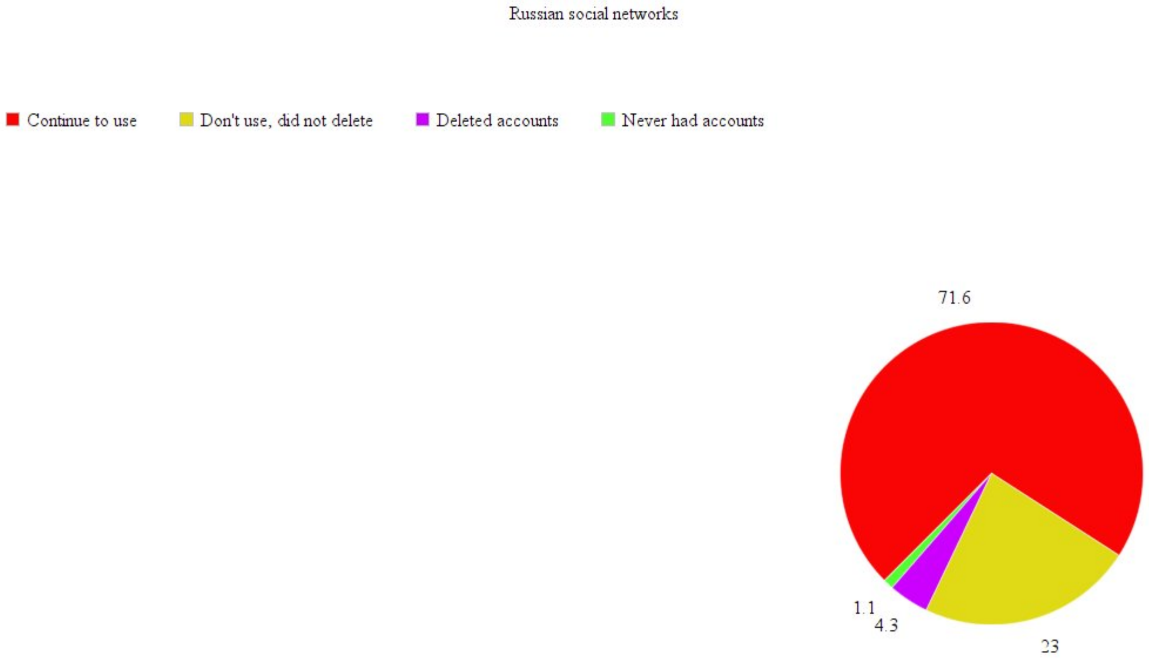


Which threats?

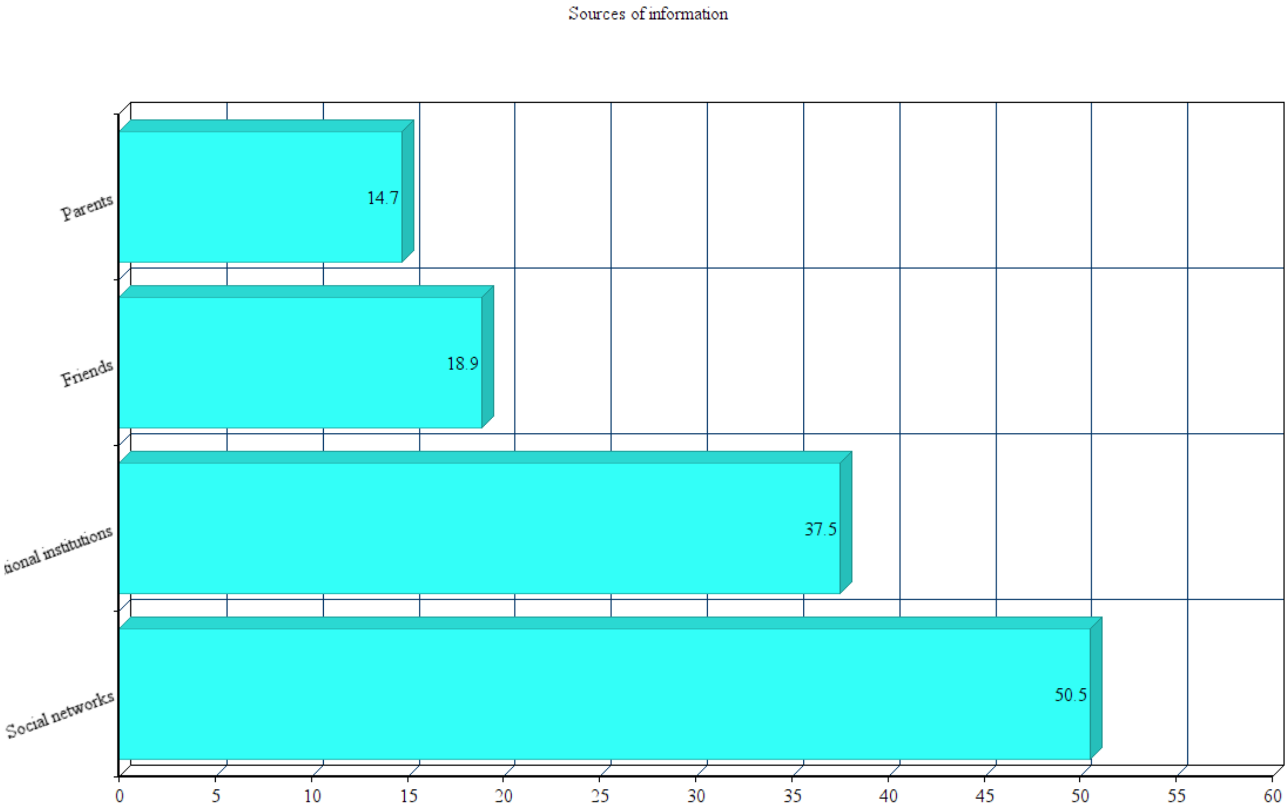
Virus – 44,2
Spam – 42,1
Scam – 25,2
Piracy – 22,1
Password theft – 21
Hacking – 17,8
Personal data theft – 16,8
DDoS attacks – 11,5
Financial theft – 9,5
Child abuse – 8,4
Phishing – 7,4
Bulling – 7,4
Child grooming – 6,3
Using computer for bitcoin mining – 4,2
Using computer as a part of botnet – 2,1
Cyberterrorism – 1
Pornography – 1



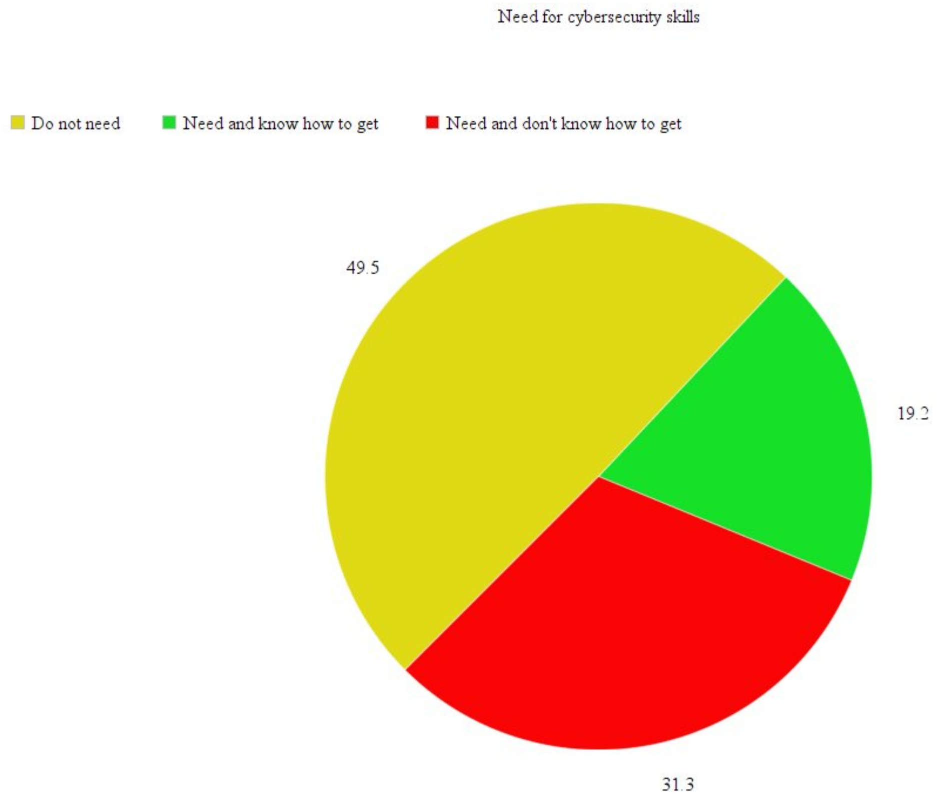
98,9% of respondents had accounts in Russian social networks, 71,6% continue to use them.



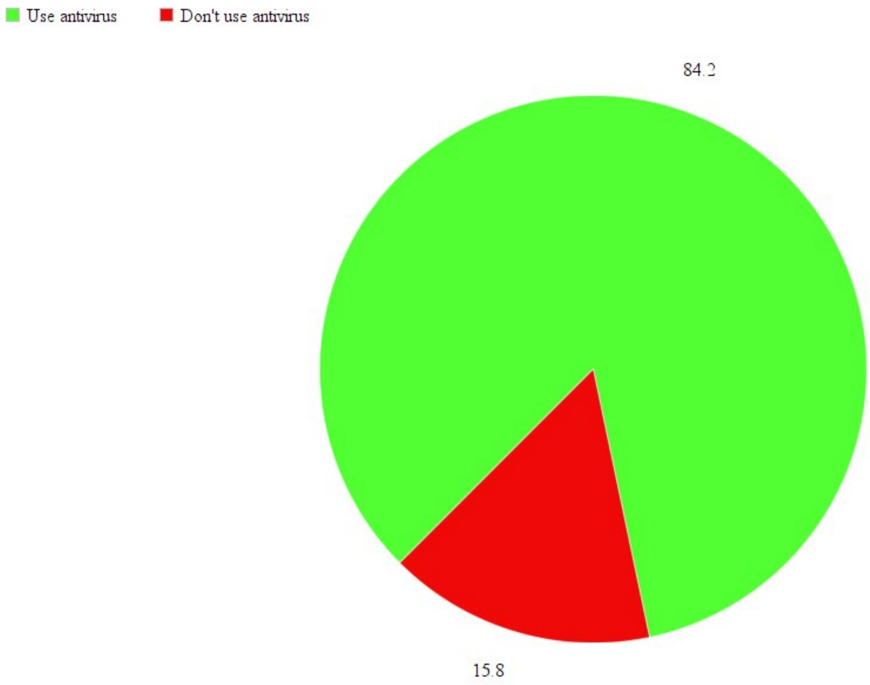
50,5% of respondents named social media as a main source of information on cybersecurity issues (37,5 – educational institutions, 18,9 – friends, 14,7 – parents).



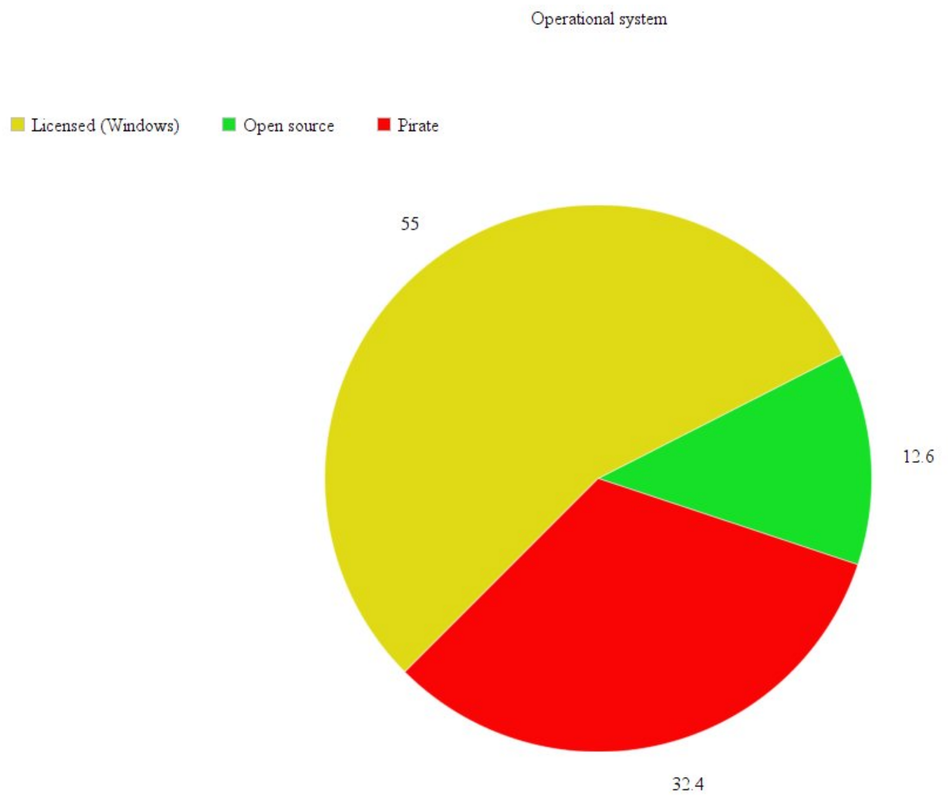
54,7% of respondents admit that they need more skills, knowledge and tools for cybersecurity, but 62% of them do not know where to get it.



84,2% of respondents use antivirus (360 Total Security, NOD, Avast mainly, in individual cases - Bitdefender, Avira, Dr.Web, Kaspersky, Zillya).



55,8% use licensed OS (Windows), 12,6% - open code OS.



36,6% of respondents think, that the dominant role in cybersecurity in Ukraine has to be played by government, 28,4% - by all stakeholders together. 47,3% think that youth has to play more active role in cybersecurity, 36,8% consider youth as the most active segment in cybersecurity, 24,2% consider youth as the most vulnerable segment of Ukrainian society regarding cybersecurity, and 24,2% think that youth is the most active segment in creating cybersecurity threats.

3. Cybersecurity market in Ukraine.
There is no information regarding value and structure of cybersecurity market in Ukraine at all.

The most obvious segment of this market is antivirus products, market assessment of this segment in Ukraine is about $100 million. Leaders of this market segment are: 360 Total Security, ESET, Avast, Bitdefender, Avira, Zillya.

Cybersecurity audit and consulting – Deloitte, ISSP, Berezha Security.

Cybersecurity equipment – Cisco, Cognitix.

4. Consultations with cybersecurity experts.

We organized our consultation with cybersecurity experts in two rounds – at first one we have sent our questionnaire (Annex B) for experts to our colleagues from IGF-UA Steering Committee, At-Large Council at State Special Communications Service of Ukraine, members of different closed groups on Facebook.

We sent them unofficial results of our survey and asked seven questions (Annex B).

Answers to these questions below.

Which results of this survey are the most crucial from the point of view of cybersecurity of Ukrainian use?

We received 20 answers to this question. The most commonly found answer (8 respondents) is about the level of actual knowledge of Ukrainian youth about cybersecurity threats (63,5% respondents (14-20 years old) met cybersecurity threats)***. 5 respondents evaluated this level as rather high, 3 of them pointed out that 36,5% met such threats, but did not recognize them, so, they evaluate the level of Ukrainian youth regarding cyberthreats as extremely low.***

The second commonly found answer is about the role of social media (6 respondents, 2 of them stress the role of Russian social network – VKontakte, Odnoklassniki). Ukrainian governmental stakeholders have to use social media in more active (and more creative) way. Extremely difficult question is about using of Russian social networks.

Three other items received the same amount of answers – 3 for each.

They are:

- using of anti-virus;

- using of licensed or open software;

- the role of youth in cybersecurity.

The most controversial is the last one – about the role of youth.

- youth suffers the role of learned helplessness (Stesin);

- we witness the formation of layer of Ukrainian society with culture of information security (Potiy).

Two respondents pointed out the problem of pornography (which is criminal crime in Ukraine). The most illustrative comment (from Petrov) was: one respondent complained, others enjoined.

Which information is unexpected for you? Which information was predicted by you? Could you please send us links to similar surveys?

Answers to this question are extremely controversial. Unchallenged leader in both categories (expected and unexpected) is the percentage of use of Russian social networks (3 respondents marked this percentage as expendently high, 3 — as unexpendently high). The main conclusion

is that Ukrainian authorities could not convince Ukrainian youth in the danger of Russian social networks using, but at the same time a lot of Ukrainian youth learned to use VPN and other tools to avoid Internet censorship.

Two respondents called attention to high level of using of licensed or open software.

Two respondents agreed, that viruses and spam are the most actual threats, some others (in answers to another questions) pointed out, that spam is not danger (nevertheless we have new Ukrainian draft law about spam as extremely important danger).

Cyberterrorism (1%) raised a lot of questions (but not from Security Service of Ukraine).

4,2% of respondents, supposing that their computers are used for illegal bitcoin mining, was extremely fun unless information in Ukrainian media that entering web-site http://meteo.gov.ua/ (for weather prognosis) threats using of individual's computer as the tool for illegal bitcoin mining (ukrainskogo-gidromettsentra-nashli-programmu-dlya-skrytogo-mayninga-kriptovalyuty).

The role of youth in cybersecurity is also extremely controversial. Two respondents expected that majority of youth relied on governmental stakeholders, two others were surprised by the underevaluation of this role (because young people often fulfill the role of «domestic» network engineers and IT teachers for older memebers of family, and they have to create «new culture» of information society in Ukraine).

What can you recommend to all stakeholders – government, private sector, civil society, youth – to enhance the level of cybersecurity of Ukrainian youth?

100% recommendations — education, awareness raising.
There are some details in these recomendations.
For example, ideas of importance of knowing logic and rhetoric, as well as English language.

Social networks — we tried to ask governmental stakehokders about their using of Russian social networks, but did not receive any answers.

Another very popular recommendation is to secure public-private partnership (no one from experts did not mention multistakeholderism at all).

There are a lot of very specific recommendations:

- promotion of cybersecurity as future carier;
- Olimpic Games for «white hackers»;
- promotion campaign likes as antiHIV (Cisco);
- promotion campaign likes Anti LUKOIL (Tuliev, against using of Russian social networks);
- involvement of media.

Do you think we need more similar surveys? If yes, do you have any propositions for the questionnaire for youth?

From 20 respondets, answered to our questions, the only one responded with «no» - without any explanations.

We received a lot of additional questions to our survey. We are not sure that we can import all these questions into our next survey (it will be . We have to elaborate «risk model» and evaluation table of cyberthreats to Ukrainian youth.

Questions of extremely importance for us:
- personal experience;
- comparisons with other strata

How can you describe the structure of cybersecurity market of Ukraine? (Which companies are members of this market?)

- antivirus;
- audit;
- integration solutions;
- cyberaccidents investigations;
- HW vendoring;
- SW vendoring
- education;

How can you describe the structure of cybersecurity market of Ukraine? (Which companies are members of this market?)

What are the main players on this market?

Cisco, Eset, Check Point, Arbor Networks, FireEye, ArcSight, ISSP, CyS-Centrum. Active Audit Agency.

Another answer (Rvachov):
1) operators: "Volya”, "Vodafone", "KyivStar";
2) vendors: "Rozetka", "АЛЛО", "Foxtrot", "Comfy";
3) software producer "Microsoft";
4) social media owners: "Facebook" та "Вконтакте";
5) e-commerce web-site olx.ua

Cisco, IBM, IT-Integrator, ISSP, ESET, Check Point, Symantec, Berezha Security, CYS Centrum, Infosafe, IT Integrator, IT Specialist, ISSP, Netwave, SOC Prime, Smartnet, Svit IT

What is your evaluation of cybersecurity market volume?

From $100 mln to unlmtd

Based on answers to this survey, we contacted main representatives of all stakeholders with more detailed questions (in process).

Preliminary results of this consultation

The most unexpected for us – there were no such polls at all! Only two respondents (from 30+ - we are still receiving answers) sent us links to surveys (regarding cybersecurity risks for companies and about Internet dependence of youth).

The most crucial for us – there is no model of cybersecurity risks for Ukrainian youth (that is why it is impossible to evaluate any threat to cybersecurity of Ukrainian youth and to pick up 3-5 of the most dangerous ones). For example – what threats are related to the continuation of using of Russian social networks and to leaving them without deleting them?

The most unanimous results:

- We need more such surveys;
- We need cybersecurity lessons in schools and even in kindergardens;
- We need more active participation of key cybersecurity actors in social networks.

Terminology:
- what are we talking about at all? (cybersecurity, informational security);
- child abuse in Ukrainian translation;
- OS and gadgets (licensed, open code and pirate)

Cybersecurity threats:
- it is extremely good that 63,5% recognized any cybersecurity threats;
- it is extremely bad that 36,5% did not recognize any cybersecurity threats

5. Recommendations:

- All-Ukrainian poll (based on recommendations from social scientists);
- cybersecurity as a part of educational program at school;
- more active use of social networks regarding cybersecurity issues;
- open and transparent discussion of cybersecurity of Ukrainian youth with the participation of all key representatives of all stakeholders

Annex A.

The text of questionnaire for youth focus groups:

1.1. How can you evaluate your own level of literacy in cybersecurity:

0 – the lowest level; 5 – the highest level:
0
1
2
3
4
5

1.2. What is the main source of your knowledge and skills in cybersecurity:

- parents
- school (college, university)
- workspace
- friends
- social networks
- traditional media (TV, newspapers, radio)
- Ukrainian governmental structures (please specify)
- private entities (please specify)
- international resources (please specify)
- other (please specify)

1.3. Did you ever meet personally any cybersecurity threats?

- Yes (please specify)
    - fishing
    - hacking
    - scam
    - spam
    - virus
    - financial theft
    - personal data theft
    - password theft
    - child abused
    - child grooming
    - bulling
    - cyber terrorism
    - DDoS attack
    - using computer as a part of botnet
    - using computer for bitcoin mining
    - piracy
    - what are you talking about at all?
    - other (please specify)
- No

1.3.1. If yes, did it harm you?
- yes

- in money (if yes, please specify how much);
    - in other aspects (please specify)
- no harm (I do not see any harm)

1.3.2. If yes, did you ask for help?

- police/cyberpolice (please specify)
- Service of Security (SBU)
- CERT-UA
- national hot-line (please specify)
- international hot-line (please specify)
- parents
- teachers
- friends
- bank(s)
- ISP
- mobile service provider
- private cybersecurity companies
- social media
- on-line educational tips
- other (please specify)
- I did not ask for help

1.3.c.1.

If you asked for help, did you receive it?

- yes (please specify)
- no (please specify)

1.4. Do you use antivirus?

- yes (please specify)
- no

1.5. What soft do you use?

- open code/source (please specify)
- licensed soft (please specify):
    - licensed version (please specify how you received it)
    - pirate version

1.6. Did you ever have account in Vkontakte, Odnoklassniki, mail.ru?

1.6.1. If yes, do you use them now?
- yes
- no

1.6.2. If you do not use this (these) account(s) now, did you delete it (them)?

- yes
- no

1.6.2.a. If you deleted it (them), when you did it:

- before 16 May 2017 (Decree of Ukrainian President regarding blocking of these platforms);
- after 17 May (entering into force of this Decree) – please specify did you use VPN or not

1.7. Do you need any additional tools to enhance your personal level of cybersecurity knowledge and skills?

- yes
- no

1.7.1. If yes, do you know how to do it?

- yes (please specify)
- no

1.8. What is your evaluation of the level of cybersecurity knowledge and skills of Ukrainian youth in average?

0 – the lowest level; 5 – the highest level:
0
1
2
3
4
5

1.9. What is your evaluation of the role of youth in cybersecurity:

- youth is the most vulnerable segment of Ukrainian society regarding cybersecurity;

- youth is the most active segment of Ukrainian society in cybersecurity;

- youth is the most active segment in creating cybersecurity threats;

- youth has to play more pro-active role in counteracting cybersecurity threats;

- other (please specify).

1.10. Who has to play dominant role in cybersecurity in Ukraine?

- government(s)
- private sector;
- civic society;
- all stakeholders together;
- other (please specify)

1.11. What is your age?
- under 15
- 15-25
- 25-35

- above 35

1.13. What is your stakeholder group:

- government
- private sector
- civil society
- students (schoolchildren)
- teachers
- other (please specify)

1.14. Are you interested to participate in any future surveys or events, devoted to the role of Ukrainian youth in cybersecurity?

- yes (if yes, please mark your agreement for using your contact information for sending you results of this survey, future surveys, invitations for future events by clicking on this option and provide your personal e-mail)
- no

Annex B. Questions for cybersecurity experts.

1. Which results of this survey are the most crucial from the point of view of cybersecurity of Ukrainian use?

2. Which information is unexpected for you? Which information was predicted by you? Could you please send us links to similar surveys?

3. What can you recommend to all stakeholders – government, private sector, civil society, youth – to enhance the level of cybersecurity of Ukrainian youth?

4. Do you think we need more similar surveys? If yes, do you have any propositions for the questionnaire for youth?

5. How can you describe the structure of cybersecurity market of Ukraine? (Which companies are members of this market?)

6. What are the main players on this market?

7. What is your evaluation of cybersecurity market volume?