ROADMAP – CYBER SECURITY IN UKRAINE

ROOT LEVEL RESOURCES

One of the most important tasks of the Ukrainian government is presented with is to ensure network security of the country since the welfare of the nation depends on the security of its information. In practice, this involves the development and implementation of advanced prevention measures, where electronic computing machines are concerned (referred to simply as "Computers"), as well as automated systems, computer networks or telecommunication networks.

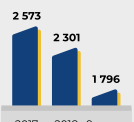
Ukraine's socio-economic problems mean that the country continues to lag behind many EU member states when it comes to the development of cybercrime prevention measures. Cyber warfare, cyber terrorism, cyber espionage have become commonplace. Crime in the information sphere now poses a serious national security threat.

To date, official government statistics can be found in:

The criminal offenses outlined in Section XVI of the Criminal Code of Ukraine (referred to as the "Criminal Code of Ukraine" from now on), can be best understood in the context of the reports of the Prosecutor General's Office of Ukraine.

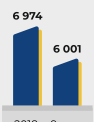
In addition to the criminal offenses described in Section XVI of the Criminal Code of Ukraine, the reports of the National Police of Ukraine contain information about other types of crimes associated with the use of the Computers.

According to the data of the Prosecutor General's Office of Ukraine, the rate of registered criminal offenses under the Section XVI of the Criminal Code of Ukraine for the recent years is as follows:



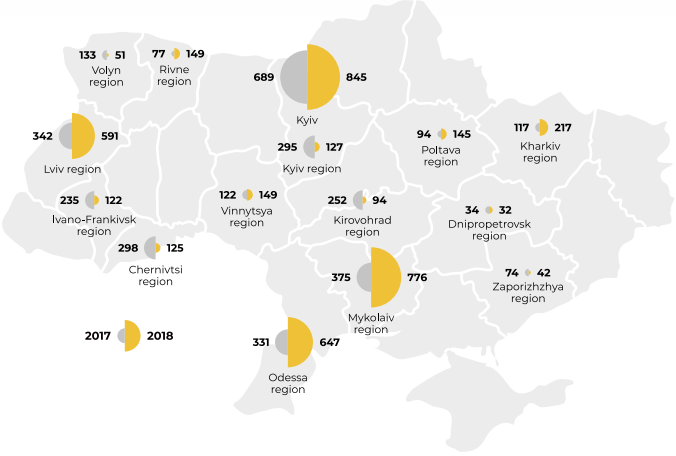
Article of the Criminal Code of Ukraine	2017	2018	9 mon. of 2019
361 – Unauthorized interference with the functionality of electronic computing machines (computers), automated systems, computer networks or telecommunication networks	1 795	1 023	1 014
361¹ – Unauthorized activities involving the use, dissemination and distribution of harmful software or hardware	35	134	165
361² – Unauthorized dissemination and distribution of information clarified as restricted-access information, and storage of such information on the electronic computing machines (computers), automated systems, computer networks or information carrying medium	64	52	33
362 – Unauthorized actions involving information which is being processed in the electronic computing machines (computers), automated systems, computer networks or information being saved on an information-carrying medium, committed by any person not entitled to access to such information	670	1 070	576
363 – Violation of operating rules of electronic computing machines (computers), automated systems, computer networks or telecommunications networks and violation of the rules governing the protection of information which is processed with the help of these computers	6	12	4
363¹ – Hindering the normal functioning of electronic computing machines (computers), automated systems, computer networks or telecommunication networks by means of mass distribution of electronic messages	3	10	4
Committed by women:	24	84	39

As reported by the Department of Cyber Police of Ukraine, the number of registered criminal offences committed with the use high information technology is as follows:



Article of the Criminal Code of Ukraine	2018	9 mon. of 2019
176 – Violation of Copyright and Relevant Rights	29	59
185 – Burglary.	860	767
Part 3,4 Art. 190 – Fraud.	2 798	1 598
200 – Illegal actions in respect of remittance documents, payment cards and other means of access to bank accounts, and equipment for their production.	311	364
229 – Illegal use of a trademark, registered trade name, any other indication of origin.	10	24
231 – Illegal collection with the intent of use or use of information that constitutes bank or trade secrets.	58	218
part 3, 4 and 5 Art. 301 – Import, production, sale or distribution of pornographic items.	463	597
361 – Unauthorized interference with the work of electronic computing machines (computers), automated systems, computer networks or telecommunication networks.	1 618	1 108
361¹ – Creation for the purpose of use, dissemination and distribution of harmful software or hardware.	28	142
361² – Unauthorized dissemination and distribution of information with restricted access, which is stored in the electronic computing machines (computers), automated systems, computer networks or information-carrying medium.	57	49
362 – Unauthorized actions with information, which is processed in the electronic computing machines (computers), automated systems, computer networks or saved on the information carrying medium, committed by a person not entitled to access such information.	729	1 049
363 – Violation of operating rules of electronic computing machines (computers), automated systems, computer networks or telecommunications networks and the rules governing the protection of information which is processed with the help of these computers.	11	15
363¹ – Impeding the normal functions of electronic computing machines (computers), automated systems, computer networks or telecommunication networks by mean of mass distribution of electronic messages.	2	11

The roadmap of Ukraine by the number of criminal offenses committed using information technology looks as follows:

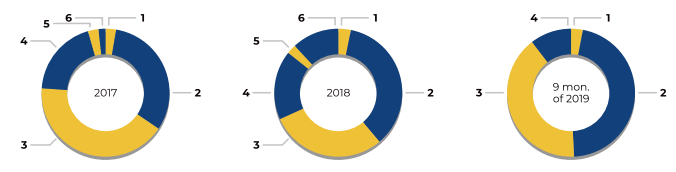


Perpetrators of Cybercrime. Who Should We Fear?

ROOT LEVEL RESOURCES

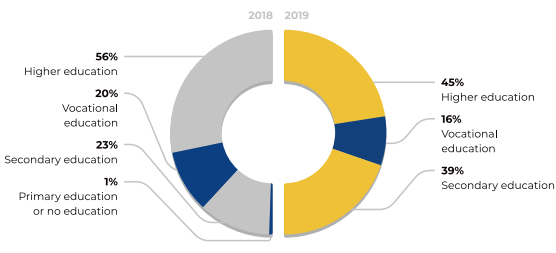
According to the General Prosecutor's Office of Ukraine and the Department of Cyber Police of Ukraine: 99.9% of crimes involving computers, automated systems, computer networks or telecommunication networks are committed by the citizens of Ukraine.

Age pattern of the computer crimes:



Computer crime rate based on the education of criminals:

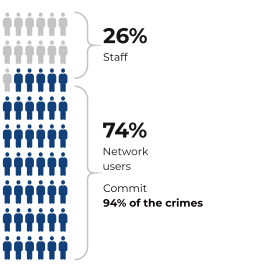
ROOT LEVEL RESOURCES



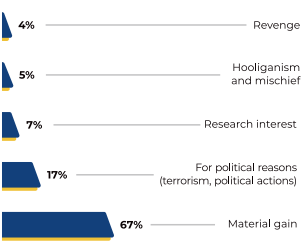
The crimes in the field of computers, automated systems, computer networks or telecommunication networks are committed by a diverse range of professionals: commercial directors, bank employees, financiers, programmers, computer equipment engineers, installers, accountants, etc.

Experts find that top management commit 26% of crimes in the field of computers, automated systems, computer networks or telecommunication networks. So senior managers and high-level specialists who have sufficient computer training and professional knowledge, as a rule, have access to a wide range of information and can give orders. As a result, they may not be directly responsible for interference with computer systems.

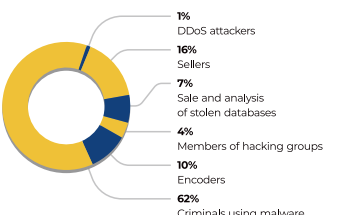
Interviews with representatives of security services organizations reveal they identify the following categories of crime perpetrators in the field of computers, automated systems, computer networks or telecommunication networks:



The motives for committing crimes in the field of computers, automated systems, computer networks or telecommunication networks are:



The Department of Cyber Police of Ukraine distinguishes the following types of crimes in the field of computer use, automated systems, computer networks or telecommunication networks:



What is at stake?

ROOT LEVEL RESOURCES

The key elements requiring network security in Ukraine are:

Communication systems that are employed to address public needs and/or used in the fields of electronic management, electronic public services, electronic commerce, electronic document management.

Communication systems that are used to meet public needs and/or the creation of legal relations in the field of electronic management, electronic public services, electronic commerce, electronic document management.

Critical information infrastructure elements.

The main types of crimes in the field of computers, automated systems, computer networks or telecommunication networks in Ukraine are:

Payment systems

1. Skimming (shimming) – illegal recording of bank account data by skim devices.

2. Cash trapping – a type of ATM fraud by way of installing s special device on ATM.

3. Carding - illegal financial transactions using payment cards or their details that are not initiated or approved by its owner.

4. Unauthorized debit orders from bank accounts using remote banking systems.

Intellectual property

1. Piracy is the illegal distribution of Intellectual Property on the Internet.

2. Card sharing is the provision of illegal access to satellite and cable TV.

E-commerce and business

1. Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords to electronic wallets, online auction services, money transfer or currency exchange

2. Internet fraud is the seizure of funds of the individuals through online auctions, online stores, websites and telecommunication facilities

Information security

1. Social engineering - technology for manipulating people in the Internet

2. Malware is the creation and distribution of viruses and malware

3. Illegal content is a content that promotes extremism, terrorism, drug addiction, pornography, a cult of cruelty and violence

4. Refiling is illegal substitution of telephone traffic.

Potential policyholders in Ukraine:

ROOT LEVEL RESOURCES

Potentially, everyone can become a victim of cyber-attacks from the public sector company to online stores and media companies' websites. However, cybercriminals are particularly interested in:

1. **Financial institutions, in particular banks, that widely use information technology.** Unauthorized interventions in the operation of Internet-Client-Bank and Internet banking systems, theft of data from bank accounts and payment cards of clients is the result of a large number of crimes in the financial sphere. According to the National Bank of Ukraine, in 2018 there were 777.6 thousand cases of fraud with bank cards, which led to the loss of 163.7 million UAH.
2. **Subsidiaries with foreign investments.**
3. **Enterprises associated with financial flows and large amounts of personal data (GDPR)**
4. **Companies that cooperate with partners from the European Union.**

The development of a domestic cyber insurance market requires the following: improved mechanism of innovation activity management of insurance companies, accounting for the influence of endogenous and exogenous factors, combination of state and private support tools with the goal of diversifying insurance products.

The main problems are as follows: state regulation of such insurance markets, flaws in the current regulatory framework, the lack of consistent legal standards and lack of state financial support. The main bodies regulating the insurance market in Ukraine are the National Commission, which regulates the financial services market, the State Financial Monitoring Service of Ukraine, and the State Audit Service of Ukraine.

Cyber insurance market development requires close cooperation between insurance companies and the Department of Cyber Police, as well as the National Commission, which is responsible for the enforcement of state regulations in the field of communications and information. Joint efforts should be aimed at monitoring cyber threats and combating cybercrime. Cooperation within the national and international insurance sectors is also crucial for the continued development of cyber insurance expertise and best practices.

Types of Cyber Risks and Cyber Insurance in Ukraine:

ROOT LEVEL RESOURCES

Types of Cyber Risks	Type of cyber insurance risks
The risk of information loss and system malfunction as a result of password cracking or a DDoS attack.	It refers to the risk of information loss and disruption of computer systems. Cyber insurance indemnifies for the protection of information technology, such as a website.
Risk of financial losses as a result of disruptions of computer systems.	It refers to the risk of lost profits in offline insurance. Cyber insurance protects IT companies from losses due to cybercrime in the case of a malfunction in the computer systems. This type of insurance is suitable for the protection of online stores, cinemas, torrent systems.
The risk of financial losses from recourse claims in the cases of theft, disclosure or use of personal information.	It refers to the risk of losses from recourse claims to the data owner in the cases of theft, disclosure and use of personal information by cybercriminals. This type of insurance reimburses the losses of a company affected by recourse claims filed by the owner of personal information.
The risk of financial losses as a result of extortion, due to a virus-related blocking of the system.	This has to do with cyber-extortion or coercion to pay for the unblocking of information or data systems when computer programmes or databases are infected by a virus. Cyber insurance covers costs associated with the unblocking of information systems.
The risk of financial losses associated with the recovery of software and/or data as a result of the acts committed by cybercriminals.	It is similar to property insurance and refers to the risk of financial losses due to software damage and/or data disruptions experienced as a result of the actions of cybercriminals. Cyber insurance indemnifies for the recovery of software and/or data.

Today, there are few network security providers in Ukraine. This is primarily due to the fact that it is difficult to assess security risks and set appropriate rates. In addition, citizens themselves do not fully understand what to demand from the companies to which they provide their personal data.

Cyber insurance in Ukraine should become a new type of insurance against criminal cyber risks and threats of interference with the normal operation of automated systems. As the country is in the process of digitization, they are actively introducing information technologies to all areas of public life.

Overview of the laws governing the issues of legal protection of network security in the Ukraine:

ROOT LEVEL RESOURCES

Constitution of Ukraine of 28.06.1966 №254к/96-ВР : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

Codified rules and regulations:

- Civil Code of Ukraine of 16.01.2003 №435-IV : https://zakon.rada.gov.ua/laws/show/435-15
- The Code of Ukraine on Administrative Offenses of 12/07/1984 №8073-X : https://zakon.rada.gov.ua/laws/show/80731-10 2) https://zakon.rada.gov.ua/laws/show/80732-10
- Criminal Code of Ukraine of 05.04.2001 №2341-III: https://zakon.rada.gov.ua/laws/show/2341-14
- The Labour Code of Ukraine of 10.12.1971 №322-VIII: https://zakon.rada.gov.ua/laws/show/322-08
- The Tax Code of Ukraine of 02.12.2010 №2755-VI: https://zakon.rada.gov.ua/laws/show/2755-17

Laws of Ukraine:

- The Law of Ukraine "On Copyright and Related Rights" of 23.12.1993 №3792-XII: https://zakon.rada.gov.ua/laws/show/3792-12
- The Law of Ukraine "On State Regulation of Activities in the Field of Technology Transfer" of 14.09.2006 №143-V: https://zakon.rada.gov.ua/laws/show/143-16
- The Law of Ukraine "On Ratification of the Convention on Cybercrime" of 07.09.2005 №2824-IV: https://zakon.rada.gov.ua/laws/show/2824-15
- The Law of Ukraine "On Access to Public Information" of 13.01.2011 №2939- VI: https://zakon.rada.gov.ua/laws/show/2939-17
- The Law of Ukraine "On Protection of Information in Telecommunication Systems" of 05.07.1994 №80/94-ВР: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
- The Law of Ukraine "On Access to Public Information" of 02.10.1992 №2657-XII: https://zakon.rada.gov.ua/laws/show/2657-12
- The Law of Ukraine "On the National Informatization Program" of 04.02.1998 №74/98-ВР: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80
- The Law of Ukraine "On the National Security of Ukraine" of 21.06.2018 №2469-VIII: https://zakon.rada.gov.ua/laws/show/2469-19
- The Law of Ukraine "On the Basic Principles of Ensuring the Cyber Security of Ukraine" of 05.10.2017 №2163-VIII: https://zakon.rada.gov.ua/laws/show/2163-19
- The Law of Ukraine "On Payment Systems and Money Transfers in Ukraine" of 05.04.2001 №2346-III: https://zakon.rada.gov.ua/laws/show/2346-14
- The Law of Ukraine "On Telecommunications" of 18.11.2003 №1280-IV: https://zakon.rada.gov.ua/laws/card/1280-15

Decrees of the President of Ukraine:

- "On the Information Security Doctrine of Ukraine" of 08.07.2009 №514/2009: https://www.president.gov.ua/documents/472017-21374
- "About Regulations on Procedure of Cryptographic Information Protection in Ukraine" of 22.05.1998 №505/98: https://zakon.rada.gov.ua/laws/show/505/98
- "About Regulations on the Technical Protection of Information in Ukraine" of 27.09.1999 №1229/99: https://zakon.rada.gov.ua/laws/show/1229/99
- "On the Cyber Security Strategy of Ukraine» of 15.03.2016 №96/2016: https://zakon5.rada.gov.ua/laws/show/96/2016
- "On the National Security Strategy of Ukraine" of 26.05.2015 №287/2015: https://zakon.rada.gov.ua/laws/show/287/2015