Cybercrime as a threat for critical infrastructure protection

Vladimir Golubev
Candidate of Legal Sciences
Director of Cybercrime Prevention Department
"Cyber Safety Unit", "Noosphere Ventures" Corporation
E-mail: vladimir@crime-research.org

Sergii Kavun
Kharkiv Institute of Banking of the University of Banking of the National Bank of Ukraine, Department of Information Technologies,
Victory Av., 55, 61174, Kharkiv, Ukraine, Tel: +38067 709-55-77;
E-mail: kavserg@gmail.com

Olexandr Trydid
Kharkiv Institute of Banking of the University of Banking
of the National Bank of Ukraine, Director,
Victory Av., 55, 61174, Kharkiv, Ukraine, Tel: +38057-337-99-96;
E-mail: khibs@khibs.edu.ua

Abstract

The article discloses the problems of an Internet-crime (cybercrime) prevention that is a purpose of this article. As one of an approach for presenting of these some results is a show of currency and further events and actions, which can create a discuss for next considerations in this area. At one point, the Internet enabled to commit previous traditional offences more effectively with no punishment. At another point, it produced new, recently unknown types of social assaults, complex and system of which reflected in such negative social phenomenon as Internet-crime. Under new fast changing country (on example of Ukrainian) realities it becomes necessary systematically and successively to study Internet-crime overall and most popular types and to develop effective measures or approaches to combat and prevent crimes in the global network. As a second approach, which the authors were wanted to show some time-frequency distributions of the main definitions in this research area, which are characterize the modern tendencies and their popularity for critical infrastructure protection in throughout world. As a result of this presentation can be more deep understanding of a situation in similar areas.

Keywords: cybercrimes, computer crimes, Internet-crimes, Cyber-criminals, Cyber Security

1 Introduction

Internet cyber criminals keep perfecting their fraud methods, leading to material losses up to tens of billion dollars and posing serious risks to many countries, including Ukraine. Therefore, specialized departments and structures are created to combat this type of crime. They constantly get more and more powers and better technical facilities. One of the recent examples is European center of Cybercrime Prevention that commenced its work in the beginning of 2013.

On March 19, Europol released a report "The EU Serious and Organized Crime Threat Assessment (SOCTA 2013) with an assessment of the growing globalized and organized crime rates by means of the Internet (Official site of Europol, 2013).

Unfortunately, Ukraine has ranked the fourth (following Russia, Taiwan, and Germany) among the world countries presenting the highest cyber threats. This data was shown on the map of countries – cyber-attacks sources, visualized in the report of Deutsche Telekom, a leading German operator.

2 Time-frequency analysis for some definitions of the critical infrastructure protection

It should been mentioned that in nowadays we can see a strengthening of a popularization for some definitions or key aspects in this area (Kavun, 2009), for example, it covers the following definitions – Cybercrimes, Computer Crimes, Internet-crimes, Cyber-criminals, Cyber Security, etc. For those and some other similar definitions, the authors have carried out a research for all these definitions about their distribution on time line (2000-2013). This research is based on the method of Internet-analysis (Kavun, Mykhalchuk, Kalashnykova, Zyma, 2012). At the same, this distribution was based on their popularization or demand; also, it can called as time-frequency analysis. Some results with their normalizing of this research (for better presentation) were shown in Table 1. All of these submitted data has been normalized for better visualization and to receive a possibility of comparing those results between themselves.

As we can see from Fig. 1, which is showing very clearly and graphically, more popularity of these definitions was since 2006. In addition, only for the definition "Cyber-crime detection (CCD)", we can look a big growth since 2000 over 2004. For remaining definitions, we can see some field of "activity" since 2006, especially it concerns for the following definitions: "cyber analysis" in 2008 is received big growth, but after two years this area is has become not interesting for the most specialists; "Computer crime" is the area, which had a variable success in 2006 and 2010; also as "Internet crime" has a variable success only in 2009 and 2012. For the others definitions, which was studied in author's research, we can see a quite variable interest (ES INFECO, 2012-2013). At the same time, this interest is confirming the fact that notwithstanding that situation these areas (based on similar definitions) are remaining in the sphere of some interests for the most specialists and professionals.

Based on those data from Table 1, we could built some graphics (map's frequency distribution and linear 3D-frequency distribution), which is shown in Fig. 1-2.

Table 1

Results of the demand distributions with their normalizing

Year / Definition	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Cybercrime (CbC)	4,85	5,48	19,81	2,82	4,92	1,93	1,53	5,45	4,48	3,12	8,15	25,90	23,47	18,20
Computer crime (CpC)	8,28	6,52	2,32	1,50	6,19	2,75	31,91	16,06	6,04	5,35	11,62	8,78	5,75	4,04
Internet crime (IC)	0,05	0,03	0,02	3,09	3,06	1,20	0,05	16,73	0,07	28,48	15,28	7,47	23,03	1,55
Cyber-criminals (CbCr)	6,26	5,62	5,10	5,51	5,89	6,34	7,12	7,65	8,81	8,96	3,75	10,46	7,50	11,02
Cyber Security (CS)	1,16	1,44	1,30	2,92	2,61	6,02	17,80	11,13	22,00	5,11	2,65	3,69	9,28	16,79
Crime analysis (CA)	0,01	7,42	0,00	2,52	2,80	1,76	5,04	4,83	40,77	19,24	9,91	3,53	8,73	0,87
Cyber-infrastructure protection (CIP)	2,23	5,50	5,41	6,10	6,08	6,81	10,42	9,46	24,27	4,45	29,62	0,31	0,24	2,23
Cyber-crime detection (CCD)	2,85	34,27	33,65	37,57	34,48	2,50	2,46	3,10	3,03	3,16	3,36	3,70	3,55	3,10

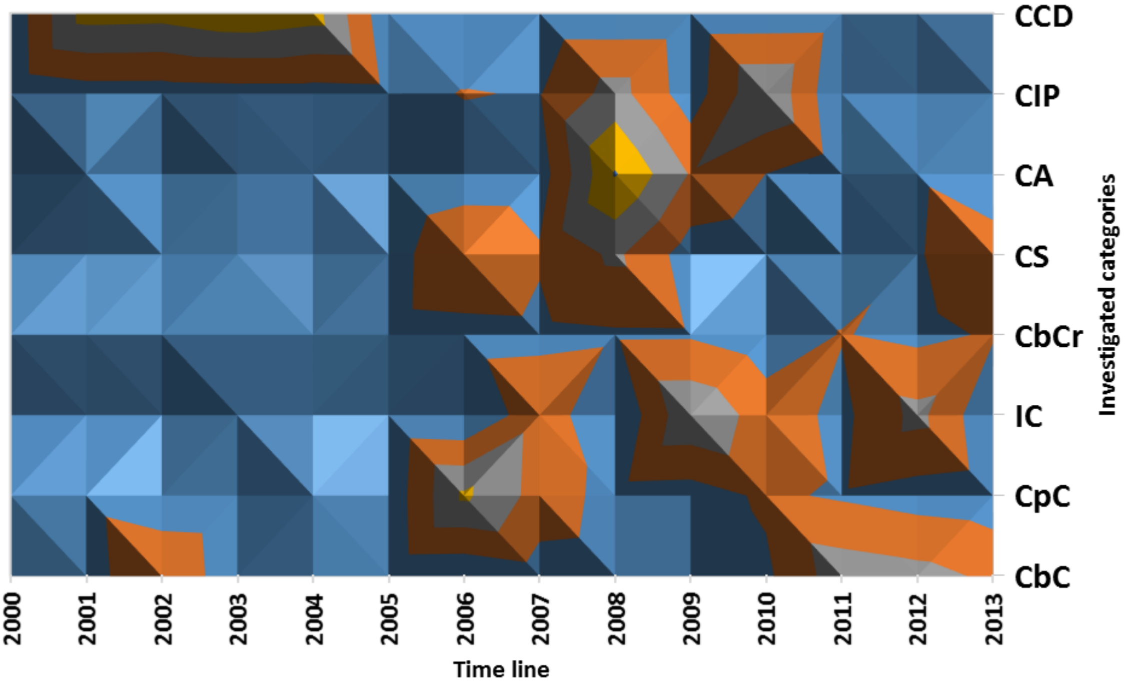
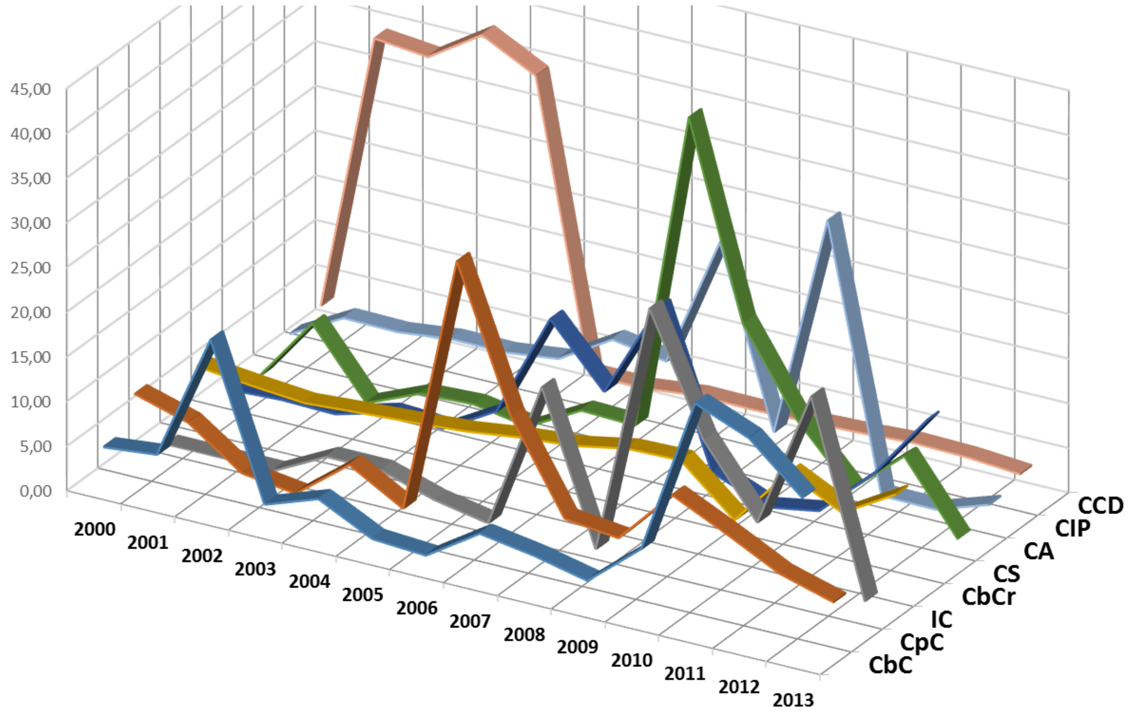


Fig. 1. Map’s frequency distribution of the definitions



Fir. 2. Linear 3D- frequency distribution of the definitions

As a continue of our research for those definitions and similar areas of security, we could built some distributions for separated definitions with forecasting on the next period of time (for next several years) based on the well-known trend models (Kavun, Sorbat, Kalashnikov, 2012). For these trend models, we also are shown their approximation functions with the accuracy of the approximation (R^2), as it is shown in Fig. 3-11.

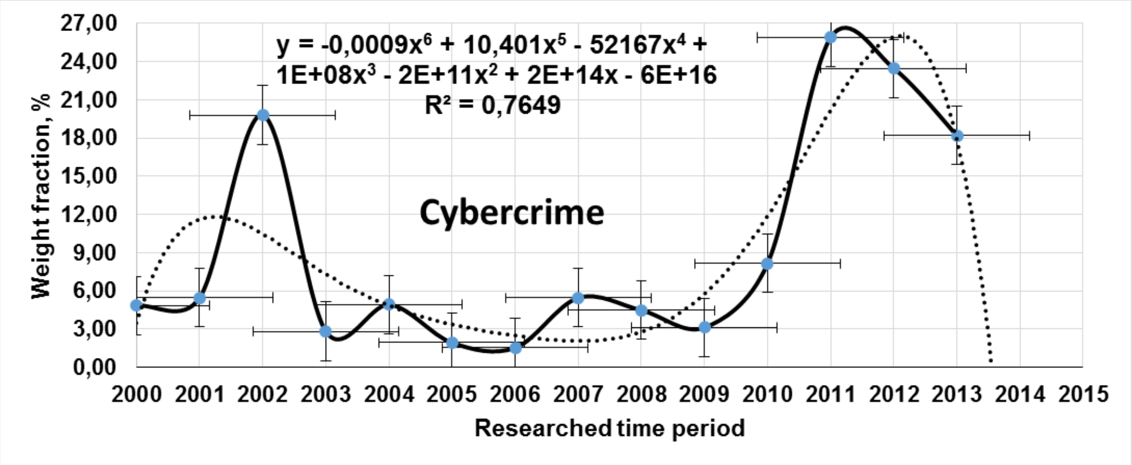


Fig. 3. Distribution graph of “popularity” or “demand” for the definition “Cybercrime” with forecasting based on a trend model (the polynomial model of 6th degree)

In Fig. 3 (also as in the next figures), the general distribution (distribution graph) is shown with help of a solid bold line and a trend line is shown with help of a dotted line. Based on the approximation function and its accuracy of the approximation (R^2, this accuracy is high enough) we can say that nowadays the popularity of cybercrime is decreasing, but it does not the fact that we have some reduction of some offenses in this area. For each point of all set of data in this Fig. 3 is shown some limits of standard accuracy (of error), which is determining an area of precision of our measuring (Kavun, 2009). In addition, you can see, in fact, this model is a model of 5th degree, because a coefficient at the variable X_6 is small enough, and is equal about 10^{-3}.

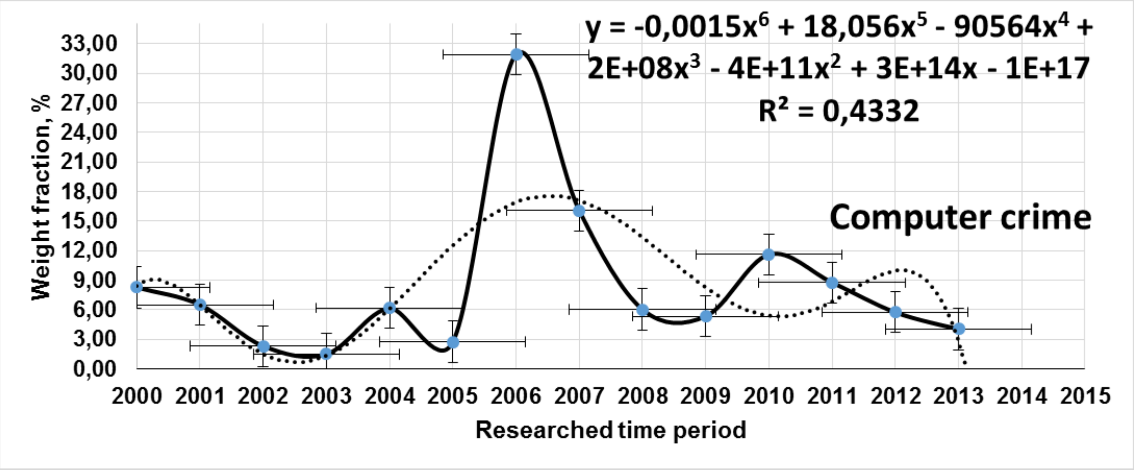


Fig. 4. Distribution graph of "popularity" or "demand" for the definition "Computer crime" with forecasting based on a trend model (the polynomial model of 6th degree)

Based on the approximation function and its accuracy of the approximation (R^2), as is shown in Fig. 4, we can say that nowadays the popularity of computer crime also is decreasing, and besides, this distribution has this reduction since 2007. Therefore, it is a good tendency and, it will be able to acknowledge about some success in a fight with computer crime of some different government and private organizations. However, we cannot trust enough of this distribution graph and its forecasting, because we have the accuracy of the approximation, which is small enough, so this forecasting we can consider only in approximate form. For the following definition "Internet crime", its distribution graph is shown in Fig. 5.

Based on the approximation function and its accuracy of the approximation (R^2), as is shown in Fig. 5, we can say the time-frequency distribution for the definition "Internet crime", in general, has a common positive linear tendency (based on common linear trend, as it show with help of long dotted line in this figure) during all researched time period, but with the enough small accuracy of the approximation (< 0,5). This fact is not confirming our forecasting for this area, so we must use this forecasting with all caution.

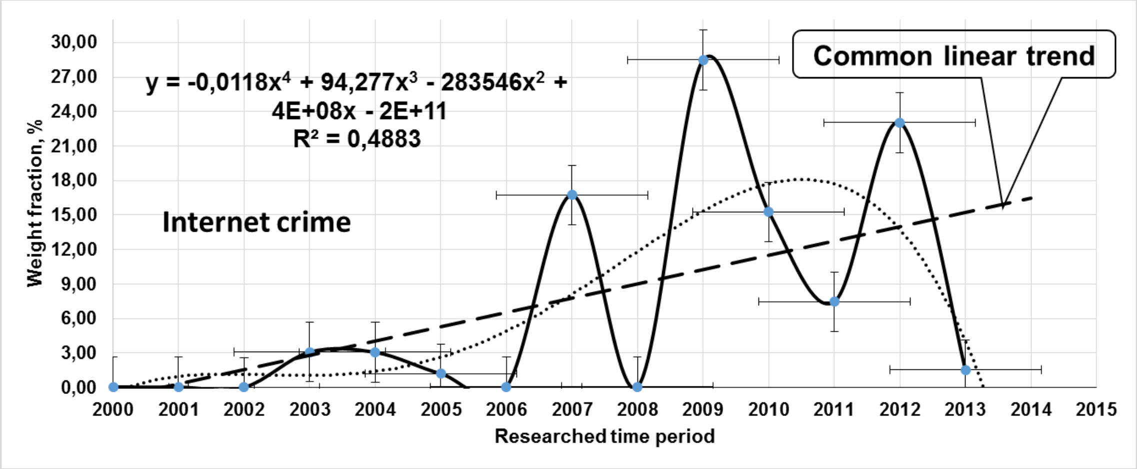


Fig. 5. Distribution graph of “popularity” or “demand” for the definition “Internet crime” with forecasting based on a trend model (the polynomial model of 4th degree)

In additional, we could be reduced a degree of this polynomial trend line to 4th degree in comparing with 6th degree without significant reducing of the accuracy of the approximation, as it showing below.

$$y = -0{,}0001x^6 + 1{,}5418x^5 - 7732{,}4x^4 + 2E{+}07x^3 - 3E{+}10x^2 + 2E{+}13x - 8E{+}15$$

$$R^2 = 0{,}4893.$$

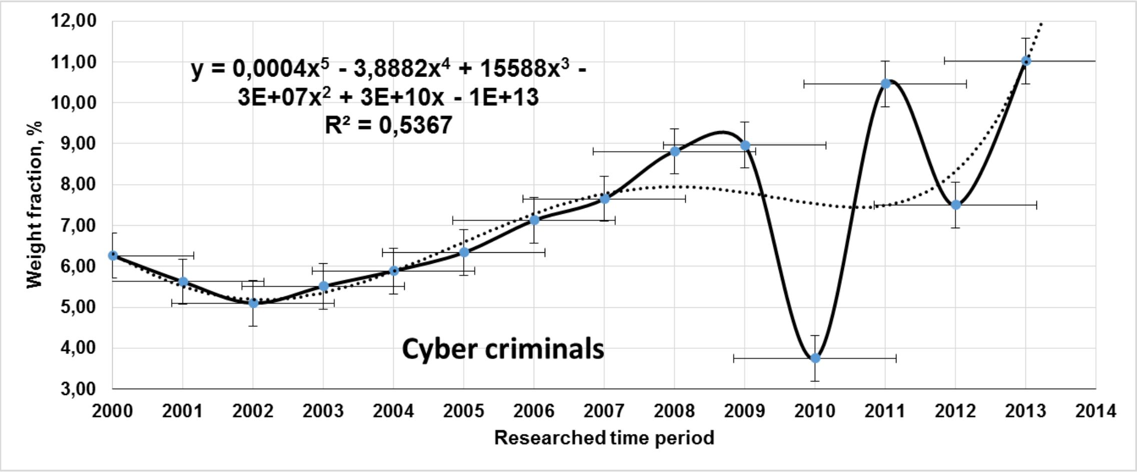


Fig. 6. Distribution graph of “popularity” or “demand” for the definition “Cyber criminals” with forecasting based on a trend model (the polynomial model of 5th degree)

Very interested distribution we can see in Fig. 6, which is presenting for the definition “Cyber criminals”. From this figure, we can see a positive (with permanent increase) trend for any kind of trend models, but with the enough small accuracy of the approximation, a little more 0,5. In addition, we can confirm that fact this distribution is sorrowful, because it is confirming a permanent increasing of different kinds of cyber criminals in throughout the world. Therefore, we must have some interest for a decreasing of this distribution, thus, this theme is actual. In fact, we could see this trend model based on the polynomial dependence has the polynomial model of 4th degree, because a coefficient at a variable X_6 is small enough (a little more 10^{-4}).

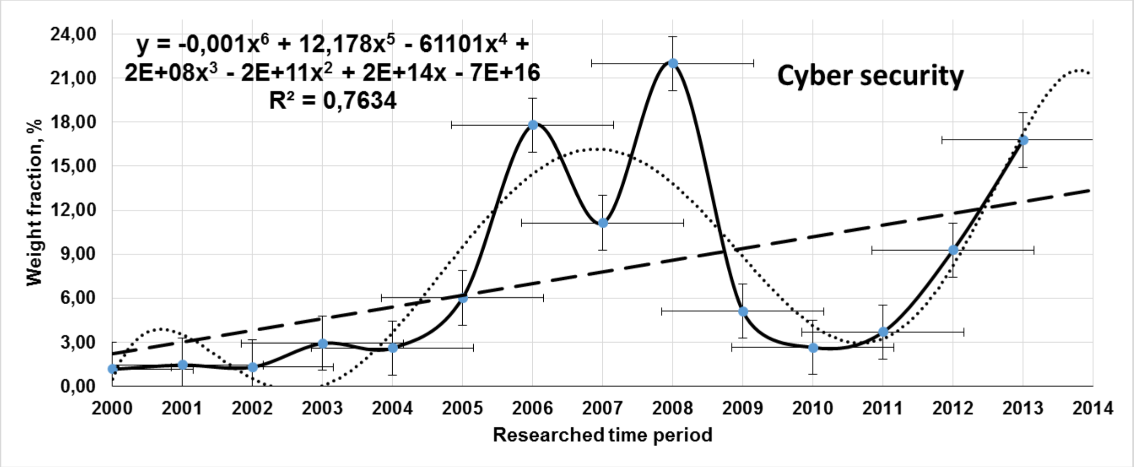


Fig. 7. Distribution graph of “popularity” or “demand” for the definition “Cyber security” with forecasting based on a trend model (the polynomial model of 6th degree)

For the confirmation of a necessity for decreasing of a growth of popularity of the area “Cyber criminals”, as opposed of this fact, we can see an increasing of a growth of popularity of the area “Cyber security”, as it is shown in Fig. 7. Moreover, this positive tendency is observed for any kind of the trend models, as for the linear, and for polynomial models. In additional, this growth is began since 2010-2011, when some well-known cyber-attacks on the different government and private infrastructures were done in throughout world. About this and other actions will describe below. The enough high accuracy of the approximation is increasing of our confidence and an independence level of forecasting, but only for determination of the general tendencies.

Based on distribution graph of the definition “Crime analysis”, which is shown in Fig. 8, we can see a significant growth of popularity for this area in 2008, but after that period of time, we also can see a significant recession up to nowadays. Moreover, we only can hope (because we have the enough small accuracy of the approximation, a little more 0,5) that in further period of time will be to rise some interest and our attention to this area. It can confirm the enough small positive tendency, which is a general tendency. The enough small confirmation of the significant growth of popularity for this area in 2008 can be some normative and legislative acts and documents (about which will be describe below), which were accepted in some EU and other countries.

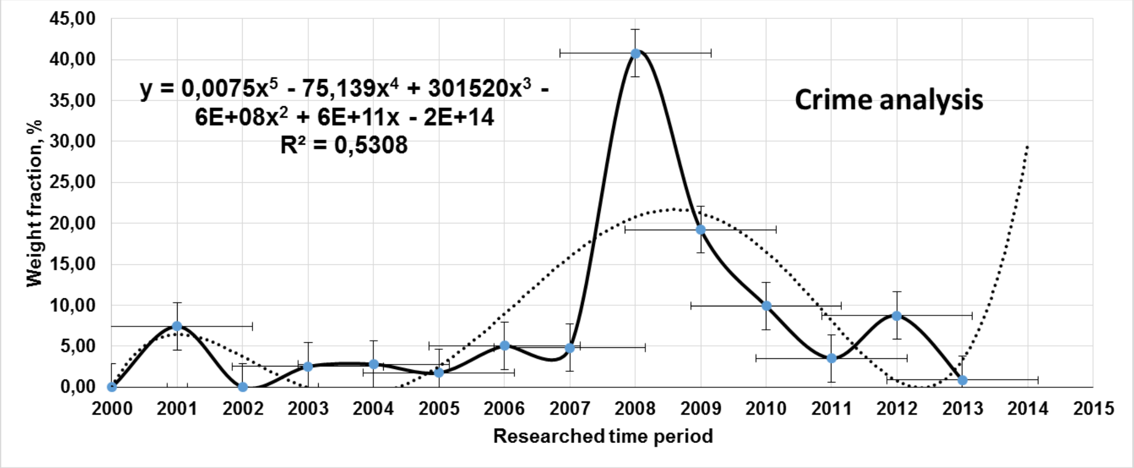


Fig. 8. Distribution graph of “popularity” or “demand” for the definition “Crime analysis” with forecasting based on a trend model (the polynomial model of 5th degree)

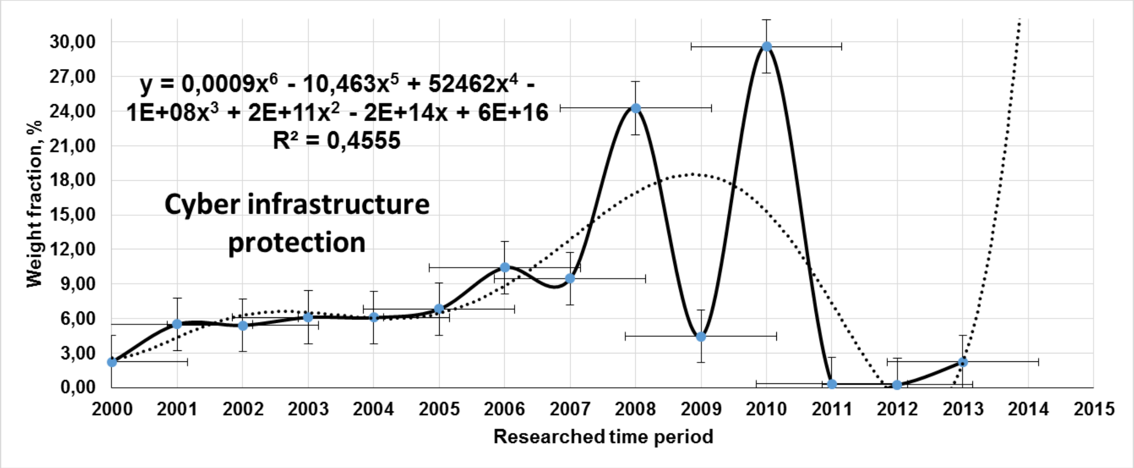


Fig. 9. Distribution graph of “popularity” or “demand” for the definition “Cyber infrastructure protection” with forecasting based on a trend model (the polynomial model of 6th degree)

For this definition “Cyber infrastructure protection”, we can say only about some tendencies, because we have the enough small accuracy of the approximation (a little less 0,5). Based on the general tendency we can see an enough small positive trend before 2010, but after 2011, we have a recession. It is also confirm some recession of an interest in this area, but we can hope after 2012 (it can see in Fig. 9) this interest and popularity will be have more growth, in compare with past actions.

In Fig. 10, we can see an enough interest distribution for the definition “Cyber-crime detection”, which somewhat similar to the Poisson distribution (with $\lambda = 4$). In addition, we can see some stabilization during period of time 2005-2013, i.e. some values of time-frequency distribution are equal between themselves.

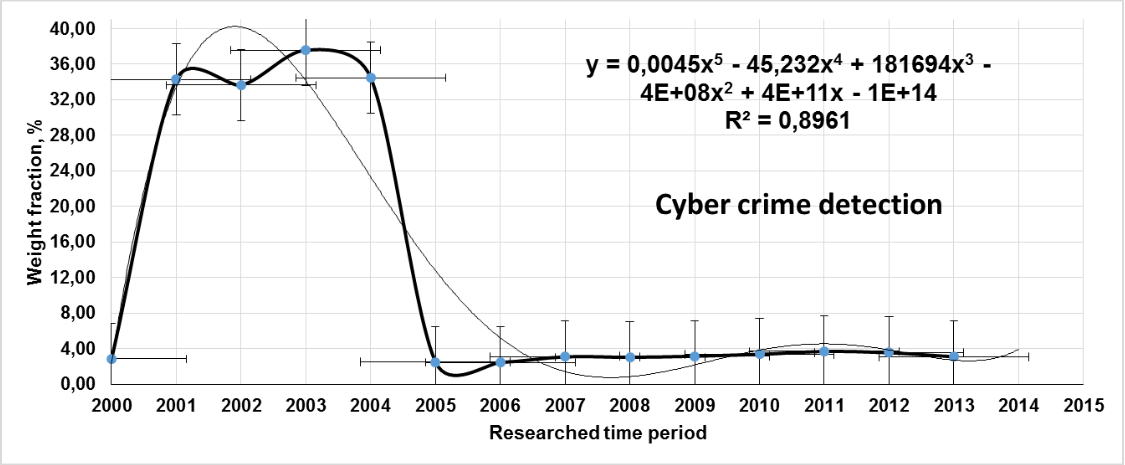


Fig. 10. Distribution graph of “popularity” or “demand” for the definition “Cyber-crime detection” with forecasting based on a trend model (the polynomial model of 5th degree)

It confirms that fact, in the beginning of the 2000s this theme or area was very interesting and popular. Besides, we can say with some confidence that the popularity and interest in this area will have quite stability in the next period, this assessment based on the enough high accuracy of the approximation (almost equal 0,9).

Thus, we can describe the common tendencies in this and other areas based on using of developed by one from authors method of Internet-analysis ().The method of Internet-analysis developed by the authors can be applied in any given area of activity, regardless of its properties and features. The purpose of using this method is to get some assessment or collection of selected concepts (terms), which form the so-called categorical apparatus of scientific research. According to estimates, authors can formulate a conclusion about the need for further research in this area, show the urgency and demonstrated the importance of the calculations, to allocate a narrow major for further research of young scientists. The proposed method can be used to study the activities of prominent scientists, professionals from designated areas of activity. Secondly, this method can be used for demonstrating the importance and the relevance of research, and the conclusions and recommendations drawn, for example, to select consultants (leaders) in their scientific activities.

For a more complete openness, authors will show the possibilities of the research conducted by the authors on the example of the work of scientists in the field of information and economic security, which was selected because of its global relevance. Using a method based on the specifics of the query language that is supported by all search engines and the shape of the query, the results on the set of selected search engines are averaged at a given time interval. Thereby, the dynamism of the study is achieved. The authors showed as an example of some limited areas of interest an interpretation of the developed method with the help of graph theory to be able to use known techniques of optimization and further analysis (Kavun and Mikhalchuk, 2009). Thus, the scope of the developed method of Internet-analysis is multi-faceted in its specificity and tolerance in limited areas of interest (Kavun, 2011).

3 Statistical and financial data in area of legislations (on example of Ukraine)

As a response to the difficult criminal situation in the Internet-area, Ministry of International Affairs of Ukraine has prepared a draft law “On cyber safety of Ukraine”, handling hacker attacks of government websites and promotion of pornography, violence and separatism as a threat to national security (Site of Security Service if Ukraine, 2003).

The crime connected with the use of computer technologies presents a broader problem, which is at first conditioned by the time, precisely by the people’s ability to engage electronics and computer technologies.

Just as there was a period of transport development and implementation into the everyday life, which required the protection of the process participants, similar period we face nowadays. If upon introduction of computer technologies there was no strictly regulating legal framework as a man had not then imagined where his invention would find its implementation, and therefore there was no defined circle of the process participants and no rhetorical question of legal protection of their interests. Presently, the inventions in computer technologies affect and involve more and more participants. Hence, the necessity of detailed and thorough regulation of this area of human achievements follows (Donetsk, 2008).

Since the beginning of 2013, a department of cybercrime prevention of the Ministry of International Affairs has detected 23 cases of illegal debiting from accounts of commercial enterprises amounting to 12.5 billion UAH, 9.2 billion UAH of which were successfully recovered. Financial frauds are gradually moving from open market to global network. The number of fraudulent payment cards, which could be accessed by criminals in the trading centers, is reducing in Ukraine. At the same time the crime rate, related to the Internet and “Client-bank” system, has boosted, and this trend continues.

It should be noted now new spheres and culture prompted by the progress has appeared, the pushing force for which was a human’s laziness. The existing world of computer technologies offers great opportunities, it enables to communicate, search and save information, shop online and pay by electronic means, work and get remuneration. Thus, today a human is also able to lead a full and productive life in cyberspace (Darlington, 2013).

However, it is not just a mass computer distribution, which forms information sphere. A significant, even a key role in this process belongs to various constantly is improving computer technologies.

This way, the advancement of information technologies, growing production of supporting technical facilities and their application along with the development of electronic payment methods as a potential object of criminal offence and increasing availability of such facilities are the natural cause of upraise, existence and growth of property offence using computer technologies (Idov, 2013).

The independent poll undertaken by the Centre of cybercrime investigation among 100 people actively using the Internet for more than one year, shopping and paying online (using bankcards, e-wallets) showed the following results:

a) 87% of respondents have suffered from criminal offences involving computer technologies,

b) 2% of respondents have realized the property loss during the first hours,

c) 5% of respondents have realized the property loss during the first month,

d) 93% of respondents have realized the property loss after the first month.

Social danger of such crimes lies in their latency time, which in turn rises from the fact that the person often has no idea that he/she had become a victim of a crime. As the result the criminal feels his impunity and therefore above the society and law.

4 Aggregated classification of some definitions in the area of cyber security

Based on the authors research, was aggregated some volume of different information from more sources (Kavun and Brumnik, 2013). Therefore, we can form some aggregated classification of these similar definitions in this area for more helpful and comfortable perception. In addition, we want to present some main definitions in this area:

1. Computer crimes in a broad sense is a criminal act or some actions, which has been perfected with using and (or) with regard to computer information, computer of any kind, computer systems, and their networks.

2. Crimes in a sphere of computer information is a criminal act or some social (publicly) dangerous actions, objects (or subjects) and (or) means of which are different computer information (data).

3. Computer crimes in the narrow sense is a criminal act or some actions, objects (or subjects) of which are different computer information (data).

Based on some lists for the EU countries, which were accepted and approved as the Recommendation No. R (89)9 of the Committee of Ministers to Member States on Computer-related Crime (adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers' Deputies), we aggregated a classification in visual type, as it shown in Fig. 11.

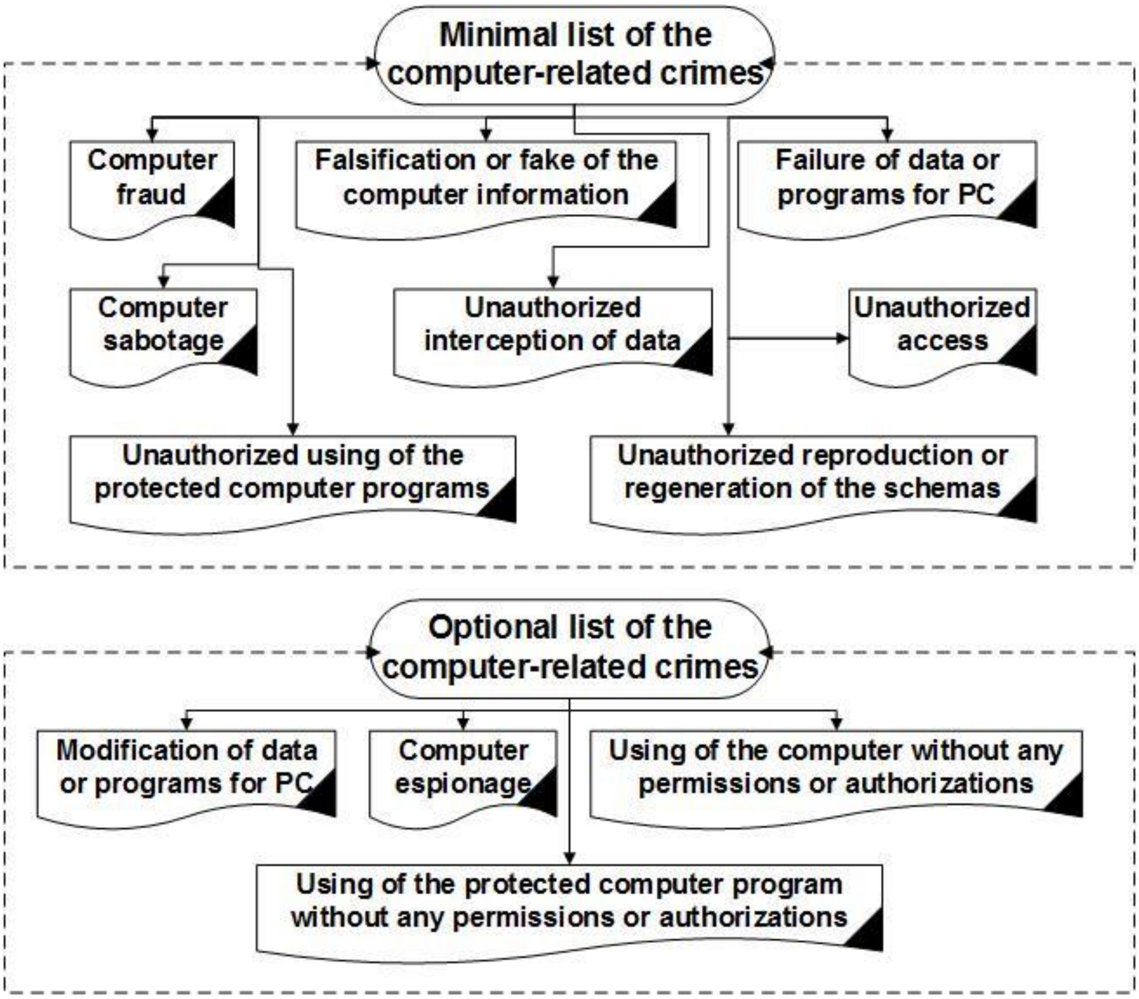

Minimal list of the computer-related crimes
Computer fraud
Falsification or fake of the computer information
Failure of data or programs for PC
Computer sabotage
Unauthorized interception of data
Unauthorized access
Unauthorized using of the protected computer programs
Unauthorized reproduction or regeneration of the schemas
Optional list of the computer-related crimes
Modification of data or programs for PC
Computer espionage
Using of the computer without any permissions or authorizations
Using of the protected computer program without any permissions or authorizations

Fig. 11. Visualized classification of the computer-related crimes

The first complete classification of the computer crimes was offered in 1983, in Paris (France) from a group of some experts of the Organization for Economic Co-operation and Development, OECD. This classification based on some interests of owners and property owners. This classification has the following differentiations:

1. **Economic and computer crimes**: computer fraud, computer and economic espionage and a theft of some programs for a computer of any kind; computer sabotage; a theft of any kind services; unauthorized entry (an access) to automated and information system(s), and the traditional economic crimes, which are doing with help a computer;

2. **Computer crimes against individual people rights and the inviolability (privacy) of the private sphere**: input to computer system(s) an incorrect and invalid data about physical or legal person (or entity); illegally collecting the right (or personal) data; illegally misuse of some information, which is presenting on some machine carriers (computer devices); illegally disclosure of some information (for example, bank secrets, medical secrets, etc.);

3. **Computer crimes against some interests of state (country) and society**: some crimes against state or public (social) safety (security); violation of some rules for a transfer of information to abroad (illegally export of information); disorganization of a work (or functioning) of defense systems; illegally misuse with automated systems for vote counting in elections and decision-making parliamentary.

In addition, we can create an aggregated classification of the all kind of computer crimes, as it shown in Fig. 12.

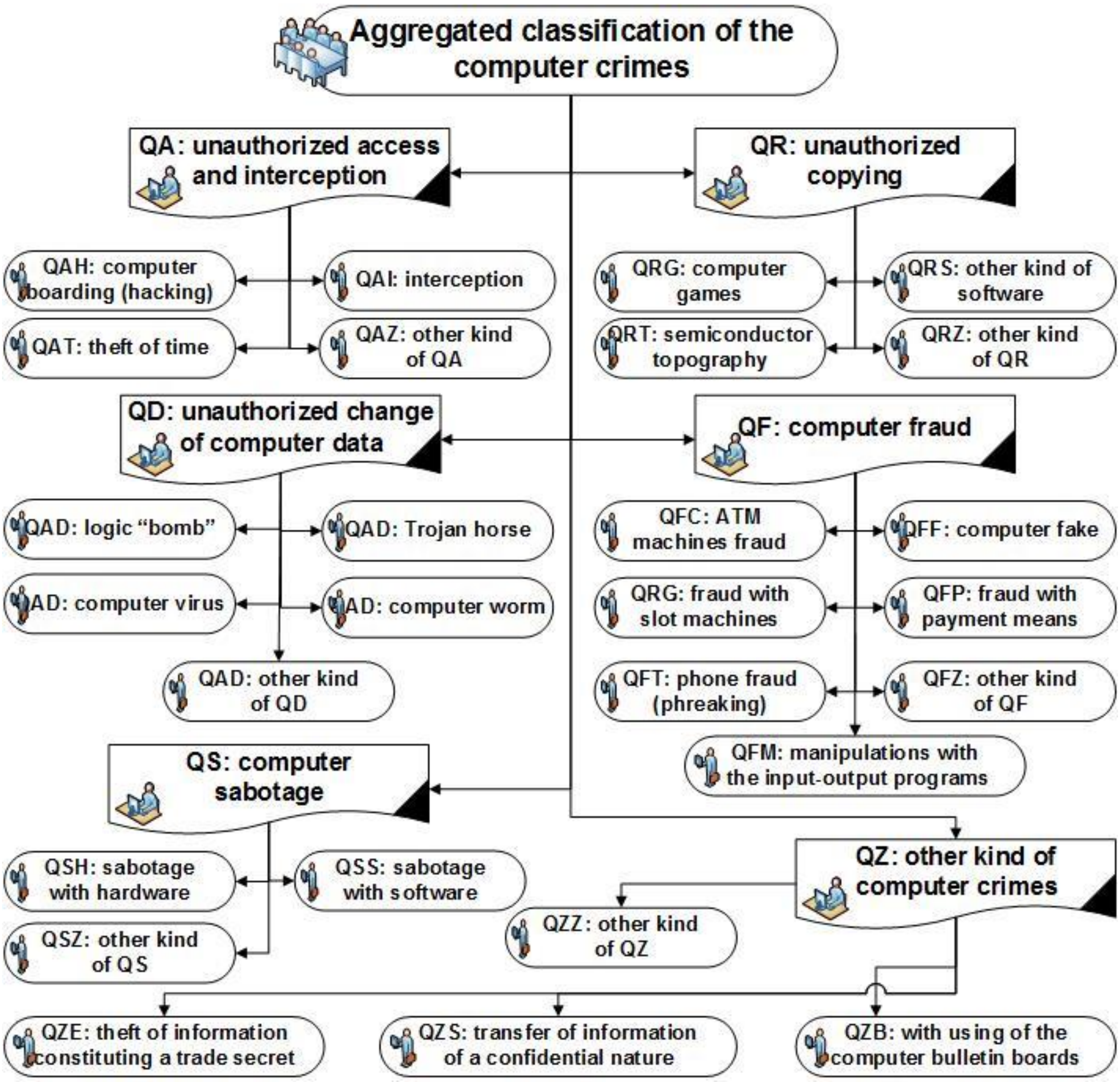

Aggregated classification of the computer crimes
QA: unauthorized access and interception
QR: unauthorized copying
QAH: computer boarding (hacking)
QAI: interception
QAT: theft of time
QAZ: other kind of QA
QRG: computer games
QRS: other kind of software
QRT: semiconductor topography
QRZ: other kind of QR
QD: unauthorized change of computer data
QF: computer fraud
QAD: logic "bomb"
QAD: Trojan horse
AD: computer virus
AD: computer worm
QAD: other kind of QD
QFC: ATM machines fraud
QFF: computer fake
QRG: fraud with slot machines
QFP: fraud with payment means
QFT: phone fraud (phreaking)
QFZ: other kind of QF
QFM: manipulations with the input-output programs
QS: computer sabotage
QZ: other kind of computer crimes
QSH: sabotage with hardware
QSS: sabotage with software
QSZ: other kind of QS
QZZ: other kind of QZ
QZE: theft of information constituting a trade secret
QZS: transfer of information of a confidential nature
QZB: with using of the computer bulletin boards

Fig. 12. Aggregated classification of any kinds of computer crimes

For well-known methods of an unauthorized access and interception of information can pick out the following basic definitions. These definitions are also relevant in other different areas, such as information security, risk management on the enterprise, cyber-infrastructure protection, etc.:

1. **Bugs** is some kind of electronic devices, which involve of the microphone setup in the computer to intercept of some conversations between service personnel.

2. **Data leakage** is a possibility for the collecting of any kind of information, which needs for receiving of main data about some technologies, which are using in the system (Linde, 1975).

3. **Scavenging** is a data search, which were of users after their working on a computer. It is dividing on the physical and electronic searching.

4. **Piggbacking** is a method, which characterized unauthorized penetration into space and electronic close zones (places).

5. "**Between the lines entry**" is a method, which based on an illegal connection to the communication link (or line) of a system user or computer network. Connection is doing in the time moment, when the user is finished its communication session, but he had not a time to disconnect from the network yet.

6. **Browsing** is a method of an unauthorized access to base data or some files of legal user, is doing based on finding of some weaknesses in the protection system or computer network. If an offender were able to find at least one weakness, then he/his will be able to use this weakness each time for further reading and analyzing of any information into system. Hi/his also can copying and using of this information for their personal purposes.

7. **Trapdoor entry** is a method of an unauthorized access, which happening during detection of some errors or mistakes in a logic of building a program. These detected errors or mistakes can using repeatedly.

8. **Trapdoor** is some development of the previous method, which differ of a fact that some special control commands are including in the detected place of program for further using for their own purposes. It also called as "program backing".

9. **Masquerading** is a method, at which the offender is penetrating into a computer system with using of necessary means pretending to be legal user.

10. **Spoofing or mystification** is a method, which is using at a random connection of an unfamiliar computer system to the system of a victim. The offender is forming some "credible" requests from the system of victims. After it, this offender can supported a delusion from that user (victim) during some period of time and received an information (confidential, secret, personal, etc.), which will be useful fir this offender.

We and some other specialists and professionals in this area are considering that this classification has one significant weakness (United Nations Crime and Justice Information Network. Centre for International Crime Prevention, 2000). It is entering for using a literal "Z", which led to a chaotic (from a point of criminalistics) mixing of criminal and law principles and the technical features of automated data processing.

Some modern classifications are including the following directions: illegal actions with a computer information; illegal actions in area of communications; illegal actions with information devices; illegal actions with other kinds of information.

Thus, as we can see in legal field has some different classifications, so you can use any kinds of these classifications based on your own purposes, tasks and personal experience.

The authors hope that these and other similar classifications (Council of Europe - Documents database, 1989) will be able to help some experts, specialists and professionals in this area for their own researches and other kinds of activity. In our opinion, these aggregated classifications can use as some fundamentals in the researches in criminal and law field.

5 Conclusion

High social danger of Internet crime mainly results from the increasing role of system of social relations, which are under its threat, and from its transnational and organized character (Chimiris, 2013). Not a single country can actively oppose this malice alone. Because of this, the intensification of international cooperation becomes of high necessity.

Under the new realities of fast Ukrainian entry to the single information space, it becomes necessary systematically and successively to counteract the cybercrime overall and most popular types, and to minimize the harm to the economy. It is important to develop effective measures of Internet crime combat and prevention, improve legal system of information security, including cyber safety.

References

1. Official site of Europol. (2013). The EU Serious and Organized Crime Threat Assessment (SOCTA 2013). Retrieved August 5, 2013, from https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf.
2. Site of Security Service if Ukraine. (2003). A draft law of Ukraine amending Law of Ukraine “On the basis of national security” on cyber safety. Retrieved August 5, 2013, from http://www.sbu.gov.ua/sbu/control/en/publish/article?art_id=89497&cat_id=42924.
3. *Problems of crime prevention in computer technologies (in Ukrainian)*. (2008). Donetsk, Ukraine.
4. Idov, R. (2013). Computer Crime Research Center. *Peculiarities of information security in Ukraine*. Retrieved August 5, 2013, from http://www.crime-research.ru/interviews/incidents22/.
5. Chimiris, M. (2013). Computer Crime Research Center. *To limit anonymity in the net does not mean to oppress liberty of speech*. Retrieved August 5, 2013, from http://www.crime-research.ru/interviews/maxim27/.
6. Darlington, Mwendabai. (2013). Zambia Daily mail. *Cyber crime: threat to economies?* Retrieved August 5, 2013, from http://www.daily-mail.co.zm/?p=5209.

7. Kavun, S. V., Mykhalchuk, I. V., Kalashnykova, N. I., Zyma, O. G. (2012). A Method of Internet-Analysis by the Tools of Graph Theory. *Intelligent Decision Technologies. Smart Innovation, Systems and Technologies*, *15* (1), 35-44.
8. International research portal (lab) of the information and economic security ES INFECO. (2013). Retrieved August 5, 2013, from http://infeco.net/infeco-overview/article/158-statistical2.html.
9. International research portal (lab) of the information and economic security ES INFECO (2012). Retrieved August 5, 2013, from http://infeco.net/test-security/statistic.html.
10. Kavun, S. V., Sorbat, I. V., Kalashnikov, V. V. (2012). Enterprise Insider Detection as an Integer Programming Problem. *Intelligent Decision Technologies. Smart Innovation, Systems and Technologies*, *16* (2), 281-289.
11. Kavun, S. (2009). *Informational security*. Kharkiv: Pub. of INZHEK.
12. Kavun, S., Mikhalchuk, I. (2009). Analysis of categorical apparatus in the field of economic and information security. *Economic of development*, *3* (51), 9-14.
13. Kavun, S. (2011). Structuring the normative and legal providing in the system of economic security of enterprise, *Foreign Trade. Economic Security*, *7*, 22-28.
14. Kavun, S., Brumnik, R. (2013). Management of corporate security: new approaches and future challenges. **E**ditorial Denis Galeta and Miran Vrsec. *Cyber security challenges for critical infrastructure protection* (pp. 141-151). Ljubljana: Institute for Corporate Security Studies. Retrieved August 5, 2013, from http://www.ics-institut.com/research/books/5.
15. Linde, Richard R. (1975). *Operating System Penetration, Proceedings*. NCC.
16. United Nations Crime and Justice Information Network. Centre for International Crime Prevention. (2000). *Documents of 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders Vienna*. Retrieved August 5, 2013, from http://www.uncjin.org/Documents/congr10/1e.pdf.
17. United Nations Crime and Justice Information Network. Centre for International Crime Prevention. (2000). *Documents submitted for the consideration of the Commission on Crime Prevention and Criminal Justice at its 9th session (Vienna, 18-20 April 2000).* Retrieved August 5, 2013, from http://www.uncjin.org/Documents/9comm/index.html.
18. Council of Europe - Documents database. (1989). Recommendation No. R(89)9 of the Committee of Ministers to Member States on Computer-related Crime (adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers' Deputies). Retrieved August 5, 2013, from https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2.