УДК 339.341

Sazonets O. M., Doctor of Economics, Professor (National University of Water Management and Nature Resources Use, Rivne)

APPLICATION OF INFORMATION SECURITY TOOLS IN INTERNATIONAL ECONOMIC SYSTEMS

The article is concerned with information protection problems' solving in global economic systems. We examined risks of hazards to economic information systems in Internet, set out legal norms concerning interactions with unsafe websites of global network, considered measures of protection from Internet security hazards.
***Keywords*: information protection, global economic systems, security hazards to economic information systems, Internet, global network websites.**

Role of online network's information in modern international companies' development is growing. Protection of the information posted on the worldwide network system is a necessary condition for this system use. Such well-known scientists as M. Zgurovskyi, L. Vynaryk, A. Shchedryn, N. Vasilieva [3, 4] turned to the issue of information system security. We may not consider transformation of the world information space as completed until we overcome main problems connected with information security in the modern world.

Aiming at arranging reliable protection of international economic information the protection system provides a number of stages, as follows: analyzing potential hazards to information system, developing protection system, implementing protection system, protection system maintenance. Management of International Company's electronic information technologies includes protection of electronic technologies as an integral part of such management.

International Company's electronic technologies management mechanism provides comprehensive application of such protection measures as legal (laws, decrees, normative acts, which regulate liability for their violation), mental and ethical (the norms which are not legally ratified however, as far as a failure to follow them, results in the organization's fall in prestige, they are binding) administrative (measures of organizational nature which regulate processes of information system's functioning, it's resources' use, personnel's activity, etc.) physical (diverse mechanical, electric and electromechanical appliances and structures, intended for creating

physical barriers on the way of possible penetration and access of potential violators to information protection components), technical measures (hardware – software arrangements which perform information protection functions). Goal of the research is to discover problems of information protection in global economic systems and the ways of their solving as well as to study legal, economic, political and engineering aspects of their protection management in global information systems.

One of the major problems of informatization process is hacker attacks on information systems which inflict direct material losses on IT developers as well as on their users. Symantec issued comprehensive report about security system which is made by the Company's analysts every half a year. The main conclusion that we come to in this paper is that the same as before the most of malicious programs are produced by USA. It's on the territory of USA that the maximum number of hacking groups operates there and causes more attacks than anywhere in the world.

In Symantec they also note that there is rather tough competition between hacking groups on underworld market of attacks and stolen data trade. It is owing to this competence that, by experts' words, today you could buy stolen data cheaper and easier than it was half a year ago.

In the Internet Security Threat Report Symantec gives a number of examples: e.g. at the beginning of current year the Company's experts could buy stolen numbers of plastic bank cards at the price of $1 per each number, and the USA black market also offers diverse bank databases. However, as opposed to Russia where such information costs from $70 to $1000 per CD, in USA the average cost of CD with stolen bank data (details of account, transactions, etc.) makes just $14, as they assert us in Symantec.

In terms of the percentage of generated malicious codes USA also ranks first in the world – for the period under review every one in three spywares and every one in three Trojan viruses was created in USA. China is the second one – 10%, and Germany takes the third place – 7%.

Besides USA are also leading by quantity of botnets that consist of a few bot-infected computers by means of which hackers distributes spam and make attacks. In vast majority of cases the computer owners don't suspect of the machine's infection and lose process's allotted CPU time and traffic for the benefit of hackers.

It is noteworthy that in the second half of 2006 the number of PC involved in hackers' botnets increased by 29% up to 6 million items, and number of servers which administer such PC reduced by 25% – to 4700 items, that points to consolidation of botnets in hands of less quantity of trespassers. Most of botnets – 26% – are located on the territory of China.

Symantec also points out the growth of spam by 59% in the second half of 2006 that, as experts say, is quite a lot. On an international scale most of spam was connected with stock-market games and various financial frauds. McAfee is one of the most powerful companies which distribute anti-spam programs. Apart from that McAfee develops software against fishing, worms and viruses. Optional module, protecting against spam, diagnoses and blocks spam and fishing, and protection is always carried out according to the running updates.

For the first time ever Symantec explored the activity on International online market of networking fraudsters (fishers) who create websites, imitates websites of large online stores and banks with the purpose of the clients' identity theft. According to Alfred Huger, who is a Vice-President of Symantec Security Response unit, fishing became extremely organized, highly organized and free from any moral barriers. Growth of fake websites made 65% in comparison with the first half of 2006.

According to the data of International Company Aladdin Malware Report 2006, if in 2005, 60% of data received by applying the spyware and Trojans were related to minor threats, and in 2006 the most of Trojan and spyware applications had a status of average and critical level. Proceeding from the Report of Aladdin:

65% of spyware applications may be related to Trojan class;

30% of spyware applications mail spam;

15% of spyware applications carry out simultaneous recording of data keyboarded by the user;

10% of spyware applications use mechanisms peculiar to tootkits (a set of software tools working on the level of OS which are designed for protection and detection).

International information networks also carry on a struggle against viruses which may penetrate into computer through the network. Antivirus programs mentioned before as well as software and hardware tools are the protection means. One of them is a new software and hardware solution WS1000, developed as a result of Partnership between the Companies Sophos and SurfControl, which provides Internet security. This device has integrated application for systematization of URL address which has data of more than 21 million web pages. This solution will enable the administrators to manage efficiency of final users by means of websites' systematized database. The existing Sophos technologies will also provide protection from known and unknown viruses, worms, Trojans, advertising software as well as fishing websites.

According to the data of the poll conducted by ITU among the employees of IT sphere [10], hazards to Internet security have the following order:

malicious programs (48%), identity theft (43%), spyware (32%), fraud (22%), spam (12%).

At the same time 87% of respondents spoke up for the need to create information portal concerned with the issues of cyberspace security.

According to the data of the poll conducted by ITU among the employees of IT sphere [10], the most unsafe websites are the ones which are shown in Figure 2.

Concerning Internet browsers Internet Explorer is still the most "attractive" one for the hackers – 77% of attacks and vulnerabilities are connected with this browser. A lot of ideas are proposed to solve the aforesaid problems in IT world.

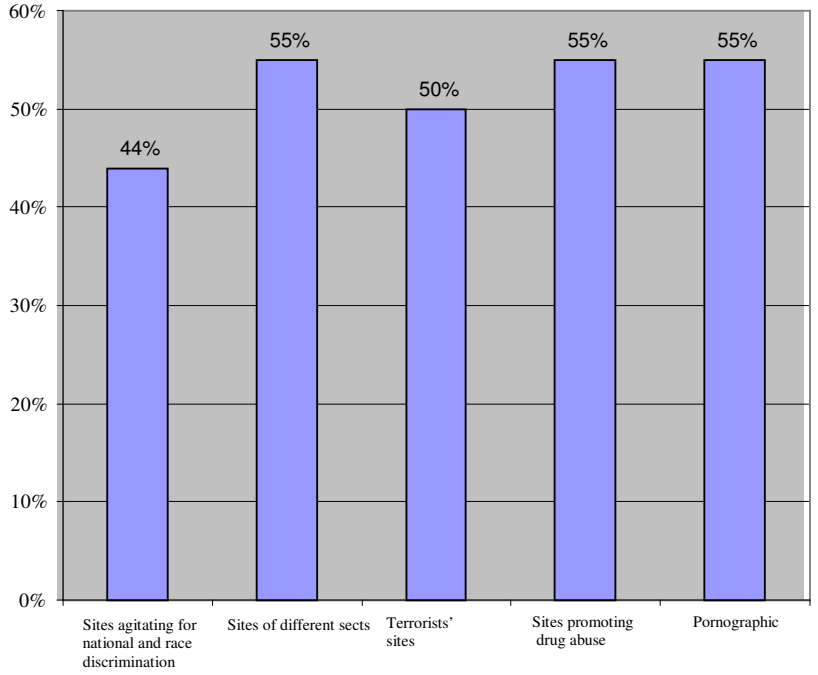

Figure. Unsafe websites

Working in Internet you should follow three legal rules:

– Only commercial use of the network is not allowed as far as considerable part of Internet is financed at expense of government subsidies;

– Internet – is an international network. Sending any information (including bits) abroad one should be governed by the laws which control export norms rather than by legal rules of his/her country;

– In case of delivery of any software or, e.g, just an idea, from one place to another you should take into consideration regional legal norms relating to intellectual property and licensing.

The Government financially supports most of Internet networks. According to the law an institution can spend money from their budget only for the purpose specified. If the Academy of Sciences finances the network than they may use such network only for scientific researches. The user may be unaware of the networks that his files are sent through, however these networks are under sphere of influence of the authorities who possess each of such networks. On our opinion it would be more rational to establish one big institution which could dispose of government subsidies and centralize all subsidized networks as far as maintaining a vast majority of networks is a waste of money. It's more expedient to create a network, as a part of Internet, e.g. for research and education which may be consequently used for any fundamental researches and education or for their support, rather than to have a majority of other similar but more specialized small networks.

It's impossible to overestimate the importance of the Ukrainian budget's article of expenses "on researches and education support". Existence of such article legalizes important sectors of the network's subsidizing which, as it may seem, do not comply with its purpose. E.g. a seller of the software, which is applied in researches or education process, may distribute his product and respond to the user's questions via e-mail. This sector complies with requirements "for researches and education support". At the same time this seller may use such network in business, e.g. in his work with market, when issuing invoices, submitting reports and bookkeeping. To carry out the aforesaid operations it is necessary to enter commercial area of the Internet.

Therefore preparing to connection with Internet the Company has to notify the network provider about the purpose of their connecting that means what way they are going to use the network: whether with research or commercial purpose. In the first case the routes which are subsidized for scientific-research and education purpose will prevail in the Network Traffic. If the organization is a commercial one then the commercial routes of data will prevail. Amount of payment for using this network depends on this factor as well. Usually commercial routes cost much more than the routes "for researches and education support", as far as they are not subsidized. It's only network administration who can clearly specify whether the commercial use id allowed or not on this connection.

Any export is a subject of responsibility and control of the respective Export Restrictions Department. Data's export is not an exception from this rule. Therefore in this case you should also meet requirements of date export regulations.

The laws of data's export might be formulated by the following two clauses:

– Export of anything requires a license;

– Fiscally export of services is approximately equivalent to export of components which are necessary for rendering such services.

The first clause is entirely evident: forwarding of file or any other material by e-mail or any other way has to be permitted by a special export license. In this case so called general license, which eliminates all obstacles, is a loophole. General license permits to export everything except what is specifically prohibited by law as well as all that may be found in public libraries. At the same time you should take into account that in case if export of any equipment (e.g. computer) is not permitted then outside countries' access to this equipment is prohibited and blocked. Therefore you should be cautious providing your colleagues from other country with access to "special resources" (like supercomputers). Nature of these restrictions, beyond all doubts, depends on the foreign country, and experience of the last decade proved that it may undergo rapid changes.

Let's mention typical mistakes which are illustrative of the legal liability beard by the operator of host computer, as follows:

– network operator is liable for illegal export only in case if he was aware about violation and nevertheless did not notify respective authorities about it;

– network operator is not liable for regular supervision over your user's activity and its legal nature.

Therefore most probably national networks' staff does not check all users' packages. However if network operator notices there any obvious violation of any directions then he is obliged to notify management about it.

Availability of national networks with cross communication lines complicates the situation of ownership rights in information networks as far as copyright and patent rights are different in various countries. For instance in the network you can find an interesting volume of forgotten technical documents where the copyrights are not valid in this country because of the expiry of the established period of limitation. Forwarding of such files to this country may put the users outside the federal law of the country that the files are sent from. The problem is also in the case that the law on electronic communications goes behind the technological progress. Even if there is a permit for e-mail sending it does mean that a message sent, by email, has

any actual protection.

Ownership rights may become a problem even in case of using any shared (public, publicly available) files. Some programs, which are available in Internet, have to be licensed by the seller. For instance, supplier of workstations may update their operating system and software through anonymous FTP. Therefore you can easily get these programs however to use them in a lawful way you should have a license for their use, e.g. you can officially buy these programs from the seller.

In respect of safety the computer which is connected to Internet is absolutely similar to the machine that you can connect through modem. Problems are the same and may differ only in their relevance. If modem is in standby mode then anyone can call there and try to crack it. However there exist some factors which defer crackers. There are three such factors, as follows:

– When telephone number of the computer is not publicly known;
– When the cracker is located beyond the local telephone network boundaries, then he has to pay for the period of his tampering attacks (unless he uses services of the nearby agent and forces the latter to work for him);
– If there is only one interface which may be attacked.

Internet does not have such mitigating factors. It's very easy to find address of any network and it's very simple to run through a few working machines and identify which one is operational. However such network's services have special security department and one entry point: ASCII terminal port. In contrast to such networks in Internet one can try to break into through dialogue window of terminal port, port of file transfer and port of e-mail, etc.

Generally speaking there are four reasons that the machine could be cracked by:

– Unfortunate choice of password;
– Import of defective software by legal users;
– Wrongly configured software;
– Errors in operating system.

It should also be noted that computer virus expansion often takes place trough programs downloaded from free unofficial sources.

Solving security problems we should point out the issue of passwords. Most of users chose passwords which are easy to recall. However the fact is that most of the things which are easy to recall, are widely known. Therefore you should follow the simple rules which are stated bellow. The password:

– should not be a word;
– should be not less than six symbols, and it's even better if eight;

– should have small and capital letters;

– should not be a typing of letters in succession on the keyboard, e.g. “ghbnnmjh” («приттьор») or “kl;’;lbnm,”(«лджєждитьб»).

Failure to comply with unauthorized access protection conditions may result in unwanted importation of information, and failure to comply with virus protection conditions may cause breakage of important systems and liquidation of many day-long operating results.

Computers which operating systems work with various tasks and which execute tasks for international companies (like Unix, VMS), are more vulnerable to virus threat. Users of multiple tasks operating systems have to meet the following requirements:

– every user should have his own individual login and password to enter Unix-server;

– a user should not disclose the password, which he set for himself, to other people;

– you should change the password not less than once per quarter as well as in cases when the password’s hacking is detected.

CONCLUSION

1) Application of scientific, methodical and practical results obtained from the research of information protection in global information networks may become a basis for many components of information technologies which are developed in the world.

2) Complex security should be based on integrity of legal norms stipulated for network usage in the word, information export restrictions and system protection factors development.

1. Law of Ukraine No. 80/94«On information protection in information and telecommunication systems», Verkhovna Rada, dated 5 July, 1994, Vedomosti of Verkhovna Rada of Ukraine, No. 31, 1994, p. 286. **2**. Law of Ukraine «On concept of National Informatization Program» No. 228-IV dated 4 February, 1998, Vedomosti of Verkhovna Rada of Ukraine, No. 27-28, 182 p. **3.** Zgurovskiy, Mikhail. Pathway to information society – from Geneva to Tunis, Mirror Weekly, 2005, No. 34, 3 Sept. **4.** Vinarik, L. S. Shchedrin, A. N., Vasilyeva, N. F. Online e-market: development, problems, Donetsk : Industrial Economics Institute, 2003, 76 p. **5.** Zhdanov, B. How to protect from insider, Director informatsionnoi sluzhby, 2007, № 3, p. 18. **6.** Endpoint Security Product, Website of Symantec antivirus product: Link: http://www.symantec.com/endpointsecurity. **7.** Pronenko, V. Viruses and antiviruses: four questions on topical subject, ComputerWorld/Ukraine, 2007, No. 11, p. 12-14. **8.** Sazonets, O. M. Government support to informatization of Ukrainian economy, Economy and State, 2006, No. 9, p. 31-33. **9.** Sazonets, O. M. Informatization of world economic relations: Teaching aid, K. : Centre of Educational Literature,

2008, 240 p. **10.** Statistics of Internet users' quantity, Information and analytical resource «Your personal Internet»: Link: http://www.content-filtering.ru/catalog.asp?ob_no=1660.

Рецензент: д.е.н., професор Сазонець І. Л. (НУВГП)

Сазонець О. М., д.е.н., професор (Національний університет водного господарства та природокористування, м. Рівне)

ЗАСТОСУВАННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ У МІЖНАРОДНИХ ЕКОНОМІЧНИХ СИСТЕМАХ

Стаття присвячена вирішенню проблем захисту інформації у глобальних економічних системах. Ми досліджували ризики небезпеки для економічних інформаційних систем у мережі Інтернет, викладених правових норм, що стосуються взаємодії з небезпечних веб-сайтів глобальної мережі, розглянули заходи захисту від небезпек Інтернет-безпеки.
***Ключові слова*: захист інформації, глобальні економічні системи, безпека економічних інформаційних систем, Інтернет, веб-сайти глобальної мережі.**

Сазонец О. Н., д.э.н., профессор (Национальный университет водного хозяйства и природопользования, г. Ровно)

ПРИМЕНЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В МЕЖДУНАРОДНЫХ ЭКОНОМИЧЕСКИХ СИСТЕМАХ

Статья посвящена решению проблем защиты информации в глобальных экономических системах. Мы исследовали риски опасности для экономических информационных систем в сети Интернет, изложенных правовых норм, касающихся взаимодействия с опасными сайтами глобальной сети, рассмотрели меры защиты от опасностей Интернет-безопасности.
***Ключевые слова*: защита информации, глобальные экономические системы, безопасность экономических информационных систем, Интернет, веб-сайты глобальной сети.**
