III INTERNATIONAL CONFERENCE
TRANSPORT SYSTEMS TELEMATICS TST`03

ZESZYTY NAUKOWE
POLITECHNIKI ŚLĄSKIEJ 2003
TRANSPORT z.51, nr kol. 1608

IT security,
IT security management

Stanisław KRAWIEC[1]

HAZARDS FOR ELECTRONIC TRANSACTIONS IN THE WIDE AREA NETWORKS

The paper presents quantitative tendencies of global network development, expressed in the growth of computer number on the Internet and growth in the area of Internet services, then the possibilities were presented how to use resources of these elements as a part of mocro-environment for the subjects operating within the Transportation System. Four models of YT applications in the transport have been presented as well as organizational, economical and qualitative aspects of dangers that are likely to apply to the collected and transmitted information, Special danger for the electronic transaction are likely to appear at the interface of the corporate network connected to the Internet and during data transmission through a wide area network.

ZAGROŻENIA TRANSAKCJI ELEKTRONICZNEJ W SIECIACH ROZLEGŁYCH

W artykule przedstawiono ilościowe tendencje rozwoju sieci globalnych, wyrażone przyrostem komputerów w sieci Internet oraz przyrostem usług internetowych, a następnie przedstawiono możliwości wykorzystania tych zasobów jako elementów mikrootoczenia dla podmiotów funkcjonujących w systemie transportowym. Przedstawiono cztery modele zastosowań telematyki w systemie transportowym oraz aspekty organizacyjne, ekonomiczne i jakościowe zagrożeń, jakie mogą dotyczyć gromadzonej i przesyłanej informacji. Szczególne zagrożenie dla transakcji elektronicznych może występować na styku sieci korporacyjnej podłączonej do Internetu oraz podczas transmisji danych przez sieć rozległą.

1. INTRODUCTION

Transportation institutions and companies operating within the subject structure of Transportation System more and more frequently use the electronic documents in their contacts between each other and with their customers. For this purpose they have to use the resources of wide area network Internet which may result in certain hazards for the information being sent, during transmission and at the interface between internet and corporate network.

[1] Faculty of Transport, Silesian University of Technology, Krasińskiego 8, 40-019 Katowice

2. QUANTITATIVE TENDENCIES OF NETWORK RESOURCES IN POLAND AND WORLDWIDE

Realization of a safe method of sending information in a wide area network is presently one of the most important challenges that the global web is facing. Unthinkable money is at the core of the matter, but also something more important than that. The wide spreading of electronic services may change entirely the model of worldwide commerce and services including transport ones. This means that the dynamic tendency of global web development measured by a number of computer connected to the Internet in each subsequent year and the number of potential customers using the new medium and awaiting new solutions in the transport area.

- Because of high complexity of computer networks and millions of computers that are connected to these networks, for the purpose of determining the wide area network dimensions a special software is used with the task of sending messages to the remote units and then their receipt and processing of answers received, Due to this operation and the continuous analyses it is possible to estimate the pace of continuously growing number of computers connected to the Internet, IP addresses or number of domains from some specific range.[2]
- Presently the number of ***hosts*** remaining in operation i.e computers with a permanent address written in the DNS registers is estimated at ***170 millions***. At the same time we have to draw attention both to the method of performing this measurement and thus establishing the number of computers on the Internet. This is related with variety of definitions assigned to the term ***„computer on the Internet"***. Basically we may use two types of approach:
  - A computer on the internet is a computer that is registered in the DNS server (host) that is not necessarily present in the Web physically but it is taken into account as it is in the register of name server,
  - A computer on the internet is a computer that is both in the name server registers and responds to the "ping" messages (this approach, however, excludes computers that are at this moment behind a *firewall* or do not respond to "ping" for othe reasons).

Results of the measurement are very different depending of the method applied. This is due not only to the firewall protection of the network but also to the fact that the majority of network use the ranges of IP addresses that are not visible beyond the network (non-routable addresses) and thus the computer with such an address will not respond to the "ping" message sent from beyond such network. Fig.1 presents the present specification of number of the computers worldwide having their addresses written in the DNS registers i.e. dimensions of the Internet estimated using the first method in the period 1969 – 2003.

[2] Certain protocols used for testing are available also to normal users. Instance of such software may be ***ping*** program that sends messages to the remote computer and informs about each answer. This enables also determination of the size of package being sent, calculation of travel in both directions (i.e. time between sending data and receipt of answer). Another instance is a program called ***traceroute***, which enables determination of intermediate computers located on the way to the receiver.

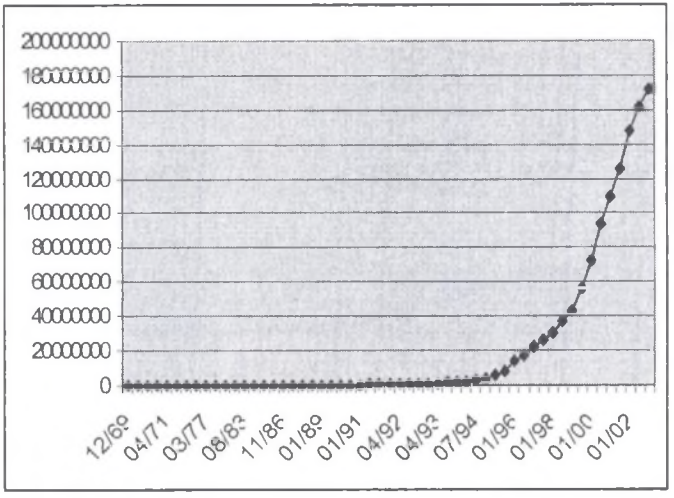

Fig.1. Development of Internet measured by the number of computers connected in the period 1969 – 2003
Source: Own study based on the service www.isc.org and document RFC 1296

The dimensions of the Internet may also be measured with other parameters, such as development of basic internet service i.e. WWW (Fig. 2) We have, however, to draw our attention to the fact that the number of WWW sites in the presented specification is equivalent to the number of servers (Web Servers) whereas in reality each host may have many WWW sites using various domains and different ports. However, the Fig.2 illustrates the dynamic development of this service, entailing development of the Internet.

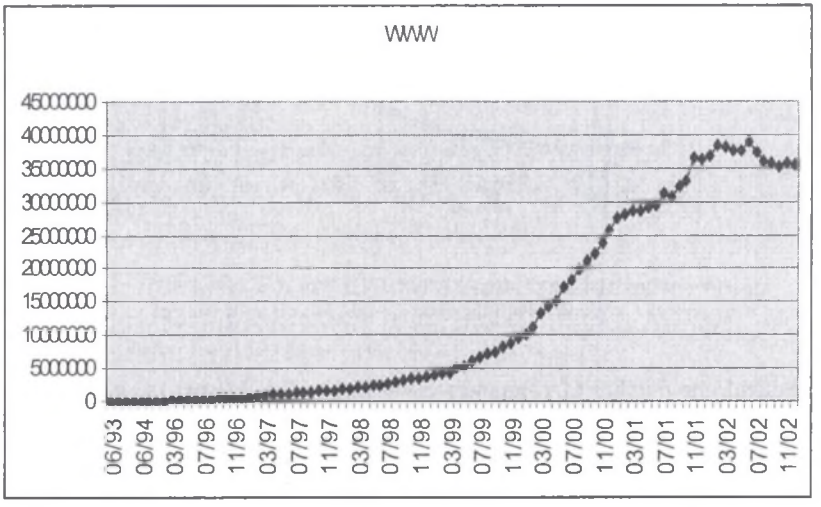

Fig. 2. Development of Internet measured by the number of WWW sites (Web Serwerów) in the period 1993-2002

In Europe, in June 2003 the number of hosts reached 20 millions, and its development is shown in Table 1 and on Fig.3.

Table 1

Number of hosts in Europe (period 1991-2003)

Date	Hosts	Annual growth index	Date	Hosts	Annual growth index
01/91	43832	-	07/97	4840248	1,60
07/91	68267	-	01/98	5942491	1,52
01/92	141308	3,22	07/98	6982995	1,44
07/92	213017	3,12	01/99	8200734	1,38
01/93	303828	2,15	07/99	9148276	1,31
07/93	426827	2,00	01/00	10818526	1,32
01/94	587135	1,93	07/00	11775430	1,29
07/94	789747	1,85	01/01	12686098	1,17
01/95	1106077	1,88	07/01	15308471	1,30
07/95	1694978	2,15	01/02	16414704	1,29
01/96	2284750	2,07	07/02	16967038	1,11
07/96	3017784	1,78	01/03	17141798	1,03
01/97	3921946	1,72	06/03	20402888	-

Source: Own study based on the service www.ripe.net

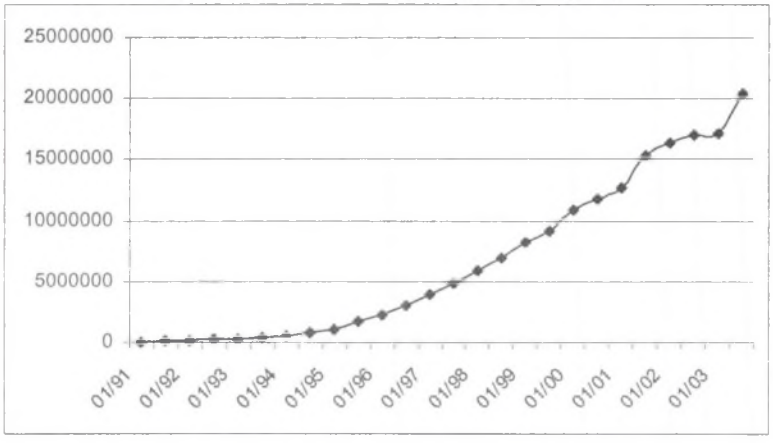

Fig.3. Growth of number of hosts in Europe (lata 1991-2003)
Source: Own study based on the service www.ripe.net

In Poland, the number of computers connected to the Internet (so-called hosts) at the end of June 2003 amounted to also 750 thousands. Taking the usual coefficient of minimum 10 users per one host we have the number of 7,5 milion Internet users in Poland. Other estimation, based on questionnaires, define the number of users amounting to 8,5 million.. Tendencies in this respect are shown on Fig 4 .

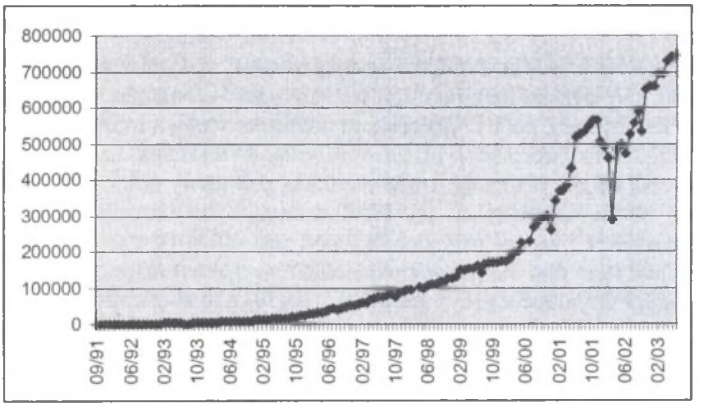

Fig.4. Number of hosts in Poland (1991-2003)
Source: Own study based on the service www.ripe.net

However taking into account the percentage of hosts, in the ninety countries aken into consideration, Poland is located on 9nth place (June 2003) - Fig.5.

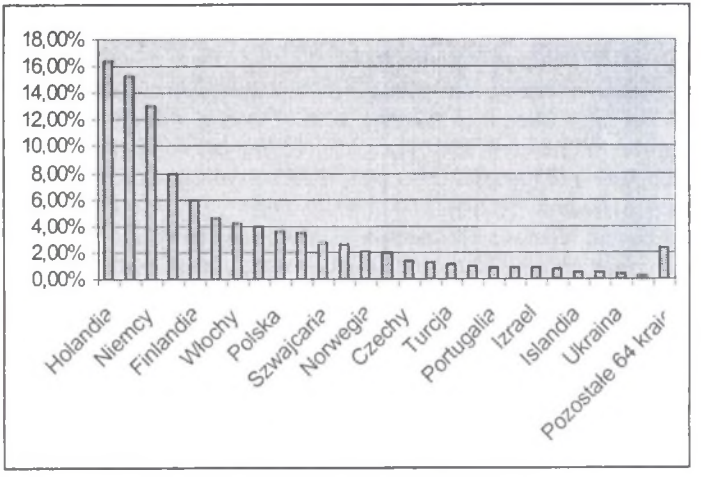

Fig.5. Graphics interpretation of the percentage of hosts in the countries of Europe
Source: Own study based on the service www.rine.net

Generally we may assume that Polans from the point of view of number of computers connected to the Internet per 1000 of inhabitants (20) is near to reaching the average that for Europe is 28. The quantitative description of the development of this phenomenon commonly named Internet cannot be without effect on the realization of transport service, related in a complementary or substitution way with data transmission and processing.

3. INFORMATION IN THE TRANSPORTATION SYSTEM

The basic network resource subject to transmission and processing is information. In XXI century in the age of information society each economic subject or institution, independent of its business, collects, keeps and processes various information, We may even say that it is addicted to information because information warrants its existence, Information about ways to operate the company, trade contracts and many other matters conditions the competitiveness of the company on the market, and in the case of business related with realization of transport process may decide upon the safest of this process, With a high probability we may state that the governmental and commercial institutions and even specific units are more and more dependent of the quick, reliable and above all secure processing and secure transmission of the enormous quantity of information, wor which purpose they use IT systems.

Application of IT solutions in the subject structure of Transportation System and its surroundings may be basically divided into four models differing by assumed objectives:

- Business – to – Business (B2B).
  B2B is a transaction[3] model between companies. As analysts say, it will generate the highest turnover (as a target even 90% of revenues). The American market leading worldwide presently the develops namely in this direction, and the similar phenomenon occurs also in the European Union countries and it well also take place in Poland, because use of modern technologies allows to have the best results i.e. reduce the costs and make the logistics more efficient. Correct use of these opportunities will be a condition for maintaining the position of competitive company on the market.
- Business – to – Consumer (Client) (B2C).
  This is solution realizing the transaction between demand and supply of transport services. The most often they take the form of selling, marketing, sending documents, searching for information, etc. The basic B2C systems task is to enable purchases online, supporting of logistics processes, reduction of transaction costs.
- Business – to – Public (B2P).
  This area covers relations between the transport company and its social surroundings. The most important tasks of the B2P system in the company are: creation of company's image (not only on the Internet), promotion of the company's mark and its products, establishing the bond between the company and its surroundings and last but not least attracting new customers
- Security – to – Business (S2B).
  It is a transaction model ensuring broadly understood security of transport services to the customers.

All these models without doubt have or will have impact on the shape of transport service, especially in the context of its quality.

---

[3] **Internet transaction** is a high level abstraction of process synchronization in the distributed systems hiding the technical issues related with synchronization such as management of critical section, preventing the blcks and reconstruction after failure and performed by the server on the customer's order. The transactions originate from databases and have the following properties: ATOMICITY – transaction is performed in full or not performed at all, CONSISTENCY – transaction does not infringe system constants, ISOLATION – the current transaction does not collide with any other, DURABILITY – upon completion of the transaction the revisions are permanently stored.

4. INFORMATION – AN ENDANGERED PRODUCT

Information as a product is endangered in many ways, and its growing value results in the increase of these dangers, thus protection of information system and information processed by them have become an issue of utmost importance. Independently of legal aspects of the information protection the real security of this "product" may be an ultimate condition of existence of a company or institution. Conviction about this significance of information is more and more common and applies to the widening circle of interested parties. The protection of a multiplying growth of information demand and supply is a mark of success of administrative, scientific, economical, political and social processes. This issue takes an exceptional meaning in the situation when the computer is connected to the network, and especially to the wide area network.

These tests, performed by the company „Mori" enabled an assessment that the cost of data loss only in the small companies of European Union countries (without possibility of restoration) would amount to 1200 milliards of pounds – i.e. four times the GNP of Switzerland. During these tests it was stated that among small companies being tested 40% of companies does not make backup of important files even once in a week. The data protection issue in small companies was taken into consideration, because namely these companies stand for employment of 60% of the European labor force, and operation of certain of them in 100% is related with the information contained in the computers. The entrepreneurs acquire an increasing understanding of the information security importance – although, according to the tests, the real implementation of the applicable protections is hardly encouraging. The entrepreneurs frequently are not able to determine where the most important information, fundamental to the company's interests are kept. Even worse situation exists in the area of awareness and knowledge of protection methods. The most frequently the managers of these companies are not able to determine even approximately how high would be the costs of loss of important information. The most reasonable say that they can be quite high.

The increased danger to the computer and network security is shown in the data published by the Computer Emergency Response Team (CERT) of Carnegie – Mellon University in Pittsburgh, in 2001. This team was appointed by the US authorities for discovering and informing about potential dangers in the Internet. In 1988 CERT has noted 6 incidents, in 1999 the number of incidents was 959 and in 2000 already 21756 incidents infringing the network security (herein 22 were important)

Incident is occurrence of a danger without regard to the scale of resulting damage, which means that the spreading of Melissa virus was treated as a single case.

The Polish division of CERT keeps its statistics since 1996. Since then the number of noted incidents is continuously growing. The types of attacks noted are not changing dramatically over the years. Since several years the most popular are attacks on electronic mail, attacks consisting in scanning specific computers or even the entire networks, attacks to the WWW servers, to applications and processes. Presently we mostly have to deal with the attacks related with scanning and very popular spamming. In its annual reports, CERT NASK presents the typology and sources of attacks notified in Poland. For instance, in 2000 there were noted 126 incidents of security infringement where 292 computers (hosts) were attacked. Majority of them 206, standing for over 70% were involved in the cases of intrusion to the system (182 cases) and attempts of such intrusion to the system (24 cases) i.e. with the deadliest cases of infringement of IT structures. The percentage specification of the deadliest IT security endangering cases may be described as follows (tab. 2).

Table 2

Network security infringement

Items .	Types of danger	% distribution of security infringement cases	% distribution of attacked computers
1	Attemts of intrusion to the system	19%	8%
2	Intrusion to the system	15%	62%
3	Host scanning	15%	7%
4	Network scanning	13%	6%
5	DoS attacks	13%	7%
6	WWW server attacks	6%	6%
7	e-mail bombs	5%	3%
8	Scanning of firewalls	3%	1%
9	other	10%	4%

Source: Own study based on the report of CERT NASK

Common research performed by The Computer Security and FBI carried out among 643 persons responsible for security in the American companies, governmental agencies, financial and medical institutions and universities have shown that 90% of responders have discovered in 200 attacks on their IT networks and 273 organizations announced financial losses to a total amount of 265 589 940 USD. This is but a part of the truth because several companies hide their losses fearing the loss of their customers.

Fig. 6 present a forecast concerning expenses and developed by the Internet Security Software, who forecasts that in 2003 it will spend 8 milliard dollars for protection of their data.

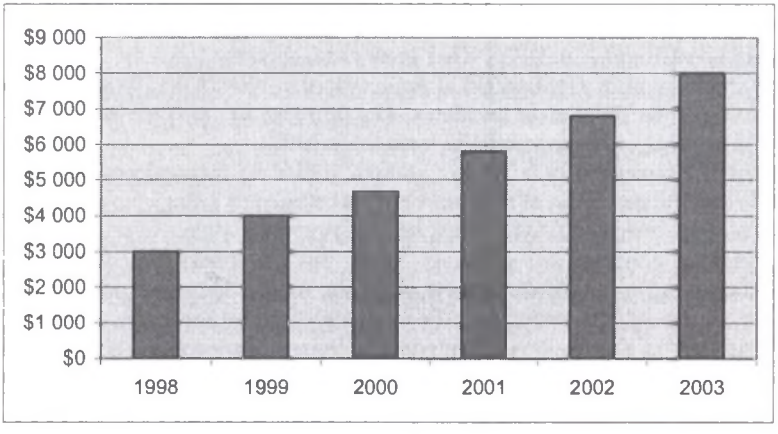

Fig.6. The worldwide expenses incurred for protection of data in mln USD
Source: Internet Security Software

It is expected that in a few years the guaranteed security for the corporate computer networks only will cost worldwide more than ten milliard dollars per year. (the forecasts concerning the market of internet security services in Europe in 2006 will cost about 4,6 milliard USD and worldwide 15 milliard USD respectively)Many indications suggest that 2003 will be the worst year in terms of network security. This is shown by the following facts:

- The time from detection of a computer program error till the moment when the network criminals make use of it is shrinking systematically:
  - in 1999 it was 500 days,
  - in the period 2000 – 2002 the time period from detection of a gap till its criminal use grew shorter to amount to 40 days,
  - in the first half of 2003 the 64% of attacks used the software errors detected within the last year, in average within ten-odd days.
- The number of errors in the distributed software is growing:
  - every day worldwide seven errors is discovered in the commonly used user's software - from databases to the operating systems; in 1999, 417 such errors were detected, in 2000 - 1090 and in 2002 already more than 2500; in the I half of 2003 there were found 12 % more errors than in the I half-year of 2002, herein 80% may be used for criminal purposes
- The viruses spread with increased speed (at the beginning of 2003 the Bugbear.B virus has infected 60 thousand computers in 3 minutes, and so-called Warhol worm enables infection of several thousand machines within one minute, or a million of computers in 8 minutes.
- The number of viruses of „blended threats" type is growing (by 20%) i.e. small vicious programs combining the features of viruses, worms and Troyans that install themselves and attack the computers in the network (two of them that are the best konw are MS Blaster and SQL Slammer); it is estimated that every year several thousands of MS Blaster type virus are created, such as CodeRed, Nimda, Sobig etc.
- Mutation of MS Blaster virus that attacked in August 2003 and SQL Slammer virus (January 2003) infected several millions of computers, exposing hundreds of companies to the multi-million losses (in total the losses incurred within 8 days in August were estimated at 2 milliard USD) and the computer were infected in a very short time.
- The network criminals most often create viruses whose purpose is to expose the companies to the losses (an exception was a very popular one, SQL Slammer whose code was set on the quickest spreading and not destroying data, but the deadliest virus of 2003 Bugbear.B was created to attack the banking systems).
- High vulnerability of Microsoft products (especially operating systems) to the attacks because of unfinished condition and numerous gaps that encourage network criminals (MS Blaster is typical revenge on the Microsoft company).

Applications used to the protection of computer systems do not give any guarantee of "immunity". There are no hundred percent efficient programs, systems, servers. In the period of open and frequently changing information environments the level of dangers and risk is increasing, thus the special attention must be paid to the efficient management of data concerning the safety level. The IT technology progress results in the fact that each subsequent generation of epidemies (following attack) may be more threatening, quickest and bring about more financial losses.

The sources of attacks change in the world's scale. Till the lat year, the head of a list countries originating the highest number of attacks per 10.000 of Internet users included Poland (one of the first ten places). In the I half of 2003 Poland in this classification occupies 16 position (Fig. 7)

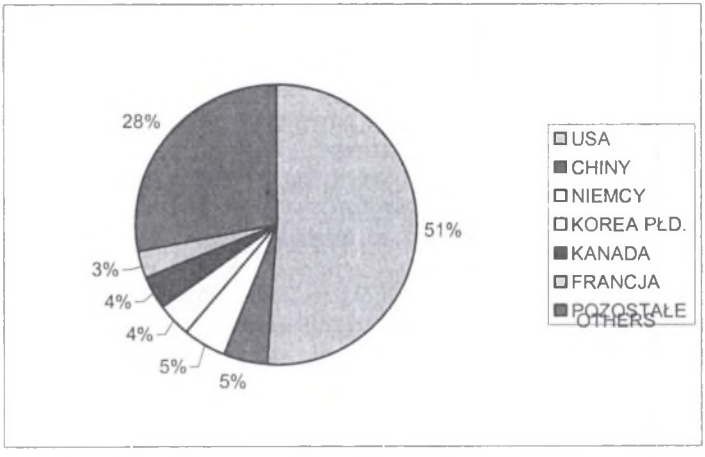

Fig.7. Sources if virus epidemies
Source: Symantec Internet Security Threat Reports

Even the best software or hardware will not protect our resources if we don't realize what we want to protect and against what. Hence the terms such as security policy or data protection management take a special meaning. On the other hand we may be aware that reaching a complete security in the contemporary computer systems is not possible inpractice. Thisis related with the fact that:

- computer system have frequently „open" character and implementation of 100% efficient protection would result in a loss of this character,
- cost of implementing an absolute security would be so high that it would be more than the value of the entire system.

Assessment of computer system security may however make one aware whar are its gaps and drawbacks and contribute significantly to the increased protection level of information kept and processed within this system.

BIBLIOGRAPHY

[1] KIFNER T.; Polityka bezpieczeństwa i ochrony informacji (IT security information and detection policy), Publication Helion, Gliwice, 1999.

[2] „Rzeczpospolita" No 73 dated 27.03.2000.

[3] KLESZYŃSKI K., TWOREK G.; Windows NT – bezpieczny serwer (Windows NT – safe server), Publication of professional information Weka, Warsaw, 2000.

[4] STRUŻ B.; Analiza występujących i możliwych zagrożeń w systemach informatycznych. Koncepcje bezpieczeństwa informatycznego i stosowane rozwiązania (Analysis of hazards occurring and likely to occur in the information systems. Concepts of information security and solutions applied), Study National Defense Academy, Information Center, Warsaw, 1995, s.6.

[5] GARFINKEL S., SAPFFORD G.; Bezpieczeństwo w Unixie i Internecie (Security in Unix and Internet), Publication RM, 1997.

[6] GARFINKEL S., SAPFFORD G.; WWW – bezpieczeństwo i handel (WWW – safety and commerce), Publication Helion, 1999.

[7] GREGOR B., STAWISZYŃSKI M., E-Commerce, Publication Branta, 2002.

[8] STROTHMANN Willy-B; Kryptografia. Teoria i praktyka zabezpieczenia systemów komputerowych (Cryptography. Theory and practice of computer system protection), Publication Read Me, 2000.

[9] LLOYD S., ADAMS C.; Podpis elektroniczny: klucz publiczny (Electronic signature. Public key), Publication Robomatic, 2002.

[10] BAUER F. L.; Sekrety kryptografii (Secrets of cryptography), Publication Helion, 2003.

[11] W. Stallings; Ochrona danych w sieci i intersieci (Data protection in the net and Internet), Wydawnictwo Naukowo-Techniczne, 1997.

[12] KOWALCZUK P., DĄBROWSKI W.; Podpis elektroniczny (Electronic signature), Mikom, 2003.

[13] SCHETINA E., GREEN K., CARLSON J.; Bezpieczeństwo w sieci (Safety in the network), Publication Helion, 2002.

[14] COMER D. E.; Sieci komputerowe i intersieci (Computer networks and inter-networks), WNT Warsaw 2000.

[15] SILICKI K., NASK; Rola zespołów reagujących na zdarzenia naruszające bezpieczeństwo sieci (Role of reaction teams to the events infringing the safety of network), Conference Paper "Przestępczość w sieciach komputerowych" (Crime in the computer networks), Legionowo '96.

[16] DUDEK A.; Nie tylko wirusy. Hacking, cracking, bezpieczeństwo internetu (Not only viruses. Hacking, cracking, internet security), Publication Helion, 1998.

[17] Act of Law dated 22 January 1999 on protection of confidential information, Dz. U. Nr 11, item. 95

[18] Ordinance of President of RM dated 25 February 1999 on basic requirements of systems and IT network security, Dz. U. Nr 18 item. 162.

[19] Recommendation of State Defense Office on TI security , version 1.1, August 2000.

[20] JĘDRZEJEK C., red; Internet w Polsce – technologie i rynek (Internet in Poland – technologies and market), Monography of IT and Information Technology Institute, Poznań 2000.

[21] BS 7799: 1995 Code of practice for Information Security Management, British Standard Institute.

[22] IS ISO/IEC 15408: 1999(E) Information technology – Security Techniques – Evaluation criteria for information technology security, IT Security Magazine nr 7-8(11-12) July/August 2000.

[23] POHORECKI G.; Secure Sockets Layer – bezpieczna komunikacja w sieci www (Secure Sockets Layer – safe communication in the web), IT Security Magazine, nr 4(8) April 2000.

[24] Vademecum teleinformatyka, praca zbiorowa (Vademecum of IT specialist I, collective work), IDG Poland S. A., Warsaw 1999.

[25] Vademecum teleinformatyka II, praca zbiorowa (Vademecum of IT specialist II, collective work), IDG Poland S. A., Warsaw 2002.

[26] Depatrment of Defence Trusted Computer System Evaluation Criteria. DOD 5200.28-STD, National Computer Security Centre, Fort Mead. MD, December 1985.

[27] Symantec Internet Security Threat Reports 2003 from H. Salik. Symantec Report on virus hazard. Gazeta Wyborcza 9.X.2003. Dodatek Gospodarczy and H. Salik Polowanie na hakerów (Hacker hunt), Gazeta Wyborcza 30.III.2003. Dodatek Gospodarczy.

Reviewer: Ph. D. Jerzy Mikulski