Academia de Studii Economice a Moldovei

Academia Militară "Alexandru cel Bun"

LSI

Laboratorul de securitate informațională al ASEM

SECURITATEA INFORMAȚIONALĂ 2013

CONFERINȚĂ INTERNAȚIONALĂ,
(ediția a X-a Jubiliară), 19 aprilie 2013

www.security.ase.md

Academia de Studii Economice
a Moldovei

Academia Militară
„Alexandru cel Bun”

Laboratorul de Securitate Informațională al ASEM

SECURITATEA INFORMAȚIONALĂ 2013

CONFERINȚĂ INTERNAȚIONALĂ
(ediția a X-a Jubiliară)

19 Aprilie 2013

Chişinău – 2013

CZU 004.056(082)=135.1=111=161.1
S 40

COMITETUL DE ORGANIZARE:

Grigore Belostecinic, rector al Academiei de Studii Economice din Moldova, academician al Academiei de Ştiinţă a Moldovei, doctor habilitat, profesor.
Tatiana Mişova, prorector al Academiei de Studii Economice din Moldova, doctor, profesor.
Ilie Costaş, doctor habilitat, profesor, Academia de Studii Economice din Moldova.
Veaceslav Perju, doctor habilitat, profesor, Vicepreşedinte al Consiliului Naţional pentru Acreditare şi Atestare al Republicii Moldova.
Serghei Ohrimenco, doctor habilitat, profesor, Academia de Studii Economice din Moldova.
Teodor Ţîrdia, doctior habilitat, profesor, Universitatea de Stat de Medicină.
Tudor Leahu, doctor, Universitatea Cooperatist – Comercială.
Leszek Fryderyk Korzeniowski, prof. nadzw. dr hab., preşedintele Asociaţiei Europene pentru Securitate.
Agop Sarkisian, doctor, Academia de Economie, Svistov, Bulgaria.
Vladimir Golubev, doctor, profesor, Centrul de Cercetare a Crimelor de Computator.
Ghenadie Safonov, locotenent-colonel, Academia Militară a Forţelor Armate „Alexandru cel Bun" .
Viktor Blagodstskih, doctor, profesor, Universitatea de Stat din Moscova de Economie, Statistică si Informatică.
Veselin Dimitrov Popov, doctor, Academia Economică.
Genadii Cernei, doctor, expert, Vice-preşedinte al Băncii comerciale "UNIBANK" S.A.
Valerii Domarev, doctor, expert (Ucraina)
Andrzej Augustynek, doctor, AGH University of Science and Technology.
Vladimir Skvir, doctor, expert, Universitatea Politehnică Naţională din Lvov.
Serghei Kavun, doctor, Universitatea Economică Naţională din Harkov.
Constantin Sclifos, MCP, expert, Academia de Studii Economice din Moldova.
Vitalie Spînachi, LL.M., expert, primar s. Cărbuna, r-nul Ialoveni, Republica Moldova.
Tatiana Monasterska, dr., The President Stanisław Wojciechowski Higher Vocational State School in Kalisz.
Dimitar Georgiev Velev, dr., University of National and World Economy.
Anatoly Krapivensky, Ph.D. in Sociology, Institute of Youth Policy & Social Work.

Descrierea CIP a Camerei Naţionale a Cărţii
"Securitatea informaţională 2013", conf. intern. (10 ; 2013 ; Chişinău). Securitatea informaţională 2013 : conf. intern., 19 apr. 2013 (ed. a 10-a Jubiliară) / com. org.: Grigore Belostecinic [et al.] ; coord. ed.: Serghei Ohrimenco. – Chişinău : ASEM, 2013. – 126 p.
Antetit.: Acad. de Studii Econ. a Moldovei, Lab. de Securitate Informaţională. – Texte: lb. rom., engl., rusă. – Rez.: lb. engl. – Referinţe bibliogr. la sfârşitul art. şi în subsol. – 25 ex.
ISBN 978-9975-75-640-2.
004.056(082)=135.1=111=161.1

Coordonatorul ediţiei - prof.univ. dr. hab. **S. Ohrimenco**

ISBN 978-9975-75-640-2

ORGANIZATORII CONFERINȚEI:

ACADEMIA DE STUDII ECONOMICE DIN MOLDOVA

ACADEMIA MILITARĂ „ALEXANDRU CEL BUN”

Laboratorul de Securitate Informațională al ASEM este membru al Asociației Europene pentru Securitate

SPONSORI:

Franzeluța®
FONDAT ÎN 1947
Căldura inimilor noastre în fiecare produs!

INFOPROTECT

Cuprins:

Veselin Popov, Agop Sarkisyan
Information security in cloud computing: challenges, threats and recommendations..... 6
Dimiter G. Velev
Main Threats in cloud security..... 11
Владимир Голубев
Детская порнография в Интернете: проблемы противодействия..... 16
Кавун С.В., Дашков А. В.
Использование интенет-анализа в сфере информационной безопасности..... 18
Maciej Szmit, Roman Jašek
About a five troublesome IT security oriented phrases..... 21
Ghenadie Safonov, Anatolie Calancea
Spațiul cibernetic - teren de confruntare..... 25
Plamen Milev
Development of university information systems for research projects..... 31
Брединский Анатолий
Носители информации и утечка данных: анализ международного опыта..... 33
Ольга Пугачева
Проблемы использования интеллектуальных ресурсов в процессе инновационной деятельности организаций научно-образовательной сферы.....36
Katia Strahilova
Importance of providing information for conducting effective local administrative policy..... 40
Ирина Балина
Формализация принципов классификации экономических рисков.....42
Сайдикрамова Анна
Новые приоритеты в информационной безопасности в современном мире..... 48
Lyubomir V. Vladimirov, Nikolai I. Kovachev
Information risks during measurements of noise pollution..... 51
Бортэ Григорий
Анализ этапов развития теневой информационной экономики.....53
Nicolae Turcan
Personal data dangers.....55
Ирина Шныр
Направления защиты авторского права в сети интернет в Республике Беларусь.....58
А. Ахмаджонов
Требования по защите информации от утечки за счет побочных электромагнитных излучений.....60
Irina Babară, Marin Lupu
Securitatea informațională în era tehnologică..... 63

Natalia Futekova
Main stages in development of software applications in telecommunications.....68
Татьяна Чикарёва
Проблемы инсайдинга.....70
Iulian Mihăescu
Protecția informațiilor clasificate, în era informațională.....73
Павлова Лилия
Внутренний контроль в системе корпоративного управления.....75
Plamen M. Manev, Lyubomir V. Vladimirov
Uncertainty of the information in analysis of the environmental and ergonomic risk of equipment for environmental protection.....78
Сторож Оксана
Метрики тестирования – необходимость обеспечения качества программного продукта.....81
Alexanru Buruc, Dan Nistor
Securitatea cibernetică şi securitatea națională. Cazul Republicii Moldova.....83
Е. Згардан, С. Жук
CRM в облаке.....89
Галина Шелеляева
Электронный документооборот и защита данных.....92
Elena Paximadi, Ion Petroșișin
Securitatea informației personale.....94
Claudia Hlopeanicov, Sergiu Munteanu
Măsurile securității cibernetice în societatea informațională.....98
Roman Gojan, Iulian Stan
Infractiunile informationale si spionajul informational.....103
Rodica Bulai
Estimarea cantitativă şi calitativă a riscurilor informaționale.....110
Дорошев Дмитрий, Корнеенко Ольга
Тенденции распространения угроз информационной безопасности.....113
Ремезова Екатерина Максимовна
Дорохов Михаил Александрович
Информационная безопасность инвестиционной деятельности предприятия.....116
Юрчук Виталий Анатолиевич
Опыт ЕС по разработке нормативно-правовой базы в сфере кибербезопасности.....119
Tsvetelin T. Borisov
Safety of electronic commerce in bulgaria – safe or risky methods of work.....122
Boryana Todorova
Prerequisites and disadvantages in e-commerce.....124

INFORMATION SECURITY IN CLOUD COMPUTING: CHALLENGES, THREATS AND RECOMMENDATIONS

Assoc. Prof. Veselin POPOV, Ph. D.,
Assoc. Prof. Agop Sarkisyan, Ph. D.
Tsenov, Academy of Economics, Svishtov, Bulgaria

The main aim of this report is to investigate the threats to information security of cloud computing. To achieve this goal, a survey of publications related to the security in the cloud is held. A classification of the most important security threats in the usage of cloud is done and recommendations to avoid them are made. The problems of security in the private cloud are examined, as one of the trends of development of this treatment in the large and medium-sized companies.

Keywords: cloud computing, information security, threats, private cloud

1. Cloud computing and trends in its use

The evolutionary development of technologies for processing and storage of data has led to the emergence of a new model of treatment - cloud computing, where documents and applications are available on the server and can be accessed remotely, over the Internet. "Cloud Computing - a model that provides extensive and convenient network access on-demand computing resources (eg, networks, servers, storage, applications, services) that can be quickly delivered and released with minimal effort on management and interaction with the service provider. "[1] Cloud computing is a new way to implement computer processing, featuring the best at this instant moment technological capabilities for flexibility and scalability, which are delivered as a service over the Internet.

The models, which are developed Cloud computing are:

- *Public clod* - cloud infrastructure which is widely available to the public and is owned by a provider of cloud services.
- *Private cloud* - cloud infrastructure that is behind a firewall and is hosted on its own network.
- *Community cloud* - cloud infrastructure which is shared by several organizations and is supported by a community that has established common requirements for its usage as politics, security requirements, and agreement for usage.
- *Hybrid cloud* - cloud infrastructure that includes two or more clouds (public, or private), which remain separate, but are interconnected by standardized or proprietary technology.

Cloud computing has established itself as one of the most promising and innovative directions in the field of information technology in recent years. According to the global leader in research and research in information technology and services Gartner Group, cloud computing is the main trend that permeates the market over the past two

years [2]. According to estimates of the mentioned analytical company, for the period until 2016 a significant increase in services offered by cloud infrastructure is expected [3] as follows: business process as a service - 15%, software as a service - 17.4%, Platform as a Service - 26.6 percent, infrastructure as a service - 41.7%. These estimates indicate the expectations of the experts that cloud services will be a priority area for the development of organizations and companies in the coming years.

2. Information security in cloud computing

Massive deployment of cloud computing in the enterprise provoked concern among consumers. The main problems, according to a survey by IDC [4] are: security - 74.6%, productivity - 63.1%, benefit - 63.1%, difficult to integrate their IT - 61.1%. Accoring to another study - "2012 Global Information Security Survey" [5] Ernst & Young, the efforts are now aimed at controlling the cloud computing, social media and mobile risks. The results of this study conducted among 1850 CIO shows that radical change is needed in the approach to security. These, and also other studies [6] show that the usage of cloud computing increases the risks to information security compared to the traditional use of IT.

In the next section, after the led research of literature, information security risks when using cloud computing are systematized.

3. Risks to information security in the cloud

The essence of the model of cloud computing lies in the usage of computing resources which are usually provided by third party service providers on the Internet. This involves storing data on the server of another provider, together with the data of many other tenants of the service. The usage of public communication networks such as the Internet is also required.

After examining the issues of security of cloud computing, we can systematize the main areas with potential risks. These are:

A) **Security of the virtual machine level** [7]. At the core of cloud computing is the virtual machine. For its operation various software tools such as VMWare, VSphere, Microsoft Virtual PC, etc. are used. Threats arising at the level of the virtual machine can be avoided through IDS (Instruction Detection System) / IPS (Intrusion Prevention System) and by implementing firewall.

B) **Network Level Security** [9]. Services provided by the cloud infrastructure are used by public or private networks which can be small area or large area networks, each of which has different security threats. The most common threats and problems that arise at this level are DNS attacks, Sniffer attacks, issue of reused IP address, Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS) etc. These threats can be avoided by ensuring the confidentiality and integrity in the network, improving access control and more.

C) **Web browser security** [10]. In the midst of the cloud, the processing is done on remote servers. The client's computer is used for input and output. The client's software, which is used is the browser as universal, widely distributed and platform-independent software. Using a Secured Sockets Layer (SSL) to

encrypt the credentials to authenticate the user, a communication from point to point is used. When with this communication is linked third-party host, this can be used to decrypt the data. Than it is possible that a hacker sniffs packages on intermediary host and receives the credentials of the user to join the cloud system as a valid user. As a measure to avoid this threat, the service provider must use WS-security, which operates at message using XML encryption of SOAP messages, which can not be decrypted at mediator hosts.

D) **Application Program Interface (API) security** [8]. The level PaaS offers a variety of business functions, security functions and applications to users. The access to these services is done with API, which should be provided with standards and tools for security, should require authentication and authorization for inclusion in the API. Another requirement is that it has insulation APIs in memory. These requirements must be met by the service.

4. Private cloud computing security

Before we could pinpoint our attention to the problems of private cloud computing let us try to define what means the term itself. There are many definitions- both technical and non-technical. All of them outline the fact that private cloud (also called internal cloud or corporate cloud) is a marketing term for a proprietary computing architecture that provides hosted services to a limited number of people behind a firewall. i. e. the advances of virtualization and distributed computing have allowed corporate network and data-center administrators to actually become service providers that meet the needs of their "customers" within the corporation. Another definition says: private cloud is a form of cloud computing where service access is limited or the customer has some control/ownership of the service implementation. In Wikipedia[1] the definition is that: a private cloud is a software-defined data center that combines essential hardware and other computing resources into a unified virtualized unit. So, a private cloud's layer of hardware and networking abstraction – again, provided by software – enables enterprises to scale and provision resources more dynamically than is possible with traditional hardware-centric computing environments. Actually, it is not only that a company server room containing a self-contained cloud infrastructure would certainly count as a private cloud, but there are other things to take into account besides the physical location of the servers themselves. For example, if a similar infrastructure, controlled by an enterprise, is located in a third-party data-center operator's facility; is that still a private cloud? We think that it should be considered as such.

This type of cloud computing have many attractive features as in public cloud computing as for instance: elasticity and scalability, pay as you go computing, service level agreements, lower costs but in contrast it offers better solutions for downsides of cloud computing model such as: loss of control over enterprise and customer data, worries about security, and issues connected to regulatory compliance, etc. Private clouds aim to avoid these objections, while still offering many of the key benefits of public cloud computing.

[1] http://en.wikipedia.org/wiki/Managed_private_cloud

So some of the differences between public and private cloud offerings, as far as security goes, are going to be:

- Your control over who sees your data - with the public cloud, you don't know what employee at that company has access to your data. And it could be - typically these companies are very large, what controls do they have over the employees that can access your data. For a company that needs to be compliant in any way, that's not going to be acceptable at all.
- You also don't have any control over any of the firewall resources that you get. It's all done in a virtual environment. So, the changes that are made to the firewall could affect you, even though you didn't ask for those changes. Now, with a private cloud, as far as security is concerned, you control every aspect of it. Those firewalls are dedicated to you. The resources - you know who has access to those resources because it's your company. We don't, as far as Online Tech's private cloud is concerned, we don't access any of your data. It's all on you. With a public cloud, you don't get that.

At the same time we should mention that there are also some drawbacks of this type of private model. Everything comes with its price. The downside is private cloud ROI (return on investment): the organization implementing the private cloud is responsible for running and managing IT resources instead of passing that responsibility on to a third-party cloud provider. Another one is that some private cloud solutions have the capability to "cloud-burst" into a public cloud at peak times when additional resources are needed.

Nevertheless most of the researchers in this area think that even these obvious drawbacks, private cloud solution is worth to use due to the fact that a private cloud allows businesses significant cost savings over legacy hardware-based deployments. It also enables far greater flexibility, and – in contrast to a public cloud – much greater security and privacy.

Concerning the security issues of private clouds we can point out that the private cloud is built behind a firewall – so it is easier to control eventual attacks on data security. Many authors offer different ideas to improve security. We think that it is worth to point out the work presented by Thomas W Shinder[1] – MSFT: *Introducing A Solution for Private Cloud Security*, which in our opinion is covers most of the themes related to the private cloud security.

A Solution for Private Cloud Security includes the following core documents:

- A Solution for Private Cloud Security – Service Blueprint
- A Solution for Private Cloud Security – Server Design
- A Solution for Private Cloud Security – Service Operations References

In each document are given details about the service, the server design and service operations instructions.

***

[1] http://blogs.technet.com/b/privatecloud/archive/2012/01/20/introducing-of-a-solution-for-private-cloud-security.aspx

In a conclusion we can summarise that cloud computing is really a better alternative for providing firms and companies data processing services or/and data storage, than the traditional usage of information technology solutions. At the same time some important concerns about the increased security risks cannot be ignored. We think that one of the solutions which decrease the mentioned above risks is developing and implementing private cloud solutions due to the fact that most of the issues related to the security can be maintained and managed in a more flexible and effective way. But , of course, the final choice of the business organisations depends in grater extend on considering all issues related to implementing any IT solution, including economic factors such as, for instance ROI.

Literature:

1. Mell T., Grance T. The NIST Definition of Cloud Computing. September 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
2. Stamfor C. Gartner Outlines Five Cloud Computing Trends That Will Affect Cloud Strategy Through 2015. <http://www.gartner.com/newsroom/id/1971515>
3. Columbis L. Forecasting Public Cloud Adoption in the Enterprise. <http://www.forbes.com/sites/louiscolumbus/2012/07/02/forecasting-public-cloud-adoption-in-the-enterprise-2/>
4. Zhou M., Zhang R., Xie W. et al. Security and Privacy in Cloud Computing: A Survey. 2010 Sixth International Conference on Semantics, Knowledge and Grids. p. 106. <>
5. Messmer E. Ernst & Young's IT security survey shows struggle to control cloud computing, social media and mobile risks. NetworkWorld. <http://www.networkworld.com/news/2012/102912-ernst-young-cloud-mobile-263695.html>
6. What's Holding Back the Cloud? Intel Survey on Increasing IT Professionals' Confidence in Cloud Security. <http://www.intel.com/content/dam/www/public/us/en/documents/reports/whats-holding-back-the-cloud-peer-research-report2.pdf>
7. Tripathi A., Mishra A. Cloud Computing Security Considerations. <http://deca.cuc.edu.cn/Community/cfs-filesystemfile.ashx/__key/CommunityServer.Components.PostAttachments/00.00.00.70.95/Cloud-computing-security-considerations.pdf>
8. Morsy M., Grundy J., Müller I. An Analysis of The Cloud Computing Security Problem. APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.
9. Bhadauria R., Chaki R., Chaki N. et al. A Survey on Security Issues in Cloud Computing. <http://arxiv.org/pdf/1109.5388>
10. Qaisar S., Khawaja K. Cloud Computing: Network/Security threats and countermeasure. <http://www.journal-archieves14.webs.com/1323-1329.pdf>
11. http://blogs.technet.com/b/privatecloud/archive/2012/01/20/introducing-of-a-solution-for-private-cloud-security.aspx
12. http://en.wikipedia.org/wiki/Managed_private_cloud

MAIN THREATS IN CLOUD SECURITY

Prof. Dr. Dimiter G.Velev
Department of Information Technologies and Communications
University of National and World Economy – Sofia, Bulgaria

The paper gives a short overview of hot problems in cloud computing. In the beginning a brief introduction to cloud computing is presented. Main threats to cloud computing are summarized and described. Some recommendations for secure cloud operations are proposed.

1. A Brief Introduction to Cloud Computing

Cloud computing is an on-demand service model for IT provision implemented on virtualization and distributed computing technologies [1, 7, 8, 10]. Cloud computing providers deliver common business applications online as services which are accessed from another web service or software like a web browser while at the same time the software and data are stored on servers. The abstraction of computing, network and storage infrastructure is the foundation of cloud computing. Cloud computing removes the traditional application silos within the data center and introduces a new level of flexibility and scalability to the IT organization. This flexibility helps address challenges facing enterprises and IT service providers that include rapidly changing IT landscapes, cost reduction pressures, and focus on time to market.

Cloud users are identified as follows [1, 10]:

- Individual consumers;
- Individual businesses;
- Start-ups;
- Small and medium-size businesses;
- Enterprise businesses.

Cloud computing architectures offer to its users many advantages [7, 10]:

- Reduced cost since services are provided on demand with pay-as-you-use billing system;
- Highly abstracted resources;
- Instant scalability and flexibility;
- Instantaneous provisioning;
- Shared resources, such as hardware, database, etc.;
- Programmatic management through API of Web services;
- Increased mobility – information is accessed from any location.

The following cloud computing categories have been identified and defined [8, 10]:

- Infrastructure as Service (IaaS): provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service Application Programming Interface (API). IaaS includes the entire infrastructure resource stack from the facilities to the hardware

platforms that reside in them. It incorporates the capability to abstract resources as well as deliver physical and logical connectivity to those resources. IaaS provides a set of APIs which allow management and other forms of interaction with the infrastructure by consumers.

- Platform as a Service (PaaS): allows customers to develop new applications using APIs, implemented and operated remotely. The platforms offered include development tools, configuration management and deployment platforms. PaaS is positioned over IaaS and adds an additional layer of integration with application development frameworks and functions such as database, messaging, and queuing that allow developers to build applications for the platform with programming languages and tools are supported by the stack.
- Software as a Service (SaaS): is software offered by a third party provider, available on demand, usually through a Web browser, operating in a remote manner. Examples include online word processing and spreadsheet tools, CRM services and Web content delivery services. SaaS in turn is built upon the underlying IaaS and PaaS stacks and provides a self-contained operating environment used to deliver the entire user experience including the content, its presentation, the applications and management capabilities.
- Multi-Tenancy: the need for policy-driven enforcement, segmentation, isolation, governance, service levels and billing models for different consumer constituencies. Consumers might utilize a public cloud provider's service offerings or actually be from the same organization, but would still share infrastructure.

The cloud services can be implemented in four deployment models [1, 7]:

- Public Cloud - the cloud infrastructure is made available to the general public or large industry group and is owned by an organization selling cloud services.
- Private Cloud - the cloud infrastructure is operated entirely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises.
- Community Cloud - the cloud infrastructure is shared by several organizations and supports a specific community. It may be managed by the organizations or a third party, and may exist on-premises or off-premises.
- Hybrid Cloud - the cloud infrastructure is a composition of two or more clouds (private, community or public) that are bound together by standardized or proprietary technology that enables portability of data and application.

2. Main Threats in Cloud Security

As companies and organizations move their computing environments with their identities, information and infrastructure to the cloud, they must be willing to give up some level of control. In order to do so they must be able to trust cloud systems and providers, as well as to verify cloud processes and events. Important building blocks of trust and verification relationships include access control, data security, compliance and

event management, implemented with existing products and technologies, and extendable into the cloud.

The cloud security principles comprise three main categories: identity, information and infrastructure [2, 10]:

- Identity security - it keeps the integrity and confidentiality of data and applications while making access readily available to appropriate users. Support for these identity management capabilities for both users and infrastructure components is a major requirement for cloud computing and identity will have to be managed in ways that build trust. Identity security requires stronger authentication and stronger authorization.
- Information security - in the traditional data center, controls on physical access, access to hardware and software and identity controls all combine to protect the data. In the cloud, that protective barrier that secures infrastructure is diffused. The data needs its own security and will require data isolation, stronger data security, effective data classification, information rights management, governance and compliance.
- Infrastructure Security - IaaS application providers treat the applications within the customer virtual instance as a black box and therefore are completely indifferent to the operations and management of a applications of the customer. The entire pack (customer application and run time application) is run on the customers' server on provider infrastructure and is managed by customers themselves. For this reason it is important to note that the customer must take full responsibility for securing their cloud deployed applications.

The top threats to cloud computing can be summarized as follows (Fig.1) [5, 6, 9] :

- Data Breaches - Data Loss and Leakage;
- Account, Service and Traffic Hijacking;
- Abuse and Unallowed Use of Cloud Computing;
- Insecure Application Programming Interfaces;
- Malicious Insiders;
- Shared Technology Vulnerabilities.

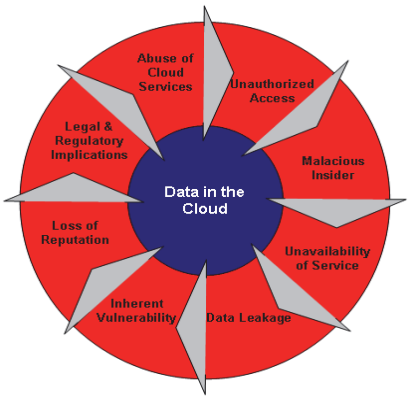

Fig.1 Priority Issues in Cloud Computing.

The following security compromises among the three cloud deployment models have been identified (Fig. 2) [3, 10]:

- SaaS provides the most integrated functionality built directly into the offering, with the least consumer extensibility, and a relatively high level of integrated security since at the least the provider bears a responsibility for the security.
- PaaS is intended to enable developers to build their own applications on top of the platform. As a result it tends to be more extensible than SaaS, at the expense of customer ready features. This tradeoff extends to security features and capabilities, where the built-in capabilities are less complete, but there is more flexibility to layer on additional security.
- IaaS provides few if any application-like features, but enormous extensibility. This generally means less integrated security capabilities and functionality beyond protecting the infrastructure itself. This model requires that operating systems, applications, and content be managed and secured by the cloud consumer.

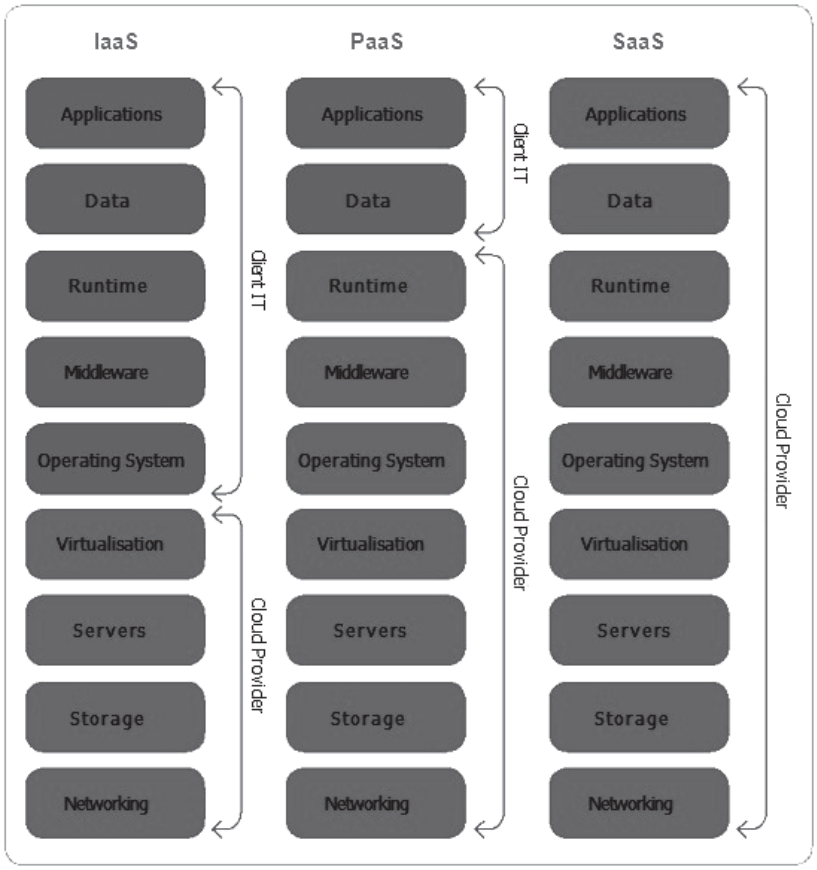

Fig. 2 Division of Responsibilities in Cloud Computing

Companies should define a pool of possible questions in order to evaluate the security approach of a certain cloud provider [4, 11]:

- Data security – type of data security technologies supported, prevention of mixing with other cloud users' data; provision of backup/restore services;
- Network security – provision of dedicated physical or virtual LANs to the clients, ability to define their own authorization and access control lists;
- Secure user access – means for provisioning secure access regarding clients, monitoring and reporting on usage and activities for audit purposes;
- Compliance - compliance certifications existence, compliance audit cycles, address requests for location-specific storage, preventing data from being moved to a non-compliant location;
- Virtual machine security - protocols for securing applications running on a virtual machine, securing virtual machines in the cloud, isolating one or a logical group of virtual machines from one other, clients' visibility into their virtual machines and servers running in their corresponding cloud, type of monitoring tools provided.

The immediate actions responding to the answers of such questions should be the implementation of a list of countermeasures [3, 6, 11]:

- Revision of the business goals;
- Maintenance of a risk management program;
- Creation of a security plan supporting company' business goals**;**
- Establishment of a corporate wide support;
- Creation of Security Policies and Procedures**;**
- Audit and Review;
- Continuous improvement.

3. Conclusion

The cloud offers a new efficient set of tools for control over complex data storage and its manipulation. However, there is quite a number of potential challenges, including security. Control over security, compatibility with existing systems, business continuity and compliance are the most commonly expressed concerns when organizations consider adopting a cloud-based strategy.

Security in a cloud environment requires a complex approach. The cloud provider plays an important role in securing both the cloud infrastructure and software. The provided cloud platform should comprise cloud hardware and software from leading providers and a cloud management system. The user interface should allow end users to configure their cloud-based solutions to meet their requirements.

References

1. Cloud Computing, http://en.wikipedia.org/wiki/Cloud_computing.
2. CSA: Security Guidance for Critical Areas of Focus in Cloud Computing, ver. 3.0. Cloud Security Alliance, 2011.

3. Dimension Data Cloud, Cloud Security: Developing a Secure Cloud Approach. http://www.codeproject.com/Articles/530421/Cloud-Security-Developing-a-Secure-Cloud-Approach/.
4. Grimes, D.: 7 Steps to Developing A Cloud Security Plan. https://blog.cloudsecurityalliance.org/2012/09/10/7-steps-to-developing-a-cloud-security-plan/.
5. Kalro, V., A. Parekh: Cloud Security & Threat, http://www.chmag.in/article/sep2010/cloud-security-threat/.
6. Krutz, R.L., R.D. Vines,: Cloud Security A Comprehensive Guide to Secure Cloud Computing. Wiley Publishing, Inc., 2010.
7. Reese, G.: Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. O'Reilly Media, Inc., (2009).
8. Rittinghouse, J.W., Ransome, J.F.: Cloud Computing: Implementation, Management and Security. CRC Press, 2009.
9. Samson, T.: 9 top threats to cloud computing security, http://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428.
10. Velev D., P. Zlateva, Cloud Infrastructure Security, IFIP conference, iNetSec 2010 "Open Research Problems in Network Security", 05-06 March 2010, Sofia, Bulgaria, Lecture Notes in Computer Science, J. Camenisch, V. Kisimov, M. Dubovitskaya (Eds.), Springer-Verlag, Berlin Heidelberg, vol. 6555, 2011, (140-148), ISBN: 978-3-642-19227-2 (Softcover), ISBN: 978-3-642-19228-9 (eBook).
11. Winkler, J.R.: Securing the Cloud Cloud Computer Security Techniques and Tactics. Elsevier Inc., 2011.

ДЕТСКАЯ ПОРНОГРАФИЯ В ИНТЕРНЕТЕ: ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ

Владимир Голубев
к.ю.н., доцент, Директор центра исследования компьютерной преступности

Подобно многих революционных технологий, глобальная сеть Интернет предоставляет огромные возможности как для прогресса, так и для злоупотреблений. Атаки в сети, мошенничества с пластиковыми платежными карточками, кражи средств из банковских счетов, корпоративный шпионаж, распространение детской порнографии - вот неполный перечень рисков и угроз негативной стороны Интернет.

Статистика показывает, что каждый пятый ребенок в возрасте от 10 до 17 лет, пользующийся Интернетом, с его помощью получил предложения сексуального характера от взрослых пользователей. Каждому четвертому ребенку, вступившему через чаты в переписку со взрослыми пользователями, были показаны картинки и фотографии порнографического характера.

Ежегодно растет и количество негативных интернет-ресурсовт. Так по данным Генпрокуратуры РФ, в настоящее время насчитывается более 7 тысяч террористических сайтов, где в подробностях учат, как сделать взрывчатку или совершить терракт. По данным американского исследовательского центра TopTenReviews, 12% всех сайтов (24,8 млн) содержат материалы для взрослых. Опасности подстерегают детей и в чатах. Существует тысячи мест в Интернете, где подростки могут бесплатно разместить свою web-страницу, а на ней - информацию о себе. К созданной однажды web-странице добавляется масса ссылок на другие подобные сайты, что, по сути, облегчает преступникам поиск потенциальных жертв.

Схема, по которой действуют Интернет-педофилы в поисках новой жертвы, проста. Преступники входят в детские on-line чаты, там знакомятся с детьми. Немного поговорив и расположив ребенка к себе, преступник назначает ребенку (подростку) персональную встречу - предлоги могут быть абсолютно разными. Чтобы простимулировать «жертву», педофил (или изготовитель детского порно) предлагает ребенку деньги или иное вознаграждение. Особенно быстро «клюют» на эту удочку детки из малообеспеченных семей и подростки, которым не хватает «карманных денег». Иногда в качестве вознаграждения ребенку предлагаются наркотики. Когда ребенок «попался в ловушку» - происходит встреча в «реале» и фотовидеосъемка.

Жертвой домогательств педофила ребенок может стать через web-камеру. Например, несколько чатов «Yahoo!» были закрыты из-за того, что их активно использовали педофилы. Через web-камеру они присылали подросткам в чатах свои фотографии в обнаженном виде. Жертвой таких «любителей детского внимания» могут стать подростки, на компьютере которых имеется web-камера. Еще одним прикрытием для развития детской порноиндустрии служат детские «модельные агентства».

Примеров тому много. Так, в 2004 году в Украине была обезврежена преступная группировка, которая под видом модельного агентства делала порноснимки и фильмы с участием девочек возрастом от 8 до 16 лет и размещала их на зарубежных порносайтах. «Моделями» в этом агентстве побывали полторы тысячи украинских девочек.

Студия, в которой проводились съемки, была арендована преступниками в центре Киева. Филиалы фирмы располагались в Харькове и Симферополе. Родителям девочек преступники рассказывали о том, что их дети занимаются модельным бизнесом. За час съемок девочкам платили от 50 до 200 гривен. Причем многие родители девочек знали или догадывались, чем занимаются их дети, однако никто в милицию не обратился. Так называемое модельное агентство существовало на протяжении трех лет. Рекламу на участие в съемках оно распространяло в СМИ, в том числе в газетах. По оперативной информации, чистый ежемесячный доход фирмы составлял около 100 тысяч долларов.

Необходимым условием эффективной борьбы с детской порнографией и педофилией в Интернете является ее законодательное определение. Разработка новой, эффективной системы противодействия и борьбы с детской порнографией в Интернете.

В борьбе с детской порнографией необходимо искать новые подходы, которые бы четко сформулировали меру ответственности изготовителей, распространителей и разного рода потребителей данной продукции. Задача эта трудная, потому что уголовное законодательство разных стран не имеет единых стандартов относительно детской порнографии и проституции.

Раскрытие данного рода преступлений чрезвычайно сложное дело, и даже когда они раскрыты, не всегда удается доказать состав преступления. Таким образом, любая страна с несовершенным законодательством является потенциальной целью для изготовителей и пользователей порнографии, особенно через систему Интернет.

ИСПОЛЬЗОВАНИЕ МЕТОДА ИНТЕРНЕТ-АНАЛИЗА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кавун С.В. к.т.н., доцент, Дашков А. В., студент
Харьковский национальный экономический университет, Харьков

В современном мире одной из проблем, свойственных практически любой области исследований, является выбор направления деятельности и/или актуальности и необходимости проводимых исследований (расчетов). Такая проблема может быть решена (а часто так и бывает) аналоговым или эмпирическим путем, т. е. она не имеет никакого математического и научного обоснования для выбора необходимых свойств. Но, в отличие от рассматриваемого метода, последний позволяет устранить указанные недостатки.

Описание метода Интернет-анализа (МИА, автора Кавуна С. В.) в области информационной безопасности и полученные результаты показаны в статье «A method of Internet-analysis by Tools of Graph Theory» [4]. Автор вышеупомянутой статьи применил МИА для анализа научной деятельности отечественных и зарубежных ученых в сфере информационной и экономической безопасности. Использование МИА базируется на языке запросов, который должен поддерживаться всеми поисковыми серверами и определяется формой самого запроса, что значительно упрощает его использование. Результаты использования МИА подтверждены экспериментами на множестве выбранных поисковых серверов (например, Google, Yandex, Yahoo и др.) и проанализированы на заданном интервале времени, это позволяет достичь объективности полученных результатов. Входными данными для МИА являются: множество объектов, в качестве которых рассмотрены персоны (с указаниями их фамилии, имени и отчества), множество категорий (совокупность терминов категориального аппарата сферы деятельности исследуемых ученых), период исследования (в годах или др. единицах времени), множество поисковых серверов.

Рассмотрим работу МИА в таких областях информационной безопасности, как правовые основы информационной безопасности (ПОИБ), формирование политики безопасности информационных систем (ФПБИС), защита интеллектуальной собственности (ЗИС), организационные меры в области информационной безопасности (ОМОИБ), тестирование и сертификация продуктов и услуг в области информационной безопасности (ТСПИБ), криптографические средства защиты информации (КСЗИ), оценка и управление рисками в информационных системах (ОУРИС), анализ информационных угроз и средств противодействия (АИУСП), аудит безопасности информационных систем (АБИС), расследование компьютерных преступлений (РКП), экономика информационной безопасности (ЭИБ), теневая информационная экономика (ТИЭ).

Результатом работы МИА является множество усредненных оценок (частотный анализ), по которому может быть определена «зона активности» в выбранном направлении деятельности, актуальность и востребованность исследований, количество публикаций авторов и их рейтинг в мировом научном сообществе. На основе данных множества усредненных оценок можно исследовать динамику их изменения, а так же актуальность категории в выбранном промежутке времени (табл. 1).

Таблица 1

Год	ПОИБ	ФПБИС	ЗИС	ОМОИБ	ТСПИБ	КСЗИ	ОУРИС	АИУСП	АБИС	РКП	ЭИБ	ТИЭ
2005	461	70	31500	50	51	152	58	51	80	432	55	8
2006	296	28	39400	10	9	275	23	8	39	228	38	4
2007	250	31	44300	21	22	275	29	21	41	331	37	4
2008	186	10	42700	8	7	337	20	7	33	258	29	3
2009	130	21	38200	6	7	77	10	6	23	261	30	4
2010	190	25	37600	8	9	63	19	8	29	956	43	5
2011	99	8	40300	6	6	69	9	6	26	279	26	6
2012	89	10	44200	7	8	339	18	7	24	405	26	4

Отчетливо видно, что направление защиты информационной собственности (ЗИС) наиболее популярно на данном временном интервале (рис. 1). Так же популярны области расследование компьютерных преступлений (РКП), правовые основы информационной безопасности (ПОИБ) и криптографические средства защиты информации (КСЗИ) (рис. 2).

Проведенный анализ полученных результатов отчетливо показывает популярность исследований и публикаций в области РКП в 2010 году, что происходило на фоне резкого спада интереса к области ТИЭ. О подобных связях или взаимосвязях можно только догадываться или проводить дополнительные исследования.

В данный момент метод Интернет-анализа применяется вручную и требует большого количество времени. Для более практичного и быстрого использования метода Интернет-анализа предлагается его автоматизировать, над чем сейчас работают авторы.

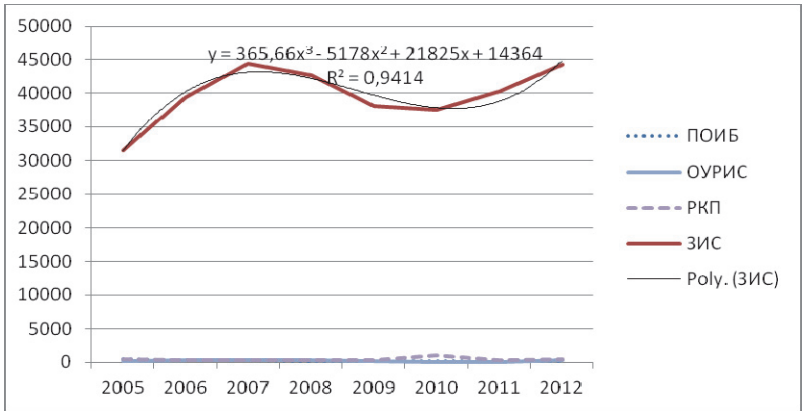

Рис. 1. **Распределение наиболее «популярных областей исследования»**

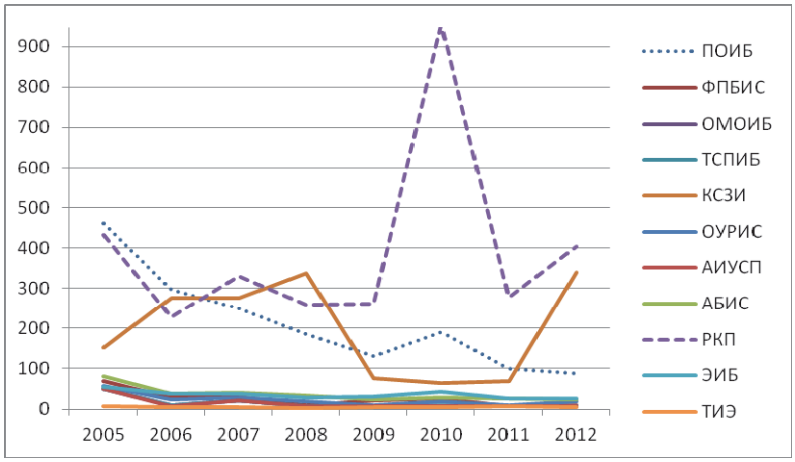

Рис. 2. **Распределение остальных областей исследования**

Литература

1. Кавун С. В. Анализ категорийного аппарата в сфере экономической и информационной безопасности / С. В. Кавун, И. В. Михальчук // Економіка розвитку: науковий журнал. – Харків: Вид. ХНЕУ, 2009. – № 3(51). – С. 9-14.
2. Кавун С. В. Информационная безопасность в бизнесе. Научное издание. – Х.: Изд. ХНЭУ, 2007. – 408 с.
3. Пономаренко В. С. Концептуальні основи економічної безпеки : монографія / В. С. Пономаренко, С. В. Кавун. – Харків : Вид. ХНЕУ, 2008. – 256 с.
4. Kavun S.V. A Method of Internet-Analysis by the Tools of Graph Theory / S.V. Kavun, I.V. Mykhalchuk, N.I. Kalashnykova, O.G.Zyma // En: Watada, J., Phillips-Wren, G., Jain, L.C., and Howlett, R.J. (Eds.), "Advances in Intelligent Decision Technologies", SpringerVerlag Series "Smart Innovation, Systems and Technologies", Vol. 15, Part 1, Heidelber, Germany, 2012, PP. 35-44.

ABOUT A FIVE TROUBLESOME IT SECURITY-ORIENTED PHRASES

Maciej Szmit
Corporate IT Security Agency,
Orange Labs, Poland
Roman Jašek
Faculty of Applied Informatics, Tomas Bata
University in Zlin, Czech Republic

The article is a try to discussion of a few specific IT security-related terms, with explanation what do they means, from where they were presumably borrowed and suggestion how they should be used (or why should not be used at all).

Introduction

One of the annoying issues in information security field is great number of dictionaries and methodologies, each of which contains its own specific vocabularies and definitions incompatible with the others. Most of IT security specialists prefer to use vocabulary from ISO/IEC 27k series (especially from ISO/IEC 27000:2009), but this series does not contain a few specific words relating to – for example – security management in IT projects and computer forensic, so specialists commonly use a few phrases borrowed from other standards or methodologies. But – as well as in the other areas – usage of non-clear defined terms causes troubles and misunderstandings1. Therefore this article is a try to discussion of a few of them, with explanation what do they means, from where they were presumably borrowed and suggestion how they should be used (or why should not be used at all).

Auditability

Auditability (ability to be audited) is used in at least three meanings:

1. Ability to check if the system or device working properly (well-defined and useful controls and metrics). The entity is auditable when one can check its functions in standardized ways and unambiguously stated if it is working properly or not.
2. Situation when another researcher can clearly follow the "decision trail" used by the investigator and could arrive at the same or comparable but not contradictory conclusions given the researcher's data, perspective, and situation (like intersubjective verifiability in science methodology)
3. Availability, completeness and reliability system logs, history files etc. This meaning can be used e.g. in computer crime investigation, when forensic specialist can rely on digital document contains information about particular resource usage.

[1] See e.g. [Korzeniowski 2012] p. 75.

The third meaning is rather unclear and may be ambiguous; especially that the auditability has at least two definitions in widely available standards, corresponding the first and the second meaning:

1. Understood to mean that it is possible to establish whether a system is functioning properly and, thereafter, that it has worked properly [OECD] http://stats.oecd.org/glossary/detail.asp?ID=5071
2. Possibility for an independent assessor or other authorized interested parties to evaluate the steps taken by a Digital Evidence First Responder and Digital Evidence Specialist (according to ISO/IEC 27037:2012-5.3.2).

Because of its ambiguity it seems to be a good idea to use term "auditability" in IT security-related context only with clear explanation in which sense the term is used. For instance ISO/IEC 27037:2012 explains that processes performed by Digital Evidence First Responder should be auditable, repeatable and defensible.

Imputability

Term "imputability" is used in criminal law and ethics, f.e. Code of Canon Law (Can. 1321 §1): "No one is punished unless the external violation of a law or precept, committed by the person, is gravely imputable by reason of malice or negligence". The imputability is not equal to responsibility - at least in law sense[1] - but it means possibility of being held accountable (for law violations, even if the side in not directly responsible for particular actions). In IT Security field the term "imputability" reigned in sense "possibility to assign unlawful action to appropriate person (especially based on digital evidence)". It seems to be a misunderstanding: there is well-defined term "accountability" in ISO/IEC 2382-8, which may be used in that context.

Risk mitigation

There are two definitions of „Risk Mitigation" term:

1. Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process (NIST SP 800-30 rev. 0),
2. Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process (CNSSI-4009).

The NIST 800-30 (rev. 0) meaning has been commonly used because ISO/IEC 27005 was published in 2008 and NIST SP 800-30 has been available since June 2002 (revision 1 was published at 2011 and CNSSI-4009 definition is included in the revision). In ISO/IEC 27000 the term "risk treatment" is used: "risk treatment process of selection and implementation of measures to modify risk" ISO/IEC 27000:2008-2.43.

There are two problems with "risk mitigation" term:

1. "Mitigate" means to became milder, lessen in force or intensity (as wrath, grief, harshness, or pain); moderate or to make less severe (e.g. to mitigate a punishment), to

[1] See e.g. Assanidze v. Georgia (The European Court of Human Rights, 71503/01, ECHR 2004-II).

make (a person or one's state of mind) milder or more gentle, but one of Risk Mitigation options in NIST SP 800-30 is Risk Assumption described as below:

- Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.

It may raise doubts if "accept the potential risk" can be named "risk mitigation"

2. The term "risk" is commonly used in the meaning "combination of the probability of an event and its consequence" (ISO/IEC 27000:2009-2.34) so there are a two possible ways for decreasing the risk: decrease the impact (consequences) of the event or decrease its likelyhood[1]. The second option is usually used less frequently, but is possible (for example: training employees reduces the likelihood that they commit an error). In the NIST SP 80-300 there are only one option of risk limitation: by implementing controls that minimize the adverse impact of a threat's exercising vulnerability. There is no explicit described way to reduce threat likelihood, there is only option "Research and Acknowledgment" as follows: "To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability".

Because of these two problems it seems one should prefer use "risk reduction" term form ISO/IEC 27005:2008.

Risk Transfer

Risk transfer is still one of variants of risk treatment in ISO/IEC 27001:2005 (as well as Risk Transference in NIST 80-300) but in ISO 31000:2009 it is replaced by risk sharing. ISO 31000:2009-5.5.1.f: „sharing the risk with another party or parties (including contracts and risk financing)". The term „risk sharing" seems to be better because of possibility of reverting the transferred risk to the first party (e.g. in case of problems with insurance policy) and taking into consideration a part of threat occurrence consequences (f.e. legal liability, especially criminal and administrative liability), which cannot be transferred.

It seems to be important to distinguish between the two cases and use appropriate term: risk transfer if whole risk is efficiently transferred or risk sharing if the risk is only decreased by sharing its potential consequences with the other entity.

Traceability

In logistics, traceability refers to the capability for tracing goods along the distribution chain and in metrology the term "measurement traceability" is used to refer to an unbroken chain of comparisons relating an instrument's measurements to a known standard (e.g. calibration to a traceable standard). There is also term "audit trail (in computer security)" in ISO/IEC 2882:8-08.06.07.

"Traceability" in IT security-related documents seems to sometimes be used in meaning forensics chain of custody traceability (see e.g. [Siti et. al 2011]). Interesting definition of traceability was published in ISO 8402:1995 ("The ability of trace the history, application or location of an entity, by means of recorded identifications"), but status of this standard is now withdrawn and this definition seems to be too narrow. The two other definitions uses "traceability" as follows:

[1] See ISO 31000:2009-2.25

1) Security Requirements Traceability Matrix (SRTM) – Matrix that captures all security requirements linked to potential risks and addresses all applicable C&A requirements. It is, therefore, a correlation statement of a system's security features and compliance methods for each security requirement. [CNSSI 4009]
2) Body of Evidence (BoE) – The set of data that documents the information system's adherence to the security controls applied. The BoE will include a Requirements Verification Traceability Matrix (RVTM) delineating where the selected security controls are met and evidence to that fact can be found. The BoE content required by an Authorizing Official will be adjusted according to the impact levels selected. [CNSSI 4009]

Because of these ambiguities it seems to be better use terms from ISO/IEC 27037:2012 listed above (auditability, repeatability, defensibility) in the context of chain of custody properties.

Abbreviations

CNSS - Committee On National Security Systems
IEC – International Electrotechnical Commission
ISO – International Organization for Standardization
NIST - National Institute of Standards and Technology
OECD - Organization for Economic Co-operation and Development

References

[CNSSI] 4009 CNSS Instruction No. 4009 National Information Assurance (IA) Glossary, April 2010, available at www: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
[ISO/IEC 27000] ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary, International Standard ISO/IEC 27000, rev.1, ISO/IEC 2009, available at www: http://standards.iso.org/ittf/licence.html
[ISO/IEC 27037] ISO/IEC 27037 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence, ISO 2012
ISO 31000 Risk management — Principles and guidelines International Standard ISO 31000, ISO 2009
[NIST IR 7298] NIST Glossary of Key Information Security Terms (rev. 1), Kissel R. (ed.), U.S. Department of Commerce, February 2011, available at www: http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf
[Korzeniowski 2012] Korzeniowski L. F.: Podstawy nauk o bezpieczeństwie, Diffin, Warszawa 2012
[NIST SP 800-47] NIST Special Publication 800-47 Security Guide for Interconnecting Information Technology Systems, Grance T., Hash J., Peck S., Smith J., Korow-Diks K., National Institute of Standards and Technology, August 2002, available at www: http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

[NIST SP 800-30] NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems, Stoneburner G., Goguen A., Feringa A., National Institute of Standards and Technology, July 2002, available at www: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (revision 0); available at www: http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf (revision 1)
[OECD] OECD Glossary of Statistical Terms http://stats.oecd.org/glossary/index.htm
[Siti et. al 2011] Traceability in Digital Forensic Investigation Process, Siti Rahayu S., Robiah Y., Shahrin S., Nor Hafeizah H., Mohd Faizal A., Zaheera Zainal A., [in] Proceedings of 2011 IEEE Conference on Open Systems, available at www: http://eprints2.utem.edu.my/254/1/06079259.pdf

SPAȚIUL CIBERNETIC - TEREN DE CONFRUNTARE

Ghenadie SAFONOV
Anatolie CALANCEA
Academia Militară a Forțelor Armate "Alexandru cel Bun"

Cyberspace has become a new environment of warfare (fifth after land, sea, air, space). It is obvious that all future conflicts will have a virtual component, either in the initial phase of the conflict, either as ordinar aggression, without carrying out other forms of battle. Based on this fact, every state should be prepared to deal with such threats.

I. Introducere

Implementarea activă şi multilaterală a tehnologiilor informaționale a determinat transformarea structurii societății mondiale, conducînd treptat spre dispariția frontierelor naționale. În toate domeniile de activitate au apărut noi structuri funcționale, la baza cărora se află rețeaua.

S-a creat spațiul informațional (cibernetic) global unic, în care s-a manifestat o confruntare geostrategică informațională între marile puteri, pentru atingerea superiorității în spațiul informațional mondial. Odată cu dezvoltarea şi sporirea complexității mijloacelor, metodelor şi formelor de automatizare a procesării informației creşte dependența societății de gradul de securitate a tehnologiilor informaționale utilizate, de care, uneori, depinde bunăstarea, iar uneori şi viețile multor oameni. [1]

Spațiul cibernetic a devenit un nou mediu de ducere a războiului (al cincilea după uscat, mare, aer, spațiu). Este evident faptul că toate conflictele în viitor vor avea o componentă virtuală, fie în faza inițială a conflictului, fie sub formă de agresiune în sensul direct al cuvîntului, fără desfășurarea altor forme de luptă.

În absența unor acorduri internaționale și a nedorinței de a conveni asupra normelor generale de interpretare a problemei, actorii cu intenții agresive posedă agilitate și flexibilitate în dezvoltarea și punerea în aplicare a potențialilor atacuri cibernetice. Acest

potențial fiind suficient pentru a fi categorisit drept armă. Iar odată ce există o armă, se va găsi și un război unde arma respectivă poate fi aplicată.

II. Amenințările cibernetice

Prin noțiunea de *amenințare cibernetică* se înțelege posibilitatea unui impact negativ asupra informațiilor de valoare sau asupra unui sistem de informatic. Realizarea unei astfel de amenințări reprezintă atac cibernetic, care la rîndul său înglobează în sine spionajul cibernetic, războiul cibernetic, terorismul cibernetic, precum și criminalitatea cibernetică. Autorii atacurilor cibernetice după motivele și rezultatele dorite pot fi clasificați în patru categorii:

- Hackerii amatori (hobbyiști);
- Grupe mici de hackeri;
- Organizații nonguvernamentale;
- Structuri de stat.

Fiecare dintre aceste grupuri desfășoară anumite tipuri de acțiuni care le caracterizează.

Grupurile mici de hackeri și hackerii amatori singulari (hobbyiștii) acționează din motive personale (răzbunare, dorința de a demonstra importanța sa), doresc a obține beneficii materiale sau pentru a confirma convingerile lor ideologice. Daune cauzate de atacurile lor sunt relativ mici, însă există pericolul angajării atît a grupurilor mici de hackeri, cît și a hackerilor talentați de către serviciile de informații sau grupuri de crimă organizată pentru soluționarea propriilor obiective meschine. Structurile negu-vernamentale prezintă cel mai mare pericol. În această categorie pot fi incluse:

- Corporațiile mari;
- Organizațiile teroriste;
- Crima organizată.

Aceste structuri posedă o ierarhie strict determinată și sunt capabili de a efectua atacuri complexe asupra infrastructurilor critice. Metodele utilizate preponderent sunt similare, diferența fiind numai în motivația atacurilor. Corporațiile sunt implicate în acțiuni de spionaj economic și sabotarea concurenților. Terorismul cibernetic, la rîndul său, amenință rețelele de calculatoare pentru a intimida guverne și oameni, forțînd luarea anumitor decizii. Crima organizată este motivată de posibilitatea obținerii cîștigului material. Toate acestea sunt în linii generale, în realitate relația între ele fiind mult mai complicată. De exemplu, grupurile teroriste pot utiliza atacurile virtuale pentru a obține finanțarea necesară, ca un mijloc de propagandă sau de comunicare. Toate cele trei tipuri de structuri folosesc hackeri talentați și grupuri de hackeri. [2]

Statul, la moment, este rar implicat în acest tip de acțiuni, deoarece nu poate fi garantat anonimatul, iar expunerea poate deteriora semnificativ relațiile bilaterale precum și imaginea la nivel internațional. Cu toate acestea, în categoria structurilor guverna-mentale pot fi incluse deja cele care sunt implicate în acțiuni de război informațional cu utilizarea rețelelor de calculatoare cum ar fi: operațiuni de informare, operațiuni psihologice și atacuri la scară largă asupra sistemelor informatice.

Principalele ținte ale atacurilor cibernetice la nivel național pot fi:

- Paginile web ale guvernului, organizațiilor politice și obștești, mass-media electronice;
- Sistemele ce deservesc comunicațiile importante dintre structurile puterii politice, factorii de decizie și structurile de forță;
- Sistemele de comunicații între diferitele niveluri ierarhice ale structurilor de forță;
- Sistemele de comandă cu procese periculoase de producție, sistemele de management a sistemelor de transport, sistemelor energetice.

Dacă în cazul acțiunilor hackerilor amatori acestea pot fi percepute ca un impediment, atunci spionajul economic, criminalitatea cibernetică, terorismul și războiul cibernetic necesită a fi luate în serios. În evaluarea amenințării se pot menționa două lucruri clar definite:

- Terorismul și criminalitatea cibernetică sunt cele mai des întîlnite amenințări, care, la moment, nu posedă un efect cinetic suficient și nu cauzează prejudicii fizice grave. Însă tehnologia atacurilor cibernetice se transformă dintr-un impediment într-o amenințare gravă la adresa sistemelor informaționale și a infrastructurii critice a țărilor.
- Statele suverane sunt jucători în spațiul virtual cu cel mai mare potențial periculos, deoarece pentru organizarea acțiunilor serioase de spionaj și sabotaj sunt necesare resurse, hotărîre și o relație "cost-beneficiu" prielnică pentru statul în cauză.

Ultimul deceniu a scos la iveală fenomenul conflictelor internaționale în domeniul informațiilor. Nu este important cine a fost agresorul în acest conflict, și cine este o victimă, indiferent dacă aceste războaie au fost regizate de către state sau comunități de hackeri. Cel mai important este că războaiele de amploare în spațiul virtual sunt realitate și nici un conflict de amploare nu este lipsit de componenta cibernetică. Unele state investesc deja resurse considerabile în dezvoltarea capacităților cibernetice, care pot fi utilizate în scopuri militare. După unele estimări, numărul statelor care posedă structuri cibernetice de luptă variază între 20 și 30.

Acest fapt nu este lipsit de o anumită logică, deoarece lupta cibernetică are mai multe avantaje:

- este asimetrică (disponibilă pentru statele sărace și indivizi);
- este relativ ieftină și cu efect rapid (trimiterea unui semnal prin rețea este mai simplă decît trimiterea unui contingent militar peste ocean);
- nu are încă o contramăsură eficientă pe plan juridic și politic (greu de identificat autorul atacului și gradul de răspundere).

III. Pregătirea pentru confruntare în spațiul cibernetic

Pentru a supraviețui în condițiile create, statul trebuie să ia măsuri de pregătire către eventualele lupte virtuale, pentru a dezvolta capacitățile sale cibernetice, care la rîndul său pot fi definite ca o combinație de factori, care permit eliminarea cu succes a amenințărilor cibernetice.

În scopul dezvoltării potențialului cibernetic statul trebuie să acționeze pe următoarele direcții principale:

A) la nivel de guvernare este necesar de:

- Doctrină, documentele normative (inclusiv cele internaționale);
- Prevenirea criminalității informatice (inclusiv desfășurarea cercetărilor științifice);
- Crearea instituțiilor academice de profil de stat;
- Sponsorizarea de către Guvern tehnologiilor informaționale;
- participarea la inițiative interstatale în domeniul tehnologiilor informaționale;
- Crearea structurilor specializate în securitatea cibernetică, echipelor de urgență - CERT (Computer Emergency Response Team);
- dezvoltarea potențialului de cercetare și militar.

B) în sectorul privat este necesar de:

- Sistem de învățământ în domeniul tehnologiilor informaționale, soft de securitate pentru calculatoare, studenți instruiți în țările avansate tehnologic;
- Capacități de producție de hardware și elaborare a software;
- Infrastructură pentru tehnologiile informaționale, rețeaua de cablu, numărul necesar de noduri și linii de comunicații;
- Accesul în bandă largă, disponibilitatea rețelei pentru public,
- Parteneriat în domeniul tehnologiilor informaționale;
- Sistem de management a proceselor în domeniul tehnologiilor informaționale (SCADA- Supervisory Control And Data Acquisition);
- Aportul corporațiilor internaționale în domeniul tehnologiilor informaționale;
- Companii de securitate în domeniul tehnologiilor informaționale;
- Hackeri în serviciul de stat.

În ultimii ani unele state (SUA, Germania, China, Rusia, Iran, India, Israel) și organizații (NATO) au creat structuri militare specializate în desfășurarea operațiunilor în spațiul virtual.

Există, de asemenea, și structuri guvernamentale non-militare cu acest profil. Adesea, ele sunt create pe lîngă centrele de comunicații guvernamentale. Bunăoară, pe lîngă Centrul de Telecomunicații Speciale Centrul din Moldova în 2010 a fost creat Centrul de asigurare a securității cibernetice. Acesta are misiunea de a asigura securitatea securității informaționale a instituțiilor de stat în spațiul cibernetic, prin colectarea și analiza informațiilor privind atacurile cibernetice, precum și luarea de măsuri urgente și eficiente în vederea protecției resurselor informaționale ale autorităților.

Structurile cibernetice pot fi clasificate după cum urmează:

- Unități pentru studiul problemelor și propunerea soluțiilor;
- Unități pentru realizarea securității cibernetice;
- Unități de colectare a datelor;
- Unități pentru realizarea atacurilor virtuale și diversiunilor.

Scopul principal al acțiunilor în spațiul cibernetic este realizarea și menținerea superiorității informaționale, fapt ce presupune folosirea la maximum a sistemelor de informaționale proprii concomitent cu dezorganizarea maximă a sistemului informațional al adversarului

Operațiile în spațiul cibernetic pot fi clasificate:

- Ofensive (Offensive Cyber Warfare);
- Defensive (Defensive Cyber Warfare);
- De cercetare – colectare informații (Cyber Warfare Intelligence).

Operațiile ofensive în spațiul cibernetic sunt destinate pentru rezolvarea următoarelor scopuri:

- Deconectarea temporară de la rețeaua de calculatoare a centrelor cheie ale infrastructurii de comunicații;
- Suprimarea operațiunilor și funcțiilor de calcul;
- Perturbarea funcționării și scoaterea din funcțiune a sistemelor automatizate de conducere și de comunicații;
- Denaturarea și falsificarea informațiilor, diseminare de informații false
- Scoaterea din funcțiune a sistemelor energetice, de management a transportului, obiectelor vitale de aprovizionare, capacităților industriale.

Operațiile defensive în spațiul cibernetic sunt menite să asigure funcționarea stabilă a sistemelor rețelelor informaționale în condițiile efectuării de către adversar a acțiunilor lupta în spațiul cibernetic. De asemenea din aceeași categorie fac parte operații de asigurare a securității informațiilor, prevenire a amenințărilor din spațiul cibernetic, de lichidare a consecințelor acestora, precum și de protecție, monitorizare, detectare și reacționare promptă la activitatea neautorizată în sistemele informaționale și rețelele de calculatoare.

În prezent există conceptul de ”apărare dinamică”, care prevede acțiuni cu caracter proactiv și de interzicere în afara a spațiului său cibernetic, în scopul contracarării amenințărilor emergente, precum și eliminarea potențialelor atacuri iminente. La mijloacele software de protecție cibernetică se atribuie însăși mijloacele de protecție (filtre, ecrane de rețea, soft antivirus), precum și mijloace de detectare a atacurilor cibernetice și reacționare. [2]

Cercetarea cibernetică se organizează și se desfășoară în scopul soluționării a două tipuri de sarcini:

- Cercetarea informațională (obținerea de informații din sistemele de calculatoare sau rețele informaționale și prelucrarea acestora cu ajutorul mijloacelor hardware și software);
- Cercetarea amenințărilor cibernetice (colectarea și sistematizarea datelor privind sursele potențiale de amenințări informatice, precum și amenințările înșiși).

Primul tip de sarcini se rezolvă prin intermediul aplicării unui set de măsuri coordonate de pătrundere în rețelele informaționale și calculatoarele organizațiilor guvernamentale și nonguvernamentale străine, precum și celor ce prezintă interes pentru

persoanele fizice. Soluționarea tipului doi de sarcini implică utilizarea de surse, tehnologii și tehnici inovatoare.

Reieșind din cele expuse mai sus o structură menită să activeze în spațiul cibernetic trebuie să fie constituită din cel puțin două elemente:

- Secția întîi - internă, destinată pentru analiza vulnerabilităților și amenințărilor, precum și pentru organizarea protecției sistemului informațional propriu;
- Secția a doua - externă, destinată pentru colectarea informațiilor și realizarea atacurilor și diversiunilor împotriva sistemelor informaționale ale adversarului.

Concluzii

Amenințările cibernetice au devenit un lucru obișnuit în societatea noastră. Ele devin tot mai frecvente, mai diverse și mai complexe reieșind din metodele tehnologice aplicate. Ignorarea lor a devenit imposibilă, deoarece informațiile au devenit un beneficiu absolut și vital, iar confruntarea în spațiul cibernetic duce la pagube economice și fizice considerabile.

Pentru contracararea cu succes a amenințărilor cibernetice este necesar a se concentra asupra următoarelor:

- Stabilirea unui cadru conceptual, instituțional (crearea sistemului național de securitate cibernetică, elaborarea legislației, dezvoltarea parteneriatului);
- Elaborarea programului național de dezvoltare a potențialului cibernetic (capacităților de prevenire, detectare și contracarare a atacurilor cibernetice, crearea unor structuri specializate, ridicarea nivelului de protecție, dezvoltarea producției produselor de profil);
- Consolidarea culturii de securitate informațională (informarea populației, instruirea adecvată a managerilor și a personalului tehnic);
- perfecționarea cooperării internaționale (la nivel de acte normative, schimburi de experiență, de protecție colectivă împotriva atacurilor de amploare).

Bibliografie

1. ***, „Securitatea informațională în contextul procesului de globalizare”, http://biblioteca-digitala-online.blogspot.com/2013/01/securitatea-informationala-in-contextul.html.
2. Игорь Завальский, ”Кибервойна: угрозы и защита”, Сборник докладов7-го симпозиума по вопросам безопасности Черноморского и Каспийского регионов, Одесса, 2012;

DEVELOPMENT OF UNIVERSITY INFORMATION SYSTEMS FOR RESEARCH PROJECTS

Asst. Prof. Plamen Milev, PhD
University of National and World Economy – Sofia,
Department of Information Technologies and Communications

The paper examines information management system for scientific projects. The system was developed and implemented at the University of National and World Economy - Sofia. The paper examines the main stages through which goes the application process of the project proposal and its key elements.

1. Introduction

Economic growth and the increasing application of research and applied projects necessitate the development of advanced software applications for project management. Using possibilities for electronic application and reporting of research projects can give several results:

- Availability of updated information on the project proposals;
- Each applicant can track the status of owned project;
- Facilitated formation of inquiries about submitted project proposals;
- Opportunities for electronic reporting of project costs;
- Opportunities for managing the schedule of each project;
- Opportunities for managing budgets and funds.

2. Milestones in the development of software application for managing research projects

The main stages through which go the preparation of the project proposal and project management are given in Figure 1.

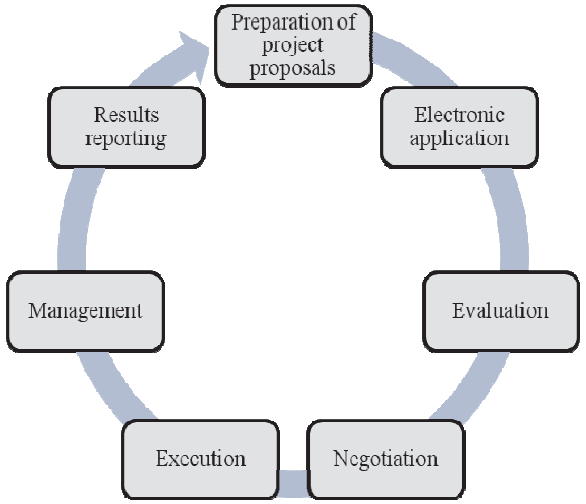

Figure 1. **Stages of application and reporting of the university research projects**

In 2012, the University for National and World Economy – Sofia (www.unwe.bg) developed and implemented a system to manage their university research projects. Home screen of this system is shown at Figure 2. There are two main types of project proposals – scientific research and scientific activity like conference, symposium, etc.

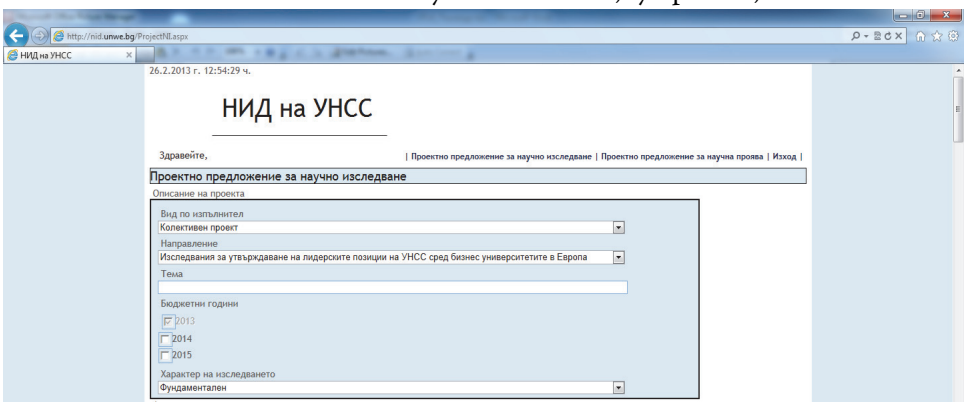

Figure 2. **System for scientific projects of University of National and World Economy – Sofia**

3. Key elements of the project proposal

Project proposals have several basic components:

- Description of the project;
- Summary, which describes the analysis of the state of research on the issue prior research objectives and content of scientific work, working hypotheses, expected results, etc.;
- The planning of the project, describing the main stages of project development and operations of each of them;
- Preliminary financial allocation – required data on the amounts by year of implementation of the proposal for the research;
- Plan cost estimate of the project is submitted budget version of the project in years;
- Composition of the research team.

There are three main groups involved in the approval process of the project proposal:

- Project owners – users of this role have the rights to submit project proposals and for each stage of the project to introduce and edit data in the project. All the adjustments and corrections are only possible within the university regulations.
- Reviewers – these users have access to certain projects and possess the possibility to give reviews, including text reasoning, numerical estimates and conclusions on the projects.
- Members of the research board – users of this role have access to all the records in project proposals and also to the reviews of the projects. Their rights include rating and ranking of the projects, negotiation and acceptance of reports.

4. Conclusion

Finally, it should be pointed out that crucial for building a knowledge-based economy is to expand the scope of application of information technologies, including information technologies in education. This project achieves its primary objective of improving the quality of management of education.

НОСИТЕЛИ ИНФОРМАЦИИ И УТЕЧКА ДАННЫХ: АНАЛИЗ МЕЖДУНАРОДНОГО ОПЫТА.

Брединский Анатолий
Г.У.Ф.И.С. РМ. старший лектор

One of the key problems of information protection is protection of devices with confidential data. The process must be based on the complexity principle: protection of devices has to be performed as a unified system of measures. Such an approach aims to prevent and neutralize possible threats by means of all resources available as an integrated whole.

Введение.

Общеизвестно, что информация находит свое отражение через материальные носители, которые могут быть представлены как в аналоговой, так и в цифровой форме. В качестве носителей могут выступать бумага или иной материал, на котором ведется запись, предметы или материалы, с которых могут воспроизводиться звуки, изображения или записи с помощью иного предмета, или механизма, любой иной регистратор информации, появившийся в результате технического прогресса.[1, ст. 3.]

Одной из важнейших проблем защиты информации является защита носителей содержащих конфиденциальные данные. При этом данный процесс должен базироваться на принципе комплексности [2, стр. 12.], т.е. защита носителей должна осуществляться как единая совокупность мер направленных на предотвращение и нейтрализацию возможных угроз, с применением всех имеющихся сил и средств, как единого целого.

Утечки информации в результате утери носителей: анализ международного опыта.

С учетом того, что носители информации часто содержат сведения, составляющие коммерческую, банковскую, следственную или государственную тайну их защите должно уделяться первостепенное значение, а сама система включать такие направления как – работа с субъектами доступа к информации, инженерно-техническая защита помещений, где хранятся носители, криптографические и иные формы защиты информации и ряд других. Однако, анализируя международную практику, мы можем придти к парадоксальным выводам – нередко утечка информации с материальных носителей происходит не в результате неких

злонамеренных действий, а как следствие халатности и непрофессионализма лиц, имеющих к ним доступ.

В качестве доказательства данному тезису можно привести многочисленные случаи из мировой практики. А именно: в 2004 году в Великобритании автомобилист, недалеко от международного аэропорта "Хитроу", подобрал папку с информацией об объектах в аэропорту, которые в первую очередь могут подвергнуться атаке террористов. Согласно его утверждению тетрадь с этой информацией была найдена им по дороге в аэропорт.[3]

В 2008 году британская полиция списала и отправила на утилизацию компьютер. По стечению обстоятельств в нем оказался носитель с конфиденциальными данными: именами, званиями, адресами и номерами телефонов сотрудников полиции британских графств Девон и Корнуолл. Сотрудник центра утилизации отходов, обнаруживший данную информацию проявил свой гражданский долг и вернул носитель сотрудникам полиции. В августе того же года, один из сотрудников Скотленд-Ярда выбросил флеш-карту с данными о сотнях тысяч заключенных. Сотрудники Королевской налоговой и таможенной службы Великобритании в 2007 году сначала потеряли личные данные 25 миллионов британцев, получающих детские пособия, а затем носитель с информацией о шести с половиной тысячах пенсионеров.[4]. Агентство по лицензированию водителей и автомобилей потеряло диски с информацией о шести тысячах британцев и их машинах (включая модель, цвет, номер). А Национальная служба здравоохранения Великобритании "куда-то дела" диски с личными данными сотен тысяч пациентов и историями их болезней. Житель Оксфорда Эндрю Чапмен, сам того не подозревая, приобрел за 60 долларов базу данных, за которую на черном рынке отдали бы несколько миллионов. Компьютер, купленный на интернет-аукционе, содержал личные данные клиентов-миллионеров Королевского банка Шотландии. В том числе сведения о счетах, номера мобильных телефонов, девичьи фамилии матерей (наиболее распространенный идентификационный контрольный вопрос) и даже подписи клиентов банка. В ноябре 2010 года Минобороны Великобритании подтвердило информацию о продаже на интернет-аукционе «eBay» ноутбука с секретной информацией о военной операции в Афганистане. В холе расследования выяснилось, что виновник этого, британский офицер — капитан Роберт Саджен. Он разбил ноутбук молотком и пребывал в полной уверенности, что уничтожил информацию. Но жесткий диск компьютера не пострадал. Всего за 18 фунтов неизвестный покупатель получил доступ к сотням фотографий из зоны ответственности британцев в афганской провинции Гельменд, данным о военных частях, складах боеприпасов, маршрутах патрулирования местности. [5] Специалисты по компьютерной безопасности отмечают, что хранение секретных данных на личном ноутбуке — грубейшее нарушение правил информационной безопасности. При этом министерство обороны Соединенного Королевства сообщило, что за четыре года британские военнослужащие потеряли в общей сложности более семисот ноутбуков с секретной информацией. Не лучшим образом обстоит ситуация и в специальных службах США, так например, ФБР признало, что за срок с 1996 года сотрудники

потеряли 184 компьютера, по поводу 13 из них существует подозрение, что они украдены. Три пропавших ноутбука содержали секретную информацию. Проверка проведенная в Национальном Космическом Агентстве США (NASA) целью которой было выявление устаревшего оборудования выявила, что нередко на информационных носителях предназначенных для списания находиться секретная информация, стоимость которой может измеряться в миллионы долларов США. Нарушения безопасности были выявлены во многих подразделениях NASA, включая те из них, что составляют основное «тело» этого агентства. Например, на некоторых жестких дисках старых ПК нашлись куски информации о программе создания «Шаттлов». Да, информация немного устарела, но актуальности не потеряла. Стоит отметить, что та же проверка выявила только в одном случае продажу более десятка б/у компьютеров и ноутбуков, на жестких дисках которых содержалась чрезвычайно важная, хоть и фрагментированная информация о космической программе США. Нет нужды говорить, что эта информация засекречена настолько, насколько это возможно. В Голландии, в интернете, были выложены документы Голландской королевской пограничной службы под грифом "совершенно секретно". Номера телефонов и записи разговоров один из сотрудников погранслужбы "случайно" разместил на одном из сайтов. Похожая история произошла в 2005 году в Германии. Студент из Потсдама за 20 евро купил компьютер, на жестком диске которого обнаружил подробные сведения о полицейских операциях, связанных с освобождением заложников.В Министерстве внутренних дел РФ, в 2008 году, была выявлена пропажа двух сейфов с секретными оперативными документами департамента уголовного розыска. В ходе проведенного расследования было установлено, что во время ремонта, который проводился в служебных помещениях, сейфы с секретной информацией были сначала помещены в коридор, где находились без контроля. А в последующим они были по ошибке приняты строителями как списанные и отправлены в пункт прима металлолома. Судьба документов установлена не была.

Вышеуказанные примеры позволяет нам утвердиться во мнении, что нередко опасность утечки таиться не там, где ее обычно ждут – в действиях третьих лиц, а в несоблюдении субъектами элементарных мер безопасности, при этом можно предположить, что часть лиц оперирующих с носителями информации не владеют даже элементарными знаниями о защите информации. В большинстве случаев система защиты присутствует только формально не осуществляя текущий оперативный контроль, а реагируя лишь постфактум, после обнаружения факта утечки.

Выводы.

Таким образом, можно сформировать следующие выводы:

1) На многих предприятиях оперирующими секретными или конфиденциальными данными информационная безопасность лишь декларируется, но фактически не реализуется.
2) Как правило столь плачевная ситуация складывается в результате отсутствия системного подхода к защите информации. В связи с этим одним из базовых шагов по защите является выработка концепции

безопасности информации, с последующей реализацией необходимых мер квалифицированными специалистами

3) Важнейшим вопросам остается надлежащая работа с субъектами, имеющими доступ к конфиденциальной информацией. Эти лица, перед получением соответствующего допуска должны, в обязательном порядке, проходить предварительную проверку, с последующим обучением их мерам информационной безопасности. При этом данный процесс не должен быть разовым и эпизодическим, а реализовываться постоянно путем оперативного текущего контроля со стороны специалистов в области безопасности.

Библиография:

1) Закон Республики Молдова «О доступе к информации» Nr. 982 от 11.05.2000.
2) Ярочкин В. "Информационная безопасность" учебник. М.: Акад. проект, 2004. - 381 с
3) Степанов Г. «Сверхсекретный план охраны аэропорта "Хитроу" найден на обочине дороги» Газета "Известия" от 9 июля 2004.
4) "Британские "налоговики" потеряли конфиденциальные данные о 25 миллионах граждан" Российская газета от 22.11.2007
5) «На аукционе продали ноутбук с военными тайнами Великобритании» http://www.km.ru/news/na_aukczione_prodali_noutbuk_s_v (доступ 22.02.2013)
6) Виноградова Е. "ФБР потеряло 184 ноутбука с секретной информацией" http://netoscoup.ru/news/2001/07/18/2926-print.html (доступ 21.02.2013)

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ РЕСУРСОВ В ПРОЦЕССЕ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИЙ НАУЧНО-ОБРАЗОВАТЕЛЬНОЙ СФЕРЫ

Ольга Пугачева,
УО «Гомельский госуниверситет им.Ф.Скорины»

Мировой и передовой отечественный опыт показывает, что в современной конкурентной борьбе идет соревнование не столько за обладание капитальными ресурсами и материальными ценностями, сколько за способность к разработке и использованию эффективных нововведений технологического, организационного и коммерческого характера.

Важное место в коммерциализации знаний как неосязаемых **интеллектуальных ресурсов** (ИР) организации занимает научно-образовательный сектор республики поскольку:

- в этой сфере сосредоточен значительный кадровый и научно-технический потенциал, генерирующий большое количество результатов научно-технической деятельности;
- на базе образовательных и научных учреждений, а также научно-инновационных предприятий идет процесс формирования учебно-научно-инновационных комплексов, способных обеспечить весь инновационный цикл - от идеи до создания конечного продукта (технологии) и распространения его на рынке, а также подготовку кадров для этой сферы;
- в системе сформирована инновационная инфраструктура, включающая технопарки, маркетинговые центры, центры трансфера технологий, научно-инновационные подразделения и др., которая призвана способствовать передаче завершенных результатов научно-технической деятельности из научно-образовательной сферы в предпринимательский сектор;
- вузы и научные организации постепенно интегрируются в международное научно-техническое сообщество и предпринимают активные попытки выйти на рынки наукоемкой высокотехнологичной продукции и услуг [1].

В целях успешной реализации инновационного потенциала научно-образовательной сферы необходимо эффективное управление ее интеллектуальными ресурсами.

В настоящее время к основным интеллектуальным ресурсам в научно-образовательной сфере могут быть отнесены: средства индивидуализации – бренды, товарные знаки и заявки по ним; интеллектуальные ресурсы, связанные с инновационной деятельностью,- патенты на изобретения, полезные модели, промышленные образцы и заявки по ним; компьютерные программы и базы данных; интеллектуальные ресурсы, характерные для отдельных видов деятельности – лицензии на вид деятельности; доменные имена, которые требуют разработки и ведения электронного реестра собственности организации.

Примером формализованного и официально охраняемого знания являются результаты научно-технической деятельности (НТД). Они включают как результаты работ по договорам о проведении исследований и разработок в соответствии с техническим заданием, которые официально приняты заказчиком, так и результаты инициативной творческой деятельности, которые формально не включены в техническое задание и в отчетную документацию, но получены исполнителем. Все это – новые знания или результаты интеллектуальной деятельности, размещенные на материальном носителе в форме оригинальной информации, которая является нематериальным объектом (таблица 1) [2].

В организациях научно-образовательной сферы наблюдаются следующие проблемы использования всех видов интеллектуальных ресурсов и проблемы ИР, связанные с интеллектуальной деятельностью:

- бизнес-проблемы, относящиеся к сфере ответственности осуществления бизнеса (связанные в основном с использованием данных ресурсов);

- правовые проблемы, обусловливающие регистрацию ресурсов и обеспечение их правовой защиты;
- управленческие проблемы, определяющие учет ресурсов, принятие решений (таблица 2) [2].

Таблица 1

Интеллектуальные ресурсы организации

Характеристика	Результаты научно-технической деятельности	Результаты интеллектуальной деятельности	Опыт сотрудников
Определение	Знание, представленное в отчетной документации	Знание, представленное на материальном носителе, не вошедшее в отчеты по договорам на НИОКР	Знание не выражено на материальном носителе, но может быть использовано
Примеры	Отчеты, комплект конструкторской документации	Статьи, результаты исследований, описание процессов, технических решений	Профессиональные навыки, творческий потенциал
Методы правовой охраны	Патентное, авторское, смежное право, служебная и коммерческая тайна		Соглашение между работником и работодателем

Таблица 2

Проблемы в области использования интеллектуальных ресурсов

Бизнес-проблемы	Правовые проблемы	Управленческие проблемы
Общие проблемы для всех видов ИР		
а) нет координации при создании, защите и эксплуатации ИР; в том числе и на уровне направлений ее бизнеса. б) недооцениваются существующие передовые технологии и опыт управления ИР, находящиеся вне сферы организации; в) сделкам для ИР уделяется недостаточное внимание	а) организации не следят за сроками поддержания ресурса в силе; б) мониторинг нарушений собственных прав и прав третьих лиц за пределами компании ведется нерегулярно	а) организации не имеют полной информации о существующих ИР, степени их защищенности, об использовании и ценности, из-за чего не принимаются адекватные решения, снижается ценность ИР; б) отсутствуют специалисты, способные решать весь комплекс проблем
ИР, связанные с инновационной деятельностью		
а) недостаточное финансирование собственных разработок; б) часто отсутствует координация разработок и они ведутся разрозненно; в) недостаточно эффективно используются инновации и разработки; г) изобретательская деятельность стимулируется слабо	а) слабо урегулированы взаимоотношения между работником и работодателем при определении авторского вознаграждения за объект интеллектуальной собственности; б) мониторинг нарушений собственных исключительных прав, нарушений прав третьих лиц, а также обеспечения патентной чистоты разработок ведется без необходимой периодичности	а) отсутствие учета возникающих ИР по всей цепи: от НИОКР до конечных продуктов; б) слабое выявление охраноспособных технических решений, а также решений о целесообразности получения охраны для дальнейшего использования этих изобретений; в) вывод интеллектуальной собственности за пределы организации контролируется нечетко; г) отсутствуют регламентирующие документы, устанавливающие практику принятия решений

Права на результаты исследований и разработок отражаются в договорах на НИОКР, в договорах между работодателем и работником по вопросам интеллектуальной собственности (ИС), в договорах о передаче права на подачу заявки, в соглашениях между соавторами, а также в лицензионных договорах и договорах уступки. Отсутствие договоров или неоднозначность в трактовке их положений – наиболее распространенная причина разногласий и споров. Поэтому важным является урегулирование трудовых отношений с работниками, создающими ИС, по следующим направлениям:

- их авторскому вознаграждению в соответствии с требованиями законодательства и организации;
- изменению должностных инструкций и профилактике нарушений авторских прав;
- предотвращению вывода ИС (изобретений, промышленных образцов, полезных моделей, научных публикаций) за пределы организации.

Следует отметить, что предотвращение вывода ИС за пределы организации связано с построением системы управления ИР с помощью бизнес-процессов по выявлению ИР и принятию решений о патентовании, а также стимулирования изобретательской и рационализаторской деятельности.

В соответствии с Законом от 5.01.2013 г. № 16-З «О коммерческой тайне» [3] в организациях для сведений, попадающих под его действие, должен быть установлен режим коммерческой тайны, который, в частности, предполагает оформление соглашения о конфиденциальности с работником. Его заключению должны предшествовать действия, направленные на формирование режима, в том числе: определение состава сведений, подлежащих охране; ограничение доступа к коммерческой тайне; учет лиц, получивших доступ к коммерческой тайне; применение не запрещенных технических средств и методов защиты информации.

Анализ состояния и развития системы управления интеллектуальными ресурсами университета в 2005-2012 гг. показывает стабильный рост основных показателей оценки результатов научно-технической и творческой деятельности. Об этом свидетельствуют данные, характеризующие число поданных заявок и полученных патентов на ОПС, изданных монографий, учебников, учебных пособий и других достижений (таблицы 3 и 4).

Таблица 3

Использование объектов авторского права

Годы	Использование научных разработок в учебном процессе (издание монографий, учебников и учебных пособий)
2005	320
2006	197
2007	256
2008	214
2009	157
2010	153
2011	121
2012	46

Таблица 4

Сведения о поданных заявках и полученных патентах на объекты промышленной собственности (ОПС)

Годы	2005	2006	2007	2008	2009	2010	2011	2012
Количество поданных заявок на ОПС	14	10	3	9	7	11	7	17
Количество полученных патентов на ОПС	8	19	21	11	9	4	6	8

Дальнейшее совершенствование инновационной деятельности на основе использования интеллектуальных ресурсов и развития инноваций закладывает фундамент роста и благосостояния экономики страны.

Литература

1. Нечепуренко, Ю.В. Управление интеллектуальной собственностью в научно-образовательной сфере / Ю.В. Нечепуренко.- Минск: БГУ, 2009.- 239 с.
2. Зинов, В. Г., Лебедева Т.Я., Цыганов С.А. Инновационное развитие компании: управление интеллектуальными ресурсами: учебное пособие / Под ред. В.Г.Зинова.- М.: Издательство «Дело» АНХ, 2010.- 248 с.
3. Национальный правовой интернет- портал РБ» [Электронный ресурс] / Нац. Центр правовой информ. Респ. Беларусь. - Режим доступа: http://pravo.by – Дата доступа: 29.01.2013

The carried out analysis of intellectual resources in the course of innovative activity of the organisations of scientifically-educational sphere allows to formulate experience and the basic problems of their use.

IMPORTANCE OF PROVIDING INFORMATION FOR CONDUCTING EFFECTIVE LOCAL ADMINISTRATIVE POLICY

Chief Asst. Prof. Katia Strahilova, PhD
University of National and World Economy – Sofia,
Department of Public Administration and Regional Development

The paper discusses the implementation of local administrative policy and the role of information technologies. The paper examines the basic questions of the construction of municipal computer information systems and problems of this process.

1. Introduction in local administrative policy

Municipalities in Republic of Bulgaria are a major local authority. As such they have separate budgets and their own policy on infrastructure, local services, health and education. Nowadays the question for the development of new administrative services is

an essential issue, including electronic services. For these reasons below we present the main issues of the use of information technologies for local administration and implementation of local administrative policy.

2. Information technologies in municipalities

From the point of view of the contractor process for deciding on investments in information technologies goes through the following stages:

- Identification of information needs and definition of information problem;
- Definition of the purpose and scope of the system and preparation of reference;
- Evaluation of economic efficiency (for private sector organizations – by assessing the financial impact in public organizations by assessing the public benefit);
- Development of the system.

The sequence of these actions can be developed as a corresponding sequence (Figure 1).

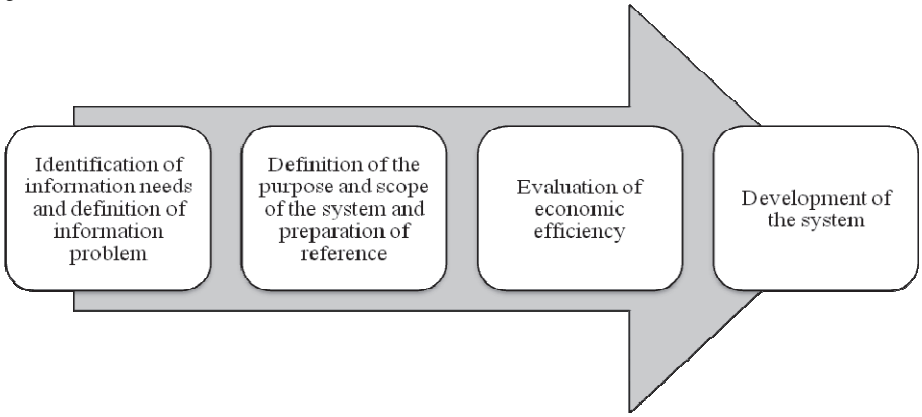

Figure 1. **Development of information solutions in municipalities**

As can be seen from the illustrated stages in the process, the evaluation phase of economic efficiency has an important place and role. This process shows whether the building the system is economically justified. Economic efficiency of investment in information and communication technologies is associated with the risk assessment and the likelihood computerized information system not to be programmed and implemented, or not to implement its functionality. Typically, investment decisions are made based on estimates, which are based on historical data from past periods. The implementation of investments in information and communication technologies is made in the above described sequence, depending on economic conditions and the behavior of individual actors. Therefore, each project has the opportunity to obtain different results than expected from the investment. Analysis of the risk of obtaining negative results in the literature is called analysis of investment risk. It is designated as a valuation uncertainty to obtain the expected results of the investment and quantitative analysis. The risk in evaluating investments in information and communication technologies for local administrative policy should be primarily analyzed at four stages (Figure 2).

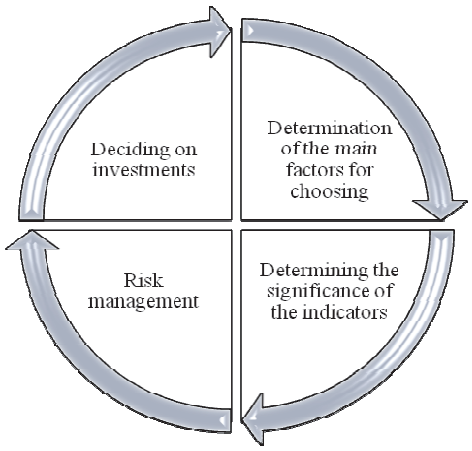

Figure 2. **Stages in the evaluation of investments in information and communication technologies for local administrative policy**

The main factors that affect the implementation of IT projects in local administration are:

- Experience in the work of the contractor;
- Time factors;
- Financial conditions;
- Legislative requirements;
- Macroeconomic factors and others.

3. Conclusion

Finally, it should be noted that the information technologies are important in order to have an effective local administrative policy and so are the role of risk analysis and return in the process.

ФОРМАЛИЗАЦИЯ ПРИНЦИПОВ КЛАССИФИКАЦИИ ЭКОНОМИЧЕСКИХ РИСКОВ

Ирина Балина, Славянский университет

Explores issues of formalizing the principles of classification of economic risks, given the major risks, and the next decade 2013

Под риском будем понимать возможную опасность потерь, вытекающую из специфики тех или иных явлений природы и видов деятельности человеческого общества. При исследовании формализации принципов классификации экономических рисков будем исходить из того, что риском можно управлять, т.е.,

использовать меры, позволяющие в определенной степени прогнозировать наступление рискового события и принимать меры к снижению степени риска. Основой функционирования эффективной системы управления экономическими рисками становится их классификация.

Под классификацией риска следует понимать распределение риска на конкретные группы по определенным признакам для достижения поставленных целей.

Научно-обоснованная классификация риска позволяет четко определить место каждого риска в их общей системе. Она создает возможности для эффективного применения соответствующих методов, приемов управления риском.

Согласно классификация Шеремета А.Д., Щербакова Г.Н. экономические риски различают по виду отношения к внутренней и внешней среде банка. Достоинством классификации является создание определенной системы рисков, включающей отдельные разновидности риска, а за основу принимается деление рисков на внешние и внутренние. Это позволяет разделить риски, возникающие вне банка, и оказывающие влияние на операционную деятельность банка и риски, возникающие внутри банка, в процессе осуществления банком своей «производственной» деятельности. Это коренное отличие двух классов рисков определяет отношение к ним со стороны банков, способы контроля и возможности управления. [5, с. 125-127]. Согласно указанной классификации риски по виду отношения к внутренней и внешней среде банка классифицируются следующим образом:

Внешние:

- риски, связанные с нестабильностью экономического законодательства и текущей экономической ситуации, условиями инвестирования и использования прибыли;
- внешнеэкономические риски (возможность введения ограничений на торговлю и поставки, закрытия границ и т.д.);
- возможность ухудшения политической ситуации, риск неблагоприятных социально-политических изменений в стране или регионе;
- возможность изменения природно-климатических условий, стихийных бедствий;
- колебания рыночной конъюнктуры, валютных курсов и т.д.

Внутренние:

- связанные с активными операциями (кредитные, валютные, рыночные, расчетные, лизинговые, факторинговые, кассовые, риск по корреспондентскому счету, по финансированию и инвестированию и др.);
- связанные с обязательствами банка (риски по вкладным и депозитным операциям, по привлеченным межбанковским кредитам);
- связанные с качеством управления банком своими активами и пассивами (процентный риск, риск несбалансированной ликвидности, неплатежеспособности, риски структуры капитала, левереджа, недостаточности капитала банка);

- связанные с риском реализации финансовых услуг (операционные, технологические, риски инноваций, стратегические, бухгалтерские, административные, риски злоупотреблений, безопасности) [5, с. 130].

При рассмотрении различных подходов к классификации рисков нельзя не отметить морфологическую таблицу рисков коммерческого банка (см. фигуру 1.), предложенную Савинской Н.А. [6, с. 89-91], которая может использоваться для создания информационно-аналитической базы системного определения и исследования банковских рисков.

Морфологическая переменная	**Виды риска**		
1. Логистика связей (тип потока)	1.1. Материальный	1.2. Финансовый	1.3. Информационный
2. Тип процесса	2.1. Инновационный	2.2. Инфраструктурный	2.3. Производственный
3. Место в системе	3.1. На выходе	3.2. В процессе	3.3. На выходе
4. Субъективный фактор	4.1. Индивидуальный	4.2. Коллективный	

***Фиг. 1.* Морфологическая таблица рисков коммерческого банка**

Источник: Савинская Н.А. [7, с. 90]

Такая классификация позволяет определить источники и виды риска путем прослеживания связей: поток — процесс — системная характеристика — субъективный фактор, а также организовать структуру и направления комплексного анализа возникающих рисков.

Основные документы, которыми руководствуются риск-менеджеры западных компаний в практической деятельности, разработаны Базельским комитетом по банковскому надзору и называются Принципы банковского надзора [1]. Данный документ содержит 25 принципов, реализация которых призвана минимально необходимым условием обеспечения эффективного банковского надзора, а также комментарии к ним, базирующиеся на рекомендациях Базельского комитета и лучшей международной практике в сфере банковского дела и банковского надзора. Среди Базельских принципов можно выделить принципы 6-15, связанные с рисками банковской деятельности. Интеграция Молдавской банковской финансовой отчетности с Международными Стандартами Финансовой Отчетности (МСФО) несомненно, получит свое развитие в применении данных принципов в банковской практике. Согласно методологии Базельского соглашения по капиталу, «Международная конвергенция измерения капитала и стандартов капитала: новые подходы» (известного как Базель II) в принципах эффективного банковского надзора действующая система классификации рисков предполагает следующие экономические риски в банковской деятельности: кредитный риск, страновой и трансферный риск, рыночный риск, процентный риск, риск потери ликвидности, операционный риск, правовой риск и риск ухудшения репутации [2].

В целом имеется множество различных классификаций экономических рисков, различаясь положенными в их основу критериями. По нашему мнению наиболее

методологически целостной представляется классификация банковских рисков, как составной части экономических, предложенная Питером С. Роузом [8, с. 156]. Группировка риска производится по видам на основные (кредитный риск, риск несбалансированности ликвидности, рыночный риск, процентный риск, риск недополучения прибыли, риск неплатежеспособности) и дополнительные (инфляционный риск, валютный риск, политический риск и риск злоупотреблений) риски. Достоинством классификации является то, что в эту систему включены как внутренние риски, возникающие в процессе обеспечения собственной деятельности банка, так и внешние риски, способные существенно повлиять на работоспособность и конкурентоспособность банковской системы. На фигуре 2 представлена предложенная Питером С. Роузом и доработанная автором формализация видов классификации рисков с учетом главных рисков 2013 года и ближайшего десятилетия.

Фиг. 2. **Структурная схема формализации видов классификации рисков с учетом главных рисков 2013 года и ближайшего десятилетия**

Источник: Модификация автором схемы классификации Питера С. Роуза

Не смотря на то, что существуют и другие научные классификации экономических рисков (Шеремета А.Д. и Щербакова Г.Н., Савинской Н.А., Гырля М.) автор считает, что с учетом специфики современного состояния международной банковской системы (МБС) классификацию Питера С. Роуза для практического применения следует дополнить:

1. в группировку по дополнительным видам рискам включить страновой и операционные риски;
2. добавить новый вид – глобальные риски международной банковской системы и включить в его классификацию риски ошибок Центробанков, хронические дисбалансы финансовых систем, риски кибератак, риски бесконтрольности и последствий пользования глобальной компьютерной сетью Интернет, а также риски непредсказуемости информационных технологий.

При этом под **глобальными рисками международной банковской системы** следует понимать риски, оказывающие существенное влияние на формирование балансов мировых финансово – банковских систем и обеспечение их бесперебойной и эффективной деятельности в зависимости от величины и возможного воздействия подверженностей.

Необходимость включения указанных рисков связана с особенностями современного развития мировой экономики и международной банковской системы на 2013- 2023 гг. С предостережениями от глобальных рисков выступают эксперты Всемирного экономического форума, обнародовавшие 8 января 2013 г. в Лондоне исследование о глобальных рисках в 2013 году.[9] Выявленные экспертами глобальные риски можно разделить на социальные (растущий разрыв между уровнем доходов населения), природно – климатические (нехватка пресной воды как результат изменения климата планеты), глобальные риски мировой экономики (хронический бюджетный дефицит стран мира, продовольственный кризис; чрезвычайная волатильность цен на энергоносители и продовольствие). В отдельную классификационную группу по мнению автора целесообразно выделить глобальные риски международной банковской системы (системный финансовый кризис, возможный крах международной финансовой системы и др.).

Исследование действительно поднимает серьезные мировые проблемы. Это и неравенство возможностей (как следствие, социальная нестабильность и демонстрации во всех развитых странах), невозможность, а порой и нежелание политических кругов в Америке и в Европе справиться с проблемой безответственной бюджетной политики и т. д. Таким образом, выделив главные риски ближайшего десятилетия, можно определить порядок их взаимного влияния: некоторые риски и угрозы, накладываясь, могут усиливать друг друга. В докладе на 2012 г. определены три главных сценария «наложения рисков». Основной из них, по мнению составителей доклада, связан с тем, что ухудшающиеся экономические условия ставят под сомнение «социальный контракт» между гражданами и властью. На это накладывается усиливающийся протекционизм, национализм и популизм, и в результате это может привести к глобальному движению мировой экономики по нисходящей спирали [9].

Среди предпосылок формирования системы глобальных экономических рисков важную роль по нашему мнению играет лоскутковый характер экономики. При этом мы понимаем лоскут как кусок, часть, элемент национальной, регио-

нальной или мировой экономики.«Лоскутная экономика», появившись в июне 2011 г. не использовалась как научный термин, не связывалась с общемировыми тенденциями, а скорее как фразеологический оборот для усиления характеристики региональной экономики Австралии – увеличение валютных и кредитных рисков, скачки курса австралийского доллара, ослабление кредитных и инвестиционных рынков, рост безработицы, инфляции и др. [3].

Лоскутковая экономика (англ. patchwork economy) представляет собой сегодня один из наиболее характерных элементов глобализации. По нашему мнению лоскутковая экономика представляет собой совокупность разнородных экономических систем (например, в рамках ЕС экономики стран Центральной и Восточной Европы с одной стороны и Германии или Франции, с другой) либо совокупность экономик имеющих различные скорости развития (от экспоненциального роста до кризисного состояния). Лоскутность в развитии отдельных элементов мировой экономической системы проявляется на всех этапах ее становления. Но ее неблагоприятная роль стала активно проявляться лишь в условиях глобализации мирового хозяйства [4]. Сегодня лоскутковое развитие мировой экономической системы стало тормозом глобального экономического роста. Особенно велико влияние разнонаправленного развития на международную банковскую деятельность. В банковской системе весьма велики национальные нормативные различия, которые в значительной мере влияют на формирование и функционирование экономических рисков. Это позволяет нам сформулировать теоретическое понятие «**лоскутковая экономика в международной банковской деятельности**» как одно их составных базовых соображений в системе предпосылок формирования экономических рисков.

Таким образом, приведенная классификация и элементы, положенные в основу экономической классификации, имеют целью не столько перечисление всех видов банковских рисков, сколько демонстрацию наличия определенной системы, позволяющей банкам не упускать отдельные разновидности при определении совокупного размера рисков в коммерческой и производственной сфере. Особенностью нахождения степени экономических рисков является его индивидуальная величина, связанная с принятием на себя конкретного риска по конкретной банковской операции. Во многом она определяется субъективной позицией каждого банка.

Библиография:

1. Basel Committee on Banking Supervision. Consultative DocumentThe Internal Ratings-Based Approach. Supporting Document to the New Basel Capital Accord. Issued for comment by 31 May 2001. Basel, Switzerland: Bank for International Settlements. Press & Communications. January 2001. – 65 p.
2. Basel Committee on Banking Supervision. An Explanatory Note on the Basel II IRB Risk Weight Functions. Basel, Switzerland: Bank for International Settlements. Press & Communications. July 2005. – 19 p. ISBN print: 92-9131-673-3

3. Despite our patchwork economy, all states are sharing in the boom. In: The conversation. Latest ideas and research. http://theconversation.edu.au/despite-our-patchwork-economy-all-states-are-sharing-in-the-boom-1964
4. Numbers reflect a patchwork economy. http://www.couriermail.com.au/spike/columnists/numbers-reflect-a-patchwork-economy/story-e6frerg6-1226352390856. [Electronic resource]. Date accessed: 11.12.2011
5. Шеремет А.Д., Щербакова Г.Н. Финансовый анализ в коммерческом банке. М.: Финансы и статистика, 2000. 310 с.
6. Савинская Н.А. Основы системной организации банковской деятельности. Риски. Надзор. Координация / Под ред. д-ра экон. наук, проф. Л.С. Тарасевича. СПб.: СПбГУЭФ, 2000. 326 с. Научная библиотека диссертаций и авторефератов disserCat http://www.dissercat.com/content/metodicheskie-osnovy-postroeniya-i-sovershenstvovaniya-sistemy-vnutrennego-kontrolya-rossiis#ixzz2HefUFBoL [Электронный документ] Дата обращения: 12.01.2012
7. Показатели финансовой устойчивости. Руководство по составлению. - Вашингтон, округ Колумбия, США: Международный Валютный Фонд, 2007, стр. 31 p. cm. http://www.imf.org [Электронный ресурс]. Дата обращения: 12.05.2010
8. Питер С. Роуз. Банковский менеджмент. М.: Дело Лтд, 2000. 230 с.
9. Глобальные риски 2012 г.http://m.forbes.ru/article.php?id=78317 [Электронный документ] Дата обращения: 08.01.13

НОВЫЕ ПРИОРИТЕТЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ МИРЕ

Сайдикрамова Анна
Eductus (Швеция)

Сегодняшний мир это мир, в котором правит информация. Она обрабатывается, накапливается, хранится и передается с помощью различных электронных средств связи. Компьютеризация многих видов человеческой деятельности открывает нам новые преимущества и возможности, создавая, при этом, новые проблемы, ранее нам неизвестные.

Важные интересы субъектов, таких как, государство, юридические и физические лица, включают конфиденциальную коммерческую и персональную информацию, которая должна быть постоянно легко доступной, но одновременно и надежно защищенной от неправомерного ее использования, нежелательного разглашения, фальсификации, незаконного тиражирования, блокирования или уничтожения.

Следует отметить, что в настоящее время большинство организаций не обеспечивает необходимый уровень информационной безопасности своих активов.

Недостаточный уровень обеспечения информационной безопасности обусловлен факторами, которые включают:

- быстрое увеличение количества пользователей, имеющих непосредственный доступ к средствам информационных технологий и массивам данных, а также их слабая грамотность в вопросах безопасности;
- быстрый рост количества персональных компьютеров, применяемых в различных видах деятельности;
- повышение уровня доверия к автоматизированным системам управления и обработки информации. Информационным системам доверяют самую ответственную работу, от выполнения которой зависят жизнь и благосостояние многих людей;
- развитие и распространение компьютерных сетей, территориально-распределенных систем и систем с удаленным доступом к совместно используемым ресурсам;
- значительное увеличение объемов информации, накапливаемой и обрабатываемой с помощью различных средств автоматизации;
- современный уровень развития средств информационной безопасности значительно отстает от темпов развития информационных технологий;
- многочисленные уязвимости и бреши в программном и сетевом обеспечениях. Это обусловлено тем, что современные программные продукты из-за конкуренции попадают в продажу с ошибками, недоработками и некачественной отладкой;
- хранение больших объемов информации, включая и конфиденциальные данные, на электронных носителях;
- отношение к информации, как к товару, что увеличивает уровень конкуренции и производственного шпионажа в области предоставления информационных услуг;
- недостаточный уровень системы законодательно-правового регулирования отношений в сфере использования и защиты информации, что приводит к возникновению и распространению компьютерной преступности.

Таким образом, новые тенденции и технический прогресс заметно увеличивает надежность информационных систем, но и влекут за собой появление новых проблем информационной безопасности, среди которых можно выделить основные:

- риски информационной безопасности при внедрении облачных вычислений и проектов с большими массивами данных;
- риск кражи данных с мобильных устройств, используемых сотрудниками для работы;
- расход времени и средств на исправление проблем выше, чем расход на их предупреждение;
- утечка конфиденциальных данных - по данным многих аналитиков более ¾ организаций страдают от несанкционированной утечки информации, в боль-

шинстве случаев персональных данных. На сегодняшний день слабым звеном в информационных системах являются сотрудники организаций компании, так как большинство утечек конфиденциальных данных связано с действиями злонамеренных инсайдеров или с обычной небрежностью персонала;

- риски, связанные с виртуальной инфраструктурой - обусловлены тем, что контролировать процесс создания и перемещения виртуальных машин намного сложнее, чем в случае физических сред.

Для эффективного обеспечения информационной безопасности необходимо уделять особое внимание основным вопросам, среди которых:

- обеспечение эффективного и прозрачного управления информационными рисками, посредством мониторинга уровня защиты и соответствия, который способен быстро выявить и устранить угрозы;
- планирование приоритетов действий на основе бизнес-рисков, связанных с потенциальными инцидентами;
- быстрое нахождение информации о любом компьютере, развертывание продуктов или обновление конфигураций за несколько секунд;
- применение комплекса решений, включающего ролевые модели доступа на уровне отдельных документов и информационных систем, а также механизмы управления доступом на основе этих моделей;
- определение правил и контроль над использованием мобильных устройств с использованием различных методов защиты и проверки уязвимости мобильных приложений при их внедрении;
- принятие решений и определение приоритетов при управлении инцидентами и предотвращении угроз, с использованием возможности учета бизнес-контекста и содержимого информационных активов;
- более эффективное обеспечение взаимодействия отделов информационной безопасности с бизнес-подразделениями в организациях, а также внедрение корпоративной культуры безопасности.

Проблемы информационной безопасности можно приравнивать к проблемам безопасного бизнеса в целом, так как по мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается и зависимость общества от уровня информационной безопасности используемых им информационных технологий и средств. Таким образом, проблема обеспечения информационной безопасности становится еще более серьезной, что предполагает применение организациями комплекса правовых, организационно-технических и экономических методов обеспечения информационной безопасности.

Используемые источники:

1. www.iso27000.ru
2. www.itsec.ru
3. www.connect.ru

INFORMATION RISKS DURING MEASUREMENTS OF NOISE POLLUTION

Lyubomir V. Vladimirov Nikolai I. Kovachev
University of Rousse, Bulgaria
E-mail: lvvladimirov@uni-ruse.bg, nkovachev@uni-ruse.bg

A method for determination of the information uncertainty in noise measurements is proposed. The criteria for evaluation of the information uncertainty is verified at first level. Then the method for their determination is justified. The information risks are verified experimentally.

Key words: information, risk, noise, pollution.

The uncertainty is typical for investigation of noise pollution in the environment [1,2]. The reasons are the entropity hierarchy, completeness, variability and lack of knowledge, information and normative differences.

The purpose of the present paper is to propose a method for determination of the uncertainty in information from imissions of noise pollution measurements. The problems to be solved are: 1) Criteria definition for information uncertainty evaluation, 2) Justification of the definition method for information uncertainty evaluation, 3) Experimental study and verification of the criteria.

Information uncertainty *Ifunsec* is presented as an summarized indicator of two composites - Information inexactness – *Ifexactness* and information unclarity - *Ifclarity* [1,2]. The information uncertainty is defined by the law of distribution *Noise Distribution* of the A-weighted sound pressure level - L_{pA}. Using Risk 4.5 software, 16 indiscrete distributions law of the noise imission were checked: 1) *Uniform*; 2) *Normal*; 3) *Lognormal*; 4) *Logistic*; 5) *Loglogistic*, 6) *Triang*, 7) *Exponent*, 8) *ExtValue*; 9) *Gama*; 10) *Beta*, 11) *Weibul*, 12) *Rayleigh*; 13) *Pearson*, 14) *Gumbel*, 15) *Erlang*, 16) *Wald*. 15 numerical characteristics of the distributions were set: *Left X* - left boundary value of the imissions, *Left P* - left boundary of the confidence interval, *Right X* - right boundary of the imissions, *Right P* - right boundary of the confidence interval, *Diff. X* - interval values of the imissions, *Diff. P* - Confidence Interval, *Minimum* and *Maximum* - minimum and maximum value of the imissions, *Mean* - mathematical expectation, m , *Mode* - Fashion, *Median* - Median, *Std. Deviation* – standard deviation, σ , *Variance* - dispersion, σ^2 , *Skewness* - asymmetry, *Kurtosis* - kurtosis. The uncertainty is measured by the value of the mathematical expectation $\overline{L}_{pA}$ of the measured A-weighted sound pressure level - L_{pA}., standard deviation σ_{LpA} and variance $\sigma_{LpA}{}^2$.

The risk for information uncertainty of the measurements $R_{Ifexact}$ for the imissions is defined from the probability P for amending of the mathematical expectation, standard deviation and variance in the defined boundaries for overall noise levels L_{pA}

variation. Therefore three variants of it are used: 1) the average information risk - $R_{Ifexact}[m]$, 2) RMS information risk - $R_{Ifexact}[\sigma]$, 3) Dispersive information risk - $R_{Ifexact}[\sigma^2]$. A check of the hypothesis of the laws of probability distribution is made. Then are calculated the probabilities of the mathematical expectation, variance and standard deviation of the imissions for their change at the preset intervals. For this purpose the integrated functions of the distribution of the above laws and the analytical dependences for calculation are derived. The program *Calc.exe* is used. The range for the imissions variations which are considered here as mathematical expectation, standard deviation and variance depend on the purposes of the study. They may vary in the preset intervals of the defined meanings m, σ and σ^2 and through the intervals determined by the minimum and maximum value of the noise imissions, standard deviation, etc.

The information unclarity *Ifclarity* is determined by setting the 11 descriptors: I. Criteria for hypotheses testing about the laws of distribution: a) criterion of Pearson χ^2, b) criterion of Anderson-Darling, $A-D$, c) criterion of Kolmogorov-Smirnov $K-S$, II. Number of the tested with RISK 4.5 distribution laws , III. Programs used for processing of the experimental data, IV. Sample size; V. Duration of the noise exposition; VI. Acoustic background in the area of measurement VII. Scheme of the measurements and the location of measuring points; VIII. Propagation medium; IX. Configuration of the sources of noise, symmetry or asymmetry, dimensions, direction of sound, X. Indicators of the area of the noise propagation; XI. Procedure for sampling formation - consistent, combined or random.

For verification of the proposed criteria - averaged risk - $R_{Ifexact}[m]$, RMS risk - $R_{Ifexact}[\sigma]$ and dispersive information risk $R_{Ifexact}[\sigma^2]$ are performed experimental studies of the noise pollution in the air of the manufacturing environment, generated by tailor manufacturing. The measurements were conducted in accordance with the standards EN ISO 11201:1995, EN ISO 11204:1995 + AC 1997 and EN ISO 3746 in their Bulgarian transpositions. The sample consist of 20000 values. The sampling rates are 10, 15, 20 kHz. They are tested by the criterion of Pearson, Anderson-Darling and Kolmogorov-Smirnov. The values of the information risks were obtained. The parameters of the first ranked from the program Risk 4.5 law of distribution are presented in Table 1 at two sampling rates – 10 and 20 kHz.

Table 1

Information risks in noise pollution's measurements

Criteria	Law	Sampling rate 10 kHz			Sampling rate 20 kHz		
		$R_{Ifexact}[m]$	$R_{Ifexact}[\sigma]$	$R_{Ifexact}[\sigma^2]$	$R_{Ifexact}[m]$	$R_{Ifexact}[\sigma]$	$R_{Ifexact}[\sigma^2]$
χ^2	*Logistic*	0,45117	0,62772	0,62119	0,63382	0,75261	0,75101
$A-D$	*Beta*	0,52922	0,47833	0,47322	0,67228	0,74331	0,71821
$K-S$	*Weibul*	0,50188	0,4338,	0,43561	0,66281	0,73811	0,72811

The analysis of the results shows that the proposed criteria for information risk uncertainty of the noise pollution values are sufficiently selective. A dependency of increasing at higher sample rate is seen. The values of risks in relation of standard deviation and variance are very close. Here's what you can use one of them. Laws of distribution have a significant influence on the values of the criteria of information risk. The difference between them is relatively small when the sampling rate of 20 kHz .

The foregoing gives us a reason to claim that the proposed method for evaluation of the information uncertainty of noise pollution's measurement is objective. The used information risks on mathematical expectation, standard deviation and variance are representative and sensitive. They allow consideration in probabilistic terms, and thus to take into account the true nature of the variables.

References

1. Vladimirov, L. Riskmetric in Environmental Security. Varna, Varna free university, 2009.
2. Vladimirov, L., N. Kovachev. Information insecurity of indiscrete measurement of noise imissions. Shumen, National military university, Proceedings of International conference Problems of Information Security, 2011. pp.228-236.

АНАЛИЗ ЭТАПОВ РАЗВИТИЯ ТЕНЕВОЙ ИНФОРМАЦИОННОЙ ЭКОНОМИКИ

Бортэ Григорий, аспирант Молдавской Экономической Академии,
Ведущий эксперт отдела информационной безопасности,
Национальный Банк Республики Молдова

This article aims to analyze the roots of underground information economics, phases of its establishment, and preconditions of its appearance. Important milestones are discussed and outlined.

Вступление.

На сегодняшний день, каждый человек, в той или иной мере использующий вычислительную технику, столкнулся с проблемой теневой информационной экономики, будь то вредоносное программное обеспечение, попавшее на компьютер или мобильное устройство, украденные персональные данные, спам, полученный на электронную почту или мобильный телефон. В последнее время всё чаще говорят о событиях, так или иначе связанных с данной областью, находящейся на стыке многих наук: информационно-коммуникационных технологий, экономики, бухгалтерии, юриспруденции.

Целью данного доклада является всесторонний анализ основных этапов развития теневой информационной экономики.

В данном докладе рассматривается проблемная ситуация теневой информационной экономики, предпосылки её развития, истоки, важные вехи и события, ключевые её элементы и участники: объекты и субъекты информационных преступлений.

Теневая информационная экономика - деятельность, связанная с исследованием, проектированием, производством, распространением, поддержкой и использованием компонент информационных и коммуникационных технологий, скрываемая от общества и государства, находящаяся вне государственного контроля и учёта, а также, чаще всего, являющаяся противоправной. Таким образом, причиной существования теневой информационной экономики является наличие условий, при которых выгодно скрывать свою деятельность, либо отдельные её элементы.

В развитии и становлении теневой информационной экономики мы выделяем три основных этапа, временные рамки и основополагающие события которых будут рассмотрены и проанализированы ниже:

Докомпьютерный. На данном этапе формируются предпосылки развития теневой информационной экономики: появляются прообразы вычислительной техники, формируется законодательство (основой для которого во многом служит Римское право), экономические и бухгалтерские (двойной учёт) аспекты. К концу данного периода, экономики стран уже сталкиваются с проблемой теневой экономики, двойной бухгалтерии.

Ранний. Начало данного этапа относится к середине 20ого века. Этот этап характерен появлением персонального компьютера и его массовым распространением, появлением первых хакеров, которые позже начали объединяться в группировки. Важной характеристикой данного этапа является особенность природы вредоносных программ: большинство из них либо несут деструктивный, либо исследовательский характер.

Современный. На данном этапе всё реже и реже встречаются хакеры-одиночки, им на смену приходят организованные группировки, которые действуют как единый отлаженный механизм: четко распределены роли, зоны ответственности. В этот период наблюдается смена направленности вредоносного программного обеспечения с деструктивных целей на кражу данных, вымогательство, использование компьютера жертвы в своих целях, например, для рассылки спама, в качестве прокси или «зомби» в ботнете. Наблюдается «коммерциализация» вредоносного программного обеспечения, уязвимостей (1). Данный период характеризуется широкомасштабными вирусными эпидемиями, например, Zeus, Conficker. Многие из хакеров, появившихся на предыдущем этапе, сейчас становятся экспертами в области информационной безопасности (2). Пиратство набирает всё большие обороты, как и борьба с этим явлением. В этом периоде появляется такое понятие, как хактивизм: использование компьютеров, компьютерных сетей и информационно-коммуникационных технологий как инструмента для выражения своего протеста. В этот период начинают набирать популярность мобильные устройства, и, как следствие, всё чаще и чаще становятся объектом атак злоумышленников. Наблюдается появление

всё большего количества информационных аналогов преступлений из «обычно» криминальной сферы, таких как вымогательство, шантаж, шпионаж, отмывание денег.

Заключение.

В данном докладе была предпринята попытка обозначить основные этапы развития теневой информационной экономики, выделить важные вехи в её становлении, основные черты, присущие каждому из этапов. Очевидно, что проблема теневой информационной экономики уходит своими корнями глубоко в историю человечества, экономики, информационных технологий, человеческой психологии. Борьба с данным явлением должна осуществляться на многих уровнях: глобальном, международном, государственном, региональном и даже корпоративном.

Список литературы

1. **Boehme, Rainer.** Vulnerability Markets. What is the economic value of a zero-day exploit? Dresden : Technische Universitat Dresden, Institute for System Architecture.
2. **Chiesa, Raoul.** Cybercrime: reasons, evolution of the players and an analysis of their modus operandi. *Bright.* [Online] July 1, 2010. http://flarenetwork.org/report/enquiries/article/cybercrime_reasons_evolution_of_the_players_and_an_analysis_of_their_modus_operandi.htm.
3. **Dekker, Thomas.** The Wonderfull yeare. 1603. *luminarium.org.* [Online] http://www.luminarium.org/renascence-editions/yeare.html.
4. **Richardson, Robert J.** Monitoring Sale Transactions for Illegal Activity. *IIMA online .* [В Интернете] 2006 г. http://www.iima.org/CIIMA/13%20CIIMA%206-1%20105-114%20Richardson.pdf.
5. **Starbuck Gerson, Emily.** Pre-plastic credit: Charge plates, coins, celluloids. *creditcards.com.* [В Интернете] 7 November 2007 г. http://www.creditcards.com/credit-card-news/credit-collectible-coins-charge-plate-1264.php.

PERSONAL DATA DANGERS

Nicolae Turcan
United World College Red Cross Nordic

In this work, a major problem of security of personal data is discussed. Mobile applications, which simplified data transfers, have also shown some threats that we should be aware of.

In the century of astonishing improvements, technology seems to occupy more and more place in our lives. Nowadays, mobile application became extremely popular, bringing plenty of advantages, but also stressing the security of personal data. Both Google and Apple have announced that they have surpassed 700,000 apps in their app stores.

This provides a tremendous amount of choice for consumers, and also enables businesses to create and deploy custom apps to their workforce. However, for the security issues, it raises lot of concerns. Regarding those facts, security officers must be extremely diligent in educating their employees about dangers of their mobile data. It could take only one application to leak data, being enough to cause infinite amount of problems for companies.

Reviewing apps from the Google and Apple stores, security has been found to be lacking. Even the apps that we would think hold our trusted information: secret–banking apps, are failing. Why are so many apps lacking some of the most basic security principles? A reasonable excuse can be that Apple and Google have done an amazing job at making it very easy to create apps. However, just because you can doesn't mean you should.

A quick internet search will return huge amount of articles and sources about creating Android and iOS apps. The marketing behind these sites is genius. They tell you how easy it is to create your own app, how you don't need to be familiar with programming languages. These apps range in sophistication with some even creating unique source code based on the platform that you are developing against. The real unexpected problem is that none of these DIY programs teach or test for security flaws.

Those problems are predominantly caused by student. As more students acquire mobile devices and start downloading applications at younger ages, data privacy is becoming even more critical. It turns out that 6 out of 10 mobile apps are sharing personal data that could put children in danger.

A report from the Federal Trade Commission examined hundreds of apps offered for children in the Google Play and Apple App stores and the privacy disclosures and practices they follow. The FTC found that most apps do not provide parents with information about what data is being collected from their children, how it is being shared, or who will access to it. Many of these apps connect to social networks and quietly send information to third parties, such as ad networks and analytics companies, without informing their parents about those actions.

Data privacy may not be top of mind for parents and teachers when it comes to student devices, but it should be a priority. The FTC found that there was a fairly small number of third parties collecting information from all types of apps. "This means the third parties that receive information from multiple apps could potentially develop detailed profiles of the children based on their behavior in different apps," the commission said in a press release on the report.

However, figuring out which apps share data is difficult. According to the report, only 20 percent of apps disclosed any information at all about the app's privacy practices. But almost 60 percent were sending information back to the app developer or, more commonly, a third party.

And many apps contained links to other functions outside the app without notifying users about them before download. Fifty-eight percent of apps contained ads, but only 15 percent disclosed that before download. Twenty-two percent linked to social networks, but only 9 percent disclosed that fact. About 17 percent allowed users to make

purchases within the app, but notifications about that were not always prominent or understandable.

The FTC is launching investigations to determine if app developers or stores are violating the Children's Online Privacy Protection Act, which prohibits collection of data on children younger than 13 without parental consent. It's also developing an education program about mobile apps and privacy for parents, and it urges all involved in the mobile app industry to offer more information, so that parents and children can understand the data being collected and shared when an app is downloaded.

The FTC report focuses on parents and their role in protecting children, but teachers and schools must also be aware in examining any apps recommended by or used in class. Schools can also play an important role in spreading knowledge about data privacy and safety to students as they become digital citizens.

One of the basic security principles that is often overlooked and even more often misunderstood is the principle known as Defense-in-Depth. The premise behind Defense-in-Depth is that each layer of security must be sound and protect the system with its own merits, therefore if one layer of the security fails the next layer is there to back it up. If however the system is designed with security flaws in place, the strategy of Defense-in-Depth is weakened. The basics to Defense-in-Depth are present in both iOS and Android apps, you just need to know where to look.

If an app is going to store private information or data then of course that information/data must be encrypted. This is where the Defense-in-Depth strategy begins. Apple and Google provide means to encrypt your information and data, but their encryption is tied to the device passcode. The developer should not rely solely on a third party to protect its information and data. By doing so, the Defense-in-Depth strategy does not exist. The developer must create their own database structure, store the information/data in their database, protect the database with separate encryption, then that which is provided by the native operating system, encrypt the database with a passphrase that is not the device password, and finally use the native operating system to protect the database. In the scenario just described the app developer is supplying their own security and then protecting their security with the security provided by Apple and Google. Now, the infringer has to defeat Apple/Google security provided on the device, which of course is protected by the device password. If the security of the device fails then the infringer still has to defeat the security provided by the app.

A great solution for protecting your password for your networks is using a token. That device generates new passwords for your bank accounts and not only, which are available only for 30 seconds. This idea could prevent a lot of data leakage caused by the wrong use of applications.

As a conclusion, I would like to state that the problem of mobile applications regarding personal data dangers is very common right now, and is growing without stop. We must implement solutions to secure ourselves, sooner we do it, less problems we'll have to face in the nearest future.

НАПРАВЛЕНИЯ ЗАЩИТЫ АВТОРСКОГО ПРАВА В СЕТИ ИНТЕРНЕТ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Ирина Шнып,
УО «Гомельский государственный университет имени Ф. Скорины»

The approaches to the problem of legal regulation of copyright in the Internet and protection of works in if.

Существует два абсолютно противоположных подхода к решению проблемы правого регулирования авторских прав в сети Интернет:

1) исключительно свободное использование произведений;
2) верховенство законодательства в сети, то есть правовое регулирование общественных отношений по использованию произведений в Интернет.

Сторонники первого подхода считают, что соблюдение авторских прав в сети Интернет мешает ее активному информационному наполнению. Они предлагают ограничить часть авторских прав, например, расширить возможности свободного использования произведений. Существует мнение о том, что следует не расширять возможность свободного использования произведений в сети Интернет, а полностью узаконить свободное использование объектов авторского права в сети. В пользу этой точки зрения приводят доводы о том, что изначально «всемирная паутина» создавалась для того, чтобы обеспечить свободный доступ пользователей к ресурсам, размещенным в сети Интернет. А введение ограничений по использованию объектов авторского права ведет к нарушению права пользователя интернет-услуг на свободный доступ к информации.

Сторонники второго подхода считают, что надо принимать дополнительные нормативные правовые акты и нормы, которые будут детально регламентировать отношения, связанные с использованием объектов авторского права в сети Интернет, и помогут авторам более эффективно защитить свои права. Однако при разработке и принятии новых нормативных актов следует учитывать специфику «всемирной паутины» и принципы ее функционирования, чтобы не происходило сдерживание развития сети Интернет.

Проблему авторского права можно решить обеспечением надлежащей защиты произведений в сети Интернет другими, помимо законодательства, специфическими средствами.

Дискуссии о защите авторских прав в Интернете ведутся достаточно давно, предлагаются многочисленные решения данного вопроса. Некоторые российские ученые в целях решения проблем авторских прав в сети Интернет предлагают издать новый нормативный правовой акт о едином интернет-реестре объектов авторских и смежных прав. Он обеспечил бы создание подобного реестра сначала на государственном уровне, а затем послужил бы модельным законом международного

частного права и возможной основой для межгосударственного соглашения о едином интернет-реестре объектов авторских и смежных прав.

Цель создания такого реестра – предоставить авторам и исполнителям гарантии фиксации их авторских и смежных прав и распоряжения ими, использую удобный механизм регистрации объектов интеллектуальной собственности. Такая регистрация должна обладать набором законодательно закрепленных характеристик, который позволит ей не быть сложной для субъектов правоотношений, а также исключит возможность злоупотреблений. Она должна соответствовать следующим критериям:

1) предлагаемая регистрация должна быть добровольной, то есть не требующей от авторов обязательного участия. Однако не должны отказывать авторам в защите каких-либо прав в случае отказа от участия в регистрации;
2) данная процедура должна быть лишена посредников. В Российской Федерации уже существуют системы, осуществляющие регистрацию, созданные в целях обеспечения фиксации и защиты авторских прав, но в которых посредники юридической нормой предусмотрены и фактически задействованы. Как показывает практика, посредники начинают злоупотреблять законом в целях личного обогащения и саботируют возложенные на них законодательством функции содействия защите прав участников отношений, вводя пошлины и сборы в свою пользу за посреднические услуги. При этом они не ведут строгой финансовой отчетности;
3) такая регистрация должна быть бесплатной, дистанционной, мгновенной, приватной (то есть обеспечивающей сохранение в тайне информации о депонируемом объекте или личности автора, если он распорядится об этом), а также не требующей, в отличие от других существующих аналогов (регистрация патентов и платное депонирование физических копий рукописей) материальных и временных затрат.

Другой вариант защиты авторских прав в сети Интернет – это использование знака охраны авторского права (знака копирайта) и технологии электронно-цифровой подписи. Знак охраны авторского права состоит из трех информативных элементов: знака©, наименования (имени) правообладателя, года первого выпуска. Но такой знак несет чисто декларативную функцию. Современные информационные технологии, применяемые в интернете, позволяют использовать знак копирайта в ином качестве, то есть реализовывать возможность его реальных защитных и информационных функций на основе легальной процедуры электронного документирования с использованием технологии электронно-цифровой подписи, обеспечивающей юридическую силу электронным документам.

Сравнение использования процедуры электронного документирования с использованием технологии электронно-цифровой подписи с регистрацией объектов интеллектуальной собственности в едином интернет-реестре объектов авторских и смежных прав показывает преимущества способа защиты регистрации в едином реестре, так как для подписания документа электронно-цифровой подписью надо приобрести ключ, что требует материальных и временных затрат. Также существует возможность несанкционированного доступа к данному ключу путем его взлома.

В западном сегменте сети Интернет распространен другой способ защиты – водяные знаки в электронных копиях документов и изображений. Они наносятся с помощью специальных программ. При обычном визуальном рассмотрении изображения пользователь не видит каких-либо закодированных обозначений – знака копирайта, имени автора, года издания. Но при применении определенного программного средства можно доказать, что файлы содержат дополнительную информацию, указывающую на лицо, ее записавшее. Важной особенностью водяных знаков является устойчивость к любым операциям над изображением: сжатию, изменению размеров, формата, цветности, которые не уничтожают и лишь слабо искажают их. Они сохраняются даже при печати снимка и последующем его сканировании.

На данный момент использование водяных знаков является самым эффективным способом защиты авторских прав в сети Интернет. Однако существуют специальные программы, позволяющие вычистить из изображения водяные знаки, но при этом остаются следы такой чистки. После работы такой программы нельзя будет вычислить, чей копирайт стоял на изображении до того, как программа поработала, но можно определить, что этот снимок является производным от другого, на котором есть водяные знаки.

Можно сделать выводы, что существуют два абсолютно противоположных подхода к решению проблемы правого регулирования авторских прав в сети Интернет: свободное использование произведений и верховенство законодательства в сети. Наиболее приемлемым следует считать последний, так как современное общество еще не готово к свободному использованию объектов авторского права в сети Интернет, поэтому целесообразно усовершенствовать законодательство в этой сфере. Помимо правового регулирования авторских прав в сети Интернет можно использовать средства защиты произведений в сети: создание единого интернет-реестре объектов авторских и смежных прав, использование знака охраны авторского права и технологии электронно-цифровой подписи, нанесение водяных знаков.

ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ УТЕЧКИ ЗА СЧЕТ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

А. Ахмаджонов
Центр разработки программных продуктов и аппаратно-программных комплексов при ТУИТ (ЦРПП и АПК при ТУИТ) г. Ташкент

In this work considered different types of check and testing, as well as requirements on protection information from the leakage to the account of side electromagnetic radiating and noise pickups

Анализ физических процессов работы технических средств и оргтехники показывает, что в окружающем их пространстве и отходящих цепях возникают информационные сигналы, которые могут обнаруживаться на значительных расстоя-

ниях от создающих их технических средств (ТС). Это обстоятельство может использоваться технической разведкой.

Средство защиты информации должно оцениваться соотношением сигнал/помеха на границе контролируемой зоны.

Усовершенствование оборудования, уменьшающего побочных электромагнитных излучений и наводок (ПЭМИН) от оборудования передачи данных, и защита от утечки информации через ПЭМИН от кабельных линий связи остаются большой проблемой. Проблема ПЭМИН для кабельных сетей актуальна лишь в случае использования в них медных кабелей. Симметричные кабели на основе витых пар имеют волновое сопротивление 100 Ом. Симметричные витые пары разработаны для передачи сигнала в «симметричном режиме», также как «дифференциальный режим передачи». Симметричная передача предполагает равенство токов, текущих по проводам витой пары в противоположных направлениях. В идеальном случае излучения в этом режиме отсутствуют. На практике идеальные режимы не достижимы и в кабельной линии всегда присутствует «несимметричный режим» передачи, т.е. неуравновешенная составляющая токов. В «несимметричном режиме» излучения от обоих проводников складываются, что приводит к значительным излучениям от витой пары. «Несимметричный режим» появляется в результате работы оконечного оборудования, дефектов и не идеальности кабелей.

Теоретическая оценка риска перехвата очень сложна, но использованием трех классических методов можно достичь цели несимметричного режима» с помощью измерения:

- паразитной составляющей токового датчика;
- напряжения, которое наводится на согласованной параллельной силовой линии.

В ходе работ на данном этапе выполняются следующие виды проверок и тестирования:

- проверка мест ближайшего доступа к линиям связи основных технических средств и систем (ОТСС), вспомогательных технических средств и систем (ВТСС), инженерных коммуникаций и металлоконструкций, имеющих выход за пределы контролируемой зоны;
- проверка прокладки цепей электропитания и шины заземления электропитания ОТСС и ВТСС на объектах;
- проверка прокладки линий пожарной и охранной сигнализации;
- проверка прокладки коммуникаций и металлоконструкций;
- проверка прокладки кабелей ОТСС и ВТСС. При наличии совместного пробега проверка длины пробега и разноса линий связи между собой и металлоконструкциями;
- проверка размещения технических средств, участвующих в обработке конфиденциальной информации;
- проверка своевременности и правильности категорирования технических средств;

- поверка на соответствие требованиям руководящих документов по правильности размещения и использования средств ЭВТ;
- проверка выполнения требований предписаний на эксплуатацию и порядок эксплуатации технических средств;
- проверка качества установки и порядка эксплуатации средств защиты информации;
- проверка выполнения рекомендаций, изложенных в заключениях (предписаниях) по проверке технических средств;
- проверка применимости имеющихся тестовых программ для данного исследуемого технического средства;
- проверка организации тестового режима работы с учетом требований, накладываемых параметрами используемой контрольно-измерительной аппаратуры:
- измерение уровней ПЭМИН и наводок информативных сигналов на объектах:
- электрической составляющей;
- магнитной составляющей;
- проверка наличия паразитной генерации, измерение реального затухания в опасных направлениях и линиях, имеющих выход за границы контролируемой зоны;
- измерение параметров применяемых средств защиты фильтров в отходящих линиях активного зашумления и т.д.;
- оценка возможности утечки информации за счет неравномерности тока потребления из сети электропитания;
- оценка возможности утечки информации при активном воздействии на СВТ высокочастотного воздействия и навязывания.

Требования по безопасности информации включают в себя:

- оценку выполнения проверяемых требований по защите информации и возможности ее обработки;
- оценку полноты представленной документации по использованию средств защиты информации;
- рекомендации и предложения по устранению выявленных недостатков, системы защиты информации на объектах в соответствии с установленными требованиями и совершенствованию этой системы, а также рекомендации по контролю за функционированием систем в объекте;
- установка в незащищенных каналах связи, линиях, проводах и кабелях, выходящих за пределы контролируемой зоны, соответствующих фильтров для защиты высокочастотных ТС;
- прокладка проводов и кабелей в экранирующих конструкциях;
- сопротивление заземлителя не должно превышать 4 Ом и заземляющий контур должен находиться в пределах контролируемой зоны;
- кабели электроснабжения необходимо размещать в пределах контролируемой зоны.

SECURITATEA INFORMAȚIONALĂ ÎN ERA TEHNOLOGICĂ

Irina Babară, Marin Lupu
Academia Militară a Forțelor Armate „Alexandru cel Bun"

The development of the means of communication, the shift of the emphasis towards the services economy, with a stress on the technological enhancement have known an irreversible evolution, and have led to results under celerity circumstances and with the engagement of minimal resources. Moreover, an ever visible aspect is the outstanding role of the information as resource and means of ensuring the economic and social progress.

From this point of view, the approach of the elements related to the organizational security and its performances – such as that of managing security incidents – is permanently one of the current themes from a theoretical but especially practical perspective.

Introducere

La începutul mileniului III, în epoca informatizării globale, devin şi mai actuale cuvintele lui Winston Churchill, care afirma că cel ce „posedă informația, stăpîneşte lumea". Într-adevăr, informația este unul dintre principalele active ale business-ului contemporan şi ale administrării de stat, activ care necesită protecție.

Întreaga societate în momentul de față se confruntă cu una din cele mai profunde transformări din întreaga ei existență, în care rolul informaticii este determinant. Trăim astăzi o lume în care sute de milioane de calculatoare, deservind utilizatori foarte diverşi, sunt interconectate într-o infrastructură informatică globală, numită de specialişti şi *Cyberspace* (Spațiul Cibernetic). Specialiştii caută şi găsesc, cu o viteză de-a dreptul incredibilă, soluții tehnice pentru dezvoltarea capacității de comunicație a calculatoarelor şi pentru sporirea calității serviciilor de rețea oferite. Totodată societatea se adaptează din mers noilor tehnologii informatice, învățând să trăiască în această lume nouă, dominată de calculatoare şi comunicațiile dintre acestea.

Securitatea sistemului informatic.

La ziua de azi este evident că sfera informațională, ca factor de organizare a societății contemporane, are o influență activă în situația politică, economică, de apărare şi alte componente ale securității statului. În mare parte, integritatea lumii contemporane, ca societate globală, este asigurată de schimbul informațional.

Globalizarea, este un fenomen amplu dezbătut, nu putea să nu influențeze aspectele legate de securitatea națională, de amenințările privind siguranța oamenilor şi informațiilor, a instituțiilor naționale şi internaționale. Extinderea la scară globală a utilizării diferitelor mecanisme de prelucrare şi comunicare a informațiilor, de control al activităților a condus şi la apariția nevoii de a lua în considerare noile aspecte ce influențează securitatea spațiului cibernetic global.

Implementarea activă şi multilaterală a tehnologiilor informaționale a determinat transformarea structurii societății mondiale, conducînd treptat spre dispariția frontierelor naționale. In toate domeniile de activitate au apărut noi structuri funcționale, la baza cărora se află Rețeaua. Acestea sînt şi corporațiile transnaționale, şi economia electronică

(e-economia), şi asocierea colectivelor ştiinţifice, care lucrează asupra unor probleme comune, dar se află în diferite regiuni ale planetei. Dar aceste schimbări au atins şi partea negativă a vieţii umane. Structurile de reţea au devenit baza criminalităţii mondiale.

Reţelele de calculatoare sunt structuri deschise, la care se pot conecta un numar mare şi uneori necontrolat de calculatoare. Complexitatea arhitecturală şi distribuţia topologică a reţelelor conduc la o mărire necontrolată a mulţimii utilizatorilor cu acces nemijlocit la resursele reţelei- fişiere, baze de date, rutere etc. de aceea putem vorbi de o *vulnerabilitate* a reţelelor ce se manifestă în diferite moduri. Din această cauză un aspect crucial al reţelelor de calculatoare, în mod special al comunicaţilor pe Internet, îl constituie *securitatea informaţiilor*. Utilizatorii situaţi la mari distanţe trebuiesc bine identificaţi-în mod tipic prin parole. Cu părere de rău şi sistemele de parole au devenit vulnerabile, atât datorită hacker-ilor care şi-au perfecţionat metodele cât şi datorită alegerii incorecte a parolelor de către utilizatori. Necesitatea de *securitate* şi de *autenticitate*, apare la toate nivelele arhitecturale ale reţelelor.

În lume s-a creat spaţiul informaţional global unic, în care s-a manifestat o confruntare geostrategică informaţională între marile puteri, pentru atingerea superiorităţii în spaţiul informaţional mondial, în special în megapolisuri, centre-cheie ale societăţii informaţionale globale. Aceasta însă provoacă frecvent situaţii critice, deoarece omul de astăzi este practic permanent supus stresului.

În condiţiile intersectării cu noile provocări şi ameninţări ale naturii, la care omul încă nu a reuşit să se adapteze şi să elaboreze contramăsuri, o actualitate deosebită capătă activitatea de asigurare a securităţii activităţii sale vitale - securitatea în sensul larg cuprinzînd toate domeniile activităţilor umane.

Securitatea naţională şi economia sînt total dependente de tehnologiile informaţionale şi de infrastructura informaţională. Nucleul infrastructurii informaţionale, de care depinde omenirea, se află Internetul. Utilizarea de către infractori a tehnologiilor informaţionale şi telecomunicaţionale, în primul rînd a reţelei Internet, prezintă un pericol serios în procesul de promovare a securităţii societăţii la nivel global. Cea mai importantă problemă de care sunt preocupaţi utilizatorii Internetului este problema securităţii informaţionale.

Utilizării tehnicii de calcul în majoritatea domeniilor vieţii, precum şi conectarea calculatoarelor în reţele internaţionale a dus la faptul că infracţiunea comisă cu ajutorul sau prin intermediul calculatorului să fie mai diversă, mai periculoasă şi mai prezentă la nivel internaţional. La studierea factorilor generatori de acţiuni criminale s-a demonstrat că reţelele de comunicare şi calculatorul modern prezintă caracteristici specifice care sînt de mare utilitate pentru criminali şi implică serioase dificultăţi pentru potenţialele victime şi pentru aplicarea legii (probleme complexe de securizare a sistemelor, diversitatea sistemelor hard şi soft, lipsa de experienţă a multor utilizatori, anonimatul comunicării, criptarea şi mobilitatea internaţională). Grupurile care activează în domeniul crimei organizate, profesionişti în spionajul economic şi serviciile secrete din întreaga lume exploatează deja aceste noi caracteristici ale acţiunilor criminale cibernetice. Multe guverne, mulţi oameni de afaceri, mulţi utilizatori particulari nu realizează pericolul la care sînt expuşi prin aceste noi

condiții de comitere a crimei, nici semnificația protecției împotriva crimei cibernetice şi nici căile tehnice şi legale de contracarare a amenințărilor infractorilor.

Odată cu avantajele şi transformările pozitive pe care le aduce globalizarea la nivelul națiunilor, nu este lipsită de aspecte ce ridică, de multe ori, probleme şi îngrijorare, între care un loc din ce în ce mai important îl ocupă problematica securizării spațiilor cibernetice, cu atît mai mult cu cît fenomenul terorismului a luat o amploare fără precedent, inclusiv terorismul informațional.

În zilele noastre, este din ce în ce mai evident că, grupările teroriste utilizează pe larg Internetul pentru aşi atinge scopurile subversive. Printre cele mai bine reprezentate sînt mişcările de gherilă latino-americane, care dispun de o tehnică informatică de înaltă performanță şi, de multe ori, de masive finanțări ce provin din fondurile unor capi ai traficanților de droguri. În condițiile existenței Internetului, teroriştii au posibilitatea de a lansa atacuri greu detectabile din orice punct al globului. Ei pot infecta sistemele informatice cu viruşi complecşi, care ar putea provoca disfuncționalități grave în sisteme.

Calculatoarele au făcut ca multe activități economice să se desfăşoare mai uşor, dar în mod similar, ele au facilitat şi multe activități ilegale. Utilizarea tehnologiilor informaționale şi comunicaționale a permis ca vechile infracțiuni (de exemplu furtul de bani) să beneficieze de noi modalități de realizare şi a creat noi posibilități de fraudă (dirijarea de fonduri de către personalul angajat, „de încredere", care are sarcina de a actualiza fişierele).

Infracțiunile comise cu ajutorul calculatorului, împotriva afacerilor sau pe seama companiilor economice, sînt comise de angajați, considerați persoane de încredere, sau de persoane din afara organizației (hackeri, concurenți neloiali, grupe criminale). Calculatorul, ca instrument al crimei, este foarte puternic. El nu numai că facilitează comiterea crimei, dar şi conferă infracțiunii un caracter devastator şi face extrem de dificilă identificarea autorului. Rețelele globale de sisteme informatice extind zona expusă infracțiunii şi fac ancheta, urmărirea judiciară şi arestul mult mai dificile. Un hoț care fură o carte de credit obține acces la o sumă mult mai mare decît cea la care ar avea acces un hoț care fură un portofel. Informații confidențiale privind afacerile pot fi furate din calculatoare şi sisteme de comunicare verbală fără să rămînă vreun semn care să indice intervenția unui terț prin „forțarea uşii".

Printre alte consecințe negative ale informatizării, cauzate de dereglarea securității informaționale, se numără terorismul şi huliganismul informațional. Dacă hacherii pătrund în memoria sistemelor computerizate pentru satisfacerea ambițiilor proprii, apoi cracherii mai şi „storc" băncile informaționale. Asemenea „specialişti" sînt extrem de periculoşi pentru sistemele computerizate care dirijează rachetele de luptă, arma cosmică şi nucleară. Consecințele amestecului lor „profesional" nu este greu de ghicit. Acest lucru poate deveni o tragedie nu numai pentru o țară, dar şi pentru întreaga omenire.

Nivelul de securitate al calculatoarelor şi al rețelelor instalate în bănci, întreprinderi, administrații şi organizații militare rămîne nesatisfăcător. O demonstrează miile de exemple de penetrări realizate de piratii informatici, sabotaje, hold-up-uri electronice soldate cu milioane de dolari transferați.

Atacurile cibernetice asupra rețelelor informaționale ale oricărei țări pot avea consecințe grave, cum ar fi întreruperea funcționării unor componente-cheie, provocarea

pierderilor de venituri şi proprietăți intelectuale sau chiar pierderea vieților omeneşti. Contracararea unor astfel de atacuri necesită crearea unor componente riguroase, cum încă nu există în prezent, dacă se doreşte reducerea vulnerabilităților şi prevenirea sau diminuarea forței capacităților îndreptate împotriva infrastructurilor critice.

Ca rezultat al globalizării factorilor economici, politici şi militari, al expansiunii rețelelor şi sistemelor informaționale globale, guvernele lumii, organizațiile internaționale sînt nevoite să-şi concentreze şi mai mult eforturile asupra asigurării securității globale, pentru că acum riscurile sînt mai mari ca oricînd, din cauza efectului de propagare în lanț. Dacă pînă la apariția rețelei globale asigurarea securității sistemelor informaționale era o problemă de politică națională, în momentul de față la stabilirea strategiilor şi politicilor de securizare a spațiului cibernetic trebuie luate în considerare şi aspectele de compatibilizare şi standardizare la nivel global.

Pe de o parte, foarte puține unități au proceduri stricte în vederea asigurării securității informațiilor. Pe de altă parte, la nivel național există proceduri foarte riguroase privind secretul de stat. De regulă, există o ierarhie a ceea ce este cunoscut sub numele de clasificare, prin care orice document şi alte elemente importante sînt încadrate într-o anumită categorie.

Se practică două strategii de bază pe linia securității naționale:

1. Tot ceea ce nu este interzis este permis.
2. Tot ceea ce nu este permis este interzis.

În multe țări de pe glob, accesul la informațiile naționale este controlat prin legi privind secretul de stat, folosindu-se cea de-a doua strategie.

Statul, ca subiect de bază în asigurarea securității informației prin intermediul organelor puterii legislative, executive şi judiciare, trebuie să asigure crearea condițiilor privind realizarea securității şi coordonarea acțiunilor de securitate.

Scopurile securității informaționale trebuie să fie stabilite pe baza priorităților constante ale securității naționale ce corespund sarcinilor de lungă durată ale dezvoltării mediului informațional al societății, incluzînd:

- apărarea intereselor naționale ale statului în condițiile globalizării proceselor informaționale şi formării rețelelor informaționale globale;
- asigurarea organelor puterii şi conducerii de stat, persoanelor fizice şi juridice cu informație veridică, completă şi oportună, necesară pentru luarea deciziilor; prevenirea încălcării integrității resurselor informaționale de stat, utilizării lor nelegitime şi ineficiente;
- realizarea drepturilor cetățenilor, organizațiilor şi statului în vederea obținerii, difuzării şi utilizării informației;
- susținerea normelor democratice, în special a principiilor de interacțiune a statului, societății şi persoanei în mediul informațional, în calitate de agenți realmente egali ai relațiilor democratice;
- protecția informațională a cetățenilor.

Activitățile de bază trebuie orientate pe următoarele direcții: depistarea, evaluarea şi pronosticarea surselor de pericol pentru securitatea informațională, elaborarea unui

complex de măsuri şi mecanisme pentru realizarea acesteia; crearea bazei normativ-legale de asigurare a securității informaționale, coordonarea activității organelor puterii şi administrării de stat, structurilor menite să asigure securitatea informațională; dezvoltarea sistemului de asigurare a securității informaționale, perfecționarea organizării ei, a formelor, metodelor şi mijloacelor de prevenire şi neutralizare a pericolelor securității informaționale, lichidarea consecințelor prejudicierii.

Dependența de informație este tot mai mare, chiar periculoasă. Există state care depind totalmente de informațiile oferite de componentele spațiului cibernetic național. Blocarea acestuia timp de cîteva ore poate să conducă la instaurarea haosului în țara respectivă, afectînd, în bună măsură, şi securitatea sistemului informațional global.

Experții au declanşat o nouă ofensivă pentru perfecționarea legislației, întărirea rolului agenților de profil şi perfecționarea produselor pentru prevenirea şi descoperirea delictelor informaționale şi informatice. Deşi fenomenul infracționalității informaționale afectează majoritatea instituțiilor publice şi private, cu consecințe de nebănuit, el capătă accente catastrofale cînd este vorba de siguranța şi apărarea națională, unde sistemul informațional are o importanță vitală în prelucrarea informațiilor şi în asigurare fundamentării deciziilor.

Iată de ce se impune cu acuitate necesitatea acordării unei atenții sporite securității informațiilor, în primul rînd prin asigurarea unei corecte clasificări a lor, dar şi prin elaborarea unor strategii coerente de securizare a spațiului cibernetic.

Concluzie

Securitatea informațională este un domeniu mult prea vast şi cu prea multe domenii conexe pentru a fi detaliat complet undeva. Lumea este în continuă mişcare, cerințele de securitate şi confidențialitate cresc pe zi ce trece, amenințările țin pasul.

Acest scurt articol a avut rolul unei introduceri generale ale principalelor aspecte din securitatea electronică din ziua de azi.

În concluzie accentuăm că noile condiții ce implică dezvoltarea societății informaționale pe baza utilizării rețelelor informaționale globale, dezvoltarea schimbului informațional transfrontalier, globalizarea sistemului economiei mondiale şi creşterea nivelului informatizării necesită scoaterea în evidență a factorilor care anterior nu reprezentau amenințări considerabile. Aceşti factori fac ca securitatea intereselor naționale în sfera informațională să fie un element important al securității naționale a statului.

Bibliografie

1. Bellamy BJ. Vulnerability Identification and Remediation Through Best Security Practices, SANS Institute, 2002.
2. Grime R.- Implementing Vulnerability Scanning in a Large Organisation, SANS Institute, June 2003.
3. Lundin E., Jonsson E. Survey of Intrusion Detection Research, Technical Report nr. 02-04, 2002.
4. Patriciu Victor-Valeriu, Pietroşanu-Ene Monica, Bica Ion, Cristea Costel-Securitatea informatică în UNIX şi INTERNET, Editura Tehnică, 1998.

5. Patriciu Victor-Valeriu, Pietroşanu-Ene Monica, Bica Ion, Priescu Justin-Semnături electronice şi securitate informatică. Aspecte criptografice, tehnice, juridice şi de standardizare, Editura BIC ALL, 2006.
6. Petersen R.Security Breaches: Notification, Treatment and Prevention, EDUCAUSE review, July/August 2005.
7. Vasilescu Andrei, Rachieru Dan, Vasile Irina, Filip Luminița, Vasilescu Elena-Ghid de aplicare a recomandărilor europene referitoare la confidențialitatea comunicațiilor, INSCC, decembrie 2005.
8. Walters N. –Into the Breach: Security Breaches and Identity Theft, AARP Public Policy Institute, July 2006.

MAIN STAGES IN DEVELOPMENT OF SOFTWARE APPLICATIONS IN TELECOMMUNICATIONS

Asst. Prof. Natalia Futekova
University of National and World Economy – Sofia,
Department of Information Technologies and Communications

The paper examines the main stages in the development of software applications in telecommunications. The paper presents the characteristics and peculiarities of the processes of analysis, design, software, programming, testing and user training. On this basis, conclusions and recommendations are formulated.

1. Introduction

The software applications are complex systems that have many characteristics in its functionality, terms of architectural organization, steps in deployment and more. On the other hand, the field of telecommunications has a number of characteristics. In our opinion, no one can give a simple answer to the question of what exactly are the stages of implementation of software applications for telecommunications, as well as their duration and efficiency. We maintain a sequence of stages of implementing similar software, which gives a finishing process and allows making timely and appropriate decisions in this area of the economy.

2. Main stages

The main stages in the development of software applications in telecommunications are given in Figure 1.

Stage 1 "Business Research" is the starting point from which begins the implementation of the software application. At this stage we will mainly have to conduct a detailed study of the analyzed firm or company in which the software application is implemented. We need to provide all necessary information for subsequent rounds. We

do mainly planning activities throughout the project implementation and for this purpose we should examine the business environment. The characteristics of the analyzed company are also exploring the desires and needs of the client. Here the main emphasis is on the unsolved or partially solved problems in the subject area and their implications for making management decisions.

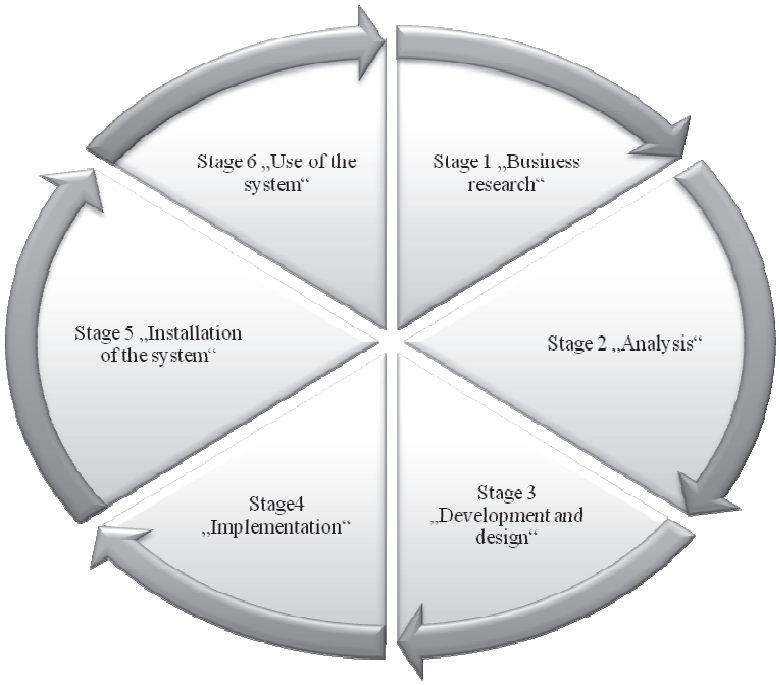

Figure 1. **Main stages in the development of software applications in telecommunications**

Stage 2 "Analysis" is the second major stage in the process of full implementation of the application. It aims at a detailed study and analysis of existing business processes and their impact on the final result achieved in the implementation. In this phase we should focus on defining the detailed work schedule and proper project scope definition. We believe that, on this base implementation, the team involved should prepare a model of project management and should determine the appropriate approach in the design of the system architecture based on a comparative analysis of knowledge in theory and applied in practice design methods. This gives us a reason to define criteria, indicators and benchmarks for success and development of a plan for identifying, planning and controlling risk.

Stage 3 "Development and design" comes after the stage of analysis. Its aim is to create complete project documentation on the design of a system implementation. To achieve this it is necessary that we develop a training plan in detail and plan for dissemination of results. Important part of this stage is to manage the state information and execution of project management proposals and quality management. During this

stage of implementation it is necessary to create conceptual, technical and security system design implementation. This means achieving a complete pipeline system and creating the necessary conditions for the creation and development of additional functionality.

Stage 4 "Implementation" has the primary goal of full program implementation (programming) of already designed system functionality. At this stage we need to create the necessary functionality that has been researched and designed based on the results of the previous stages. This stage also carries out the development project set up to design, development of design functionality of the system and the development of scenarios for testing the main use cases.

Stage 5 "Installation of the system" has as main task the designed and implemented ERP system to be installed in accordance with the plan made and to become a fully functioning software application. At this stage we must achieve final completion of system readiness, planning and conducting user training, performing testing and user acceptance.

Stage 6 "Use of the system" aims that the ERP system is finally delivered to the client and moved to her work in real life. It should not be said that at this stage the system's lifecycle ends because it is needed a period in which the system is observed and maintained. This is a prerequisite for the development of the system. At this final stage we should mainly focus on the completion of the project, planning the use of the system in real conditions, creating conditions for project support and review the results. All this creates conditions for the development and management of change.

3. Conclusion

Finally, it should be noted that in this material we have made an inventory survey of the key steps in developing and deploying software applications in telecommunications, as a prerequisite for improving information security of the business.

ПРОБЛЕМЫ ИНСАЙДИНГА

Татьяна Чикарёва,
Молдавская Экономическая Академия
(Республика Молдова)

The purpose of this article is to study the problems of insiding and the means which are used in order to withstand the actions of insider. Persons who are not attentive with confidential information are the object of this article.

Проведённое в 2003 году исследование в рамках программы «Информационная безопасность» показало, что 90% офисных работников готовы разгласить конфиденциальную информацию, например свои пароли, за какую-либо услугу или

вознаграждение. Это пример «Кви про кво», то есть «услуга за услугу», одна из техник социальной инженерии. К самостоятельным непреднамеренным инсайдерам применим данный термин «социальная инженерия» [1,2,4].

Очень выгодно быть мотивированным инсайдером, продающим конфиденциальную информацию вовне. Это классический пример инсайдеров. Хайнрих Кибер в феврале 2008 года выручил более 7 миллионов долларов, продав приватную базу своего бывшего работодателя из лихтенштейнского банка LGT немецким и британским спецслужбам. Наглядно доказано, что прибыльно заниматься банковским инсайдом [2].

Инсайдинг, по нашему мнению, – это угроза для предприятия, когда конфиденциальная информация становится публичной или частично публичной; когда в обход преградам политики безопасности злонамеренный инсайдер получает доступ к конфиденциальной информации и способствует установлению вредоносного программного обеспечения на свою машину корпоративного пользователя.

Инсайдер – работник организации, имеющий доступ к конфиденциальной информации, недоступной другим лицам, или широкому кругу лиц. Также, слово может нести негативный оттенок. Например, лицо, опубликовавшее конфиденциальную информацию, или передавшее её лицам, не имеющим доступ к данной информации [2].

Следует выделить основные мотивы инсайдинга. Среди них основными являются следующие:

- во-первых, многие сотрудники готовы на инсайдинг взамен на какое-либо вознаграждение;
- во-вторых, инсайдинг – это очень прибыльное занятие для инсайдеров;
- в-третьих, для самого предприятия, подвергающегося инсайдингу, это очень убыточное и вредоносное событие.

Для защиты конфиденциальной информации и предотвращения её утечки используются следующие средства противостояния действиям инсайдера:

- ограничение доступа подключаемых к компьютеру носителей информации, чтобы не было возможности скопировать базу данных на флэш-накопитель, к примеру;
- проверка входящей и исходящей электронной почты, используемой для связи с лицами, которые не являются персоналом предприятия [2];
- установка ограничений на прикрепление внутренних документов в письмах внешней почты;
- организация доступа для обмена внутренними документами только по внутренней корпоративной электронной почте;
- разработка адекватной политики мер безопасности на основе законодательной базы;
- обучение персонала защите конфиденциальных данных организации для избежания непреднамеренного инсайдинга, для защиты от «социальной инженерии»;

Проблема инсайдинга довольно-таки остро выражена, так было и так будет, но принимать необходимые меры борьбы с ней всё равно нужно. Для борьбы с этим явлением – все средства хороши, только использовать их нужно рационально и продуманно.

Руководство предприятий должно быть всегда проинформировано о том, что нет абсолютно идеальной политики безопасности на практике, и определённая доля угрозы всегда висит над предприятием. Этот факт должен всё время подстёгивать для периодических проверок персонала, анализа и повышения степени электронной защиты информации. Но это не значит, что бюджет для таких мероприятий безграничен, напротив, он должен быть почти всегда ниже оценочной суммы риска появления такой угрозы и её ликвидации [3].

Развивать организационный, технический уровень предприятия это очевидным образом необходимо с целью опередить действия и планы промышляющих на рынке инсайдеров.

Технический уровень предприятия можно развивать следующим набором программных средств и инструментов для защиты данных [5]:

- Cisco Security Agent (CSA) – объединяет в одном решении различные защитные механизмы и функции по предотвращению атак, защиты от вредоносного кода, блокирования утечки информации через USB-порты и другие внешние устройства [6];
- Cryptic Disk – приложение позволяет легко и надежно зашифровать диски и отдельные разделы на винчестере, защитив их от несанкционированного доступа паролем; при этом вся информация, находящаяся на защищённом диске или записываемая на него, будет автоматически шифроваться [7];
- Safe'n'Sec - программный модуль, выгодно отличается от большинства приложений, предназначенных для обеспечения безопасности; следит за активностью разнообразных приложений, процессов, а также за атаками извне и блокирует любые потенциально опасные действия, анализируя не код приложений, а их активность; Safe'n'Sec может защитить даже от самых новых вирусов, которые ещё не были созданы на момент установки программы на компьютер [8];
- Zlock – утилита для защиты от копирования информации на мобильные накопители [9-10].

Наряду с использованием готовых программных продуктов, описанных выше, следует рекомендовать: для организации правильной системы разграничения доступа к информации – применение матричного разграничения доступом ко всем электронным файлам и документам предприятия; для защиты операционной системы каждой рабочей станции предприятия – использование всеми сотрудниками в обязательном порядке сложного, трудноподбираемого пароля от 8 символов для санкционированного входа в систему; для правильной работы операционной системы на всех рабочих станциях фирмы - отключение неиспользуемых служб для защиты компьютеров от внешних угроз [11].

В вопросах информационной безопасности необходимо быть всегда осторожными и внимательными, чтобы прогрессировать, и не забывать, что «знание – сила».

Литература:

1. John Leyden "Office workers give away passwords for a cheap pen" http://www.theregister.co .uk/2003/04/18/office_workers_give_away_passwords/
2. Григорий Бортэ «Классификация инсайдеров» http://security.ase.md/materials/si2010/30-pag_96-98.pdf
3. Иван Бабенко «Инсайдер: суть явления, угрозы, противодействия» http://www.security.ase.md/publ/ru/pubru101/2.pdf
4. Алексей Комаров «Защита от инсайдера» http://www.osp.ru/search/?text=Алексей+Комаров+«Защита+от+инсайдера»&section=all&sTime=
5. Зинаида Гулка, Ольга Гешова «Организация программно-аппаратной защиты информации от инсайдеров» http://www.security.ase.md/materials/si2010/32-pag_102-106.pdf
6. Решение Cisco Security Agent для предотвращения утечки данных http://www.lwcom.ru/solutions/doc.php?do=read&doc=72
7. Козырев А.А. Информационные технологии в экономике и управлении: Учебник /А.А.Козырев. –СПб.: Изд-во Михайлова В.А., 2000. – 360 с.
8. Конев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.
9. Мельников В. Защита информации в компьютерных системах. – М.: Электроинформ, 2005.- 102 с.
10. ZECURION – Защита информации от утечек (DLP) http://www.zecurion.ru/products/zlock/
11. SurfControl E-mail Filter. Максимальная защита входящей и исходящей электронной почты от спама, вирусов и нежелательных материалов http://www.surfcontrol.ru/products/email/

PROTECȚIA INFORMAȚIILOR CLASIFICATE, ÎN ERA INFORMAȚIONALĂ

Iulian Mihăescu
infoprotect.md

The presentation makes a brief analysis of classified information security management system, particularly information protected by acredidate IT systems, which store, process or transmit classified information.

Securitatea națională este reprezentată de starea de legalitate, de stabilitate economică, politică și socială care conduce la fundamentarea existenței și dezvoltării statului și menținerea ordinii de drept, respectarea drepturilor și libertăților fundamentale ale omului, de aceea informațiile cu relevanță în acest domeniu necesită o atenție deosebită, manifestată prin secretizarea informațiilor.

De-a lungul timpului au existat categorii de informații care au fost exceptate de la accesul liber și neîngrădit al oricărui cetățean, limitare justificată de autoritățile statului, dar de multe ori contestată pentru încălcarea drepturilor omului. Mass-media și opinia publică au contestat în nenumărate rânduri, faptul că multe informații au fost exceptate de la liberul acces în mod nejustificat sau printr-o clasificare excesivă, dar există și informații care necesită un anumit nivel de protecție atunci când interesele naționale, unele măsuri de protecție a persoanelor, datele de identificare ale acestora, concurența loială, anumite proceduri judiciare, interese economice și politice strategice ale unui stat, impun luarea acestor tipuri de măsuri.

În orice stat exista informații de interes public și informații care nu sunt destinate publicității, care datorită importanței lor necesita un anumit nivel de protecție, fie că diseminarea neautorizată a lor ar aduce prejudicii persoanei fizice, juridice sau mai grav, ar produce daune intereselor naționale, securității naționale sau oridinii publice. Așadar indiferent de necesitatea ce a dus la protecția informației, acest fapt reprezintă o restrângere a liberului acces al peroanelor prevăzut majoritatea legilor fundamentale ale democrațiilor dar și în numeroase reglementări internaționale.

Măsurile restrângerii liberului acces la informații trebuie aplicată într-un mod nediscriminatoriu, realizată în concordanță cu reglementările internaționale privind drepturile omului, fiind foarte importantă o educare a cetățeanului privind aspectele care conduc la restricționarea liberului acces și motivarea importanței limitării. De-a lungul timpului au fost înregistrate cazuri de clasificate excesivă a informațiilor din partea organelor administrației publice cu atribuții în domeniu apărării, ordinii publice și siguranței naționale.

Situațiile de limitare a accesului sunt clar definite, atât de Constituție, de legile în vigoare ale statelor democratice, cât și de acte la nivelul Uniunii Europene sau al Alianței Nord Atlantice.

În majoritatea statelor democratice, informațiile exceptate de la liberul acces, vizează:

1. informațiile secrete de stat din domeniul apărării, ordinii publice și siguranței naționale
2. informațiile secrete de serviciu
3. informațiile privind datele cu caracter personal, potrivit legii
4. deliberările autorităților și informațiile de interes economic, dacă sunt clasificate
5. informațiile privind activitățile comerciale, dacă prin publicarea lor se aduce atingere principiilor concurenței loiale
6. informațiile privind procedurile judiciare, daca furnizarea lor vor aduce atingere unui proces echitabil
7. informațiile care prejudiciază masurile de protecție a tinerilor
8. informații privind proceduri de anchetă penală sau disciplinară dacă dezvăluirea lor afectează rezultatu final al anchetei

Noua eră informațională a impus majorității statelor membre ale Uniunii Europene și NATO, gestionarea informațiilor clasificate în format electronic.

În vederea acreditării de securitate a sistemelor informatice și de comunicații care stochează, procesează sau transmit informații clasificate, se impun anumite măsuri specifice. Astfel există metode specifice de acreditare care stabilesc cerințele aferente

procesului de acreditare a entităților evaluatoare a produselor și soluțiilor de securitate IT precum și a sistemelor informatice și de comunicații.

Foarte importantă este stabilirea structurilor și a personalului cu atribuții în domeniul INFOSEC principalele responsabilități ale acestora, în scopul asigurării protecției corespunzătoare a informațiilor NATO sau UE clasificate.

În contextul aderării la Uninunea Europeană și la Alianța Nord-Atlantică, majoritatea statelor din UE au încheiete între ele, acorduri reciproce de protecție a informațiilor clasificate. Deasemenea acestea, dețin structuri de legătură cu NOS (NATO Office of Security).

În România, organismul de legătură cu NOS, este Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS), cade joacă rol de Autoritate Națională de Securitate, ce se află în subordinea Guvernului României. ORNISS, desemenea este responsabil cu implementarea politicilor de protecție a informațiilor clasificare aparținând Uniunii Europene. Astfel structurile de securitate, care au atribuții de protecție a informațiilor clasificate, la nivelul fiecărei insituții publice sau agent economic, gestionar sau emitent de informații clasificate, în vederea aplicării măsurilor de protecție a informațiilor NATO sau UE clasificate, sunt obligate să își înființeze un Registru Intern, subordonat nemijlocit Registrului Central al ORNISS.

Echivalența nivelurilor de clasificare a informațiilor NATO – UE:

N.A.T.O.	U.E.
NATO COSMIC TOP SECRET	TRES SECRET UE/ EU TOP SECRET
NATO SECRET	SECRET UE
NATO CONFIDENTIAL	CONFIDENTIEL UE
NATO RESTRICTED	RESTREINT UE
NATO UNCLASSIFIED	LIMITE UE

ВНУТРЕННИЙ КОНТРОЛЬ В СИСТЕМЕ КОРПОРАТИВНОГО УПРАВЛЕНИЯ

Павлова Лилия
Экономическая Академия Республики Молдова (ASEM),
IT&IS Management SRL, Республика Молдова

В последнее время отмечена тенденция к изменению роли внутреннего контроля в системе корпоративного управления, ожидая от него содействия в достижении целей бизнеса. Системы контроля в той или иной форме существуют в каждой компании, но необходимо отметить, что практика формирования в Республике Молдова полноценных систем внутреннего контроля только начинает складываться.

При построении системы корпоративного управления в компании важным является обеспечение прозрачности управленческих и бизнес процессов для

руководства компании и ее собственников, как основы принятия эффективных и своевременных управленческих решений. Важной составляющей корпоративного управления является организация системы внутреннего контроля, посредством которой обеспечивается сохранность активов, выявление и мобилизация имеющихся ресурсов, необходимый уровень управления рисками, формируются условия для повышения эффективности корпоративного управления.

Каждая управленческая функция, реализуемая в компании, интегрирована с одной или несколькими контрольными процедурами, что в свою очередь вызывает затруднения для отделения контрольной функции или процедуры от управленческих.

Система внутреннего контроля компании характеризуется следующими компонентами:

- Контрольная среда и нравственный климат – задают тон функционирования компании и являются основой для других компонентов. Контрольная среда включает этические ценности и профессиональную компетенцию персонала компании, стиль работы руководства, разграничение полномочий и обязанностей;
- Управление и оценка рисков - заключается в выявлении и анализе как внутренних, так и внешних рисков, ставящих под угрозу достижение целей компании, а также реагировании и внедрении механизмов снижения выявленных рисков;
- Информационное обеспечение и связь – включает выявление, сбор и анализ необходимой информации, позволяющей персоналу исполнять свои обязанности. Информационные ресурсы обеспечивают идентификацию, хранение и обмен своевременной информацией в подходящей форме;
- Существующие контрольные процедуры - контрольные мероприятия включающие политику и процедуры, которые помогают гарантировать, что распоряжения руководства выполняются, и необходимые шаги для предотвращения рисковых ситуаций сделаны. Действия по контролю предпринимаются в рамках всей компании, на всех уровнях и во всех структурных подразделениях, включая комплекс таких мер, как согласования, разрешения, подтверждения, проверки, обзоры всех видов деятельности компании, обеспечение безопасности персонала и активов компании;
- Мониторинг средств контроля - процесс оценки эффективности функционирования системы внутреннего контроля в течение определенного периода. Данный процесс включает анализ и оценку организации и функционирования средств и мер контроля, планирование и осуществление необходимых корректирующих мероприятий, адаптированных в зависимости от изменений в окружающей среде, проверку выполнения требований всех внутренних положений компании.

Каждый из компонентов системы внутреннего контроля оказывает влияние на ее качество и результативность.

Эффективность и качество системы внутреннего контроля находятся в прямой зависимости от действий руководства, так как контроль является важной составляющей процесса управления. При этом система внутреннего контроля должна разрабатываться и функционировать строго в пределах утвержденной организационной структуры компании и в рамках выполняемых задач структурными подразделениями. Неадекватное увеличение объема контрольных процедур может привести к потере контроля, в том числе и над критичными процессами.

В зависимости от размеров компании и разнообразия ее видов деятельности формируется организационная структура и определяется ее влияние на результаты деятельности компании. От степени детализации информации, описывающей организационную структуру компании, зависит эффективное распределение функций и задач между структурными подразделениями. Без полноценной и работоспособной организационной структуры невозможно обеспечить эффективность системы корпоративного управления и внутреннего контроля в компании.

Регламентация деятельности компании также оказывает существенное влияние, как на корпоративное управление, так и систему внутреннего контроля. Регламентация деятельности структурных подразделений и персонала компании включает положения, регламенты, процедуры и инструкции. Важно отметить, что отсутствие регламентации ряда бизнес-процессов приводит к тому, что организация качественной системы внутреннего контроля становится невозможной. Отсутствие регламентации процессов также является следствием возникновения противоречий в системе корпоративного управления, размыванием границ ответственности руководителей структурных подразделений.

Информационная инфраструктура компании, а также используемые информационные ресурсы, влияют на качество и надежность информационного обмена как внутри компании, так и с третьими сторонами. В прямой зависимости от используемых информационных систем находится и обеспечение своевременности и полноты поддержки информационных запросов ответственных лиц.

В компании не может быть результативной системы внутреннего контроля без налаженной и эффективной системы управления рисками. При этом целью внутреннего контроля при построении системы управления рисками является внедрение в текущие бизнес процессы компании таких контрольных процедур, которые позволяют минимизировать вероятность наступления риска либо его последствия. Взаимодействие систем внутреннего контроля и управления рисками определяется, как задача системы внутреннего контроля вовлечения персонала в управление рисками, встраивая в бизнес-процессы контрольные процедуры.

Отлаженные системы внутреннего контроля и управления рисками позволяют обеспечить защищенность компании, выявить риски, сформировать и скорректировать план мероприятий по минимизации и реагированию на риски, отладить бизнес процессы компании и обеспечить ответственность за контроль и управление рисками.

Участниками систем внутреннего контроля и управления рисками являются все сотрудники компании, а функционирование данных систем основывается на принципе подотчетности всех ее участников. В качестве практики используется закрепление владельцев ключевых рисков, на которых возложена обязанность по

регулярной актуализации рисков и персональная ответственность за организацию работы по управлению рисками.

Система внутреннего контроля является основой корпоративного управления, посредством грамотного проектирования и использования которой снижается неопределенность, уменьшаются риски, тем самым позволяя со стороны взглянуть на деятельность компании в целом.

Система внутреннего контроля является одной из функций управления для постоянного наблюдения и проверки функционирования компании с целью оценки обоснованности и эффективности принятых управленческих решений, выявления и предупреждения неблагоприятных ситуаций. Вне зависимости от рода и масштаба деятельности компании в основе внимания должна быть четко выстроенная, отлаженная, гибкая и своевременно реагирующая на любые изменения система внутреннего контроля.

Литература

1) Committee of Sponsoring Organizations the Treadway Commission. Guidance on Monitoring Internal Control Systems. http:// www.coso.org
2) Амброжевич О. Борьба с мошенничеством с помощью системы внутреннего контроля, Сентябрь 2010
3) Винтер Г. Внутренний контроль: развитие и риски. Симпозиум по проблемам аудита, Университет Канзаса, Делойтт, 1992 г.
4) Постникова О.Г. Система внутреннего контроля в корпоративном управлении. МГУ им. М.В. Ломоносова. [Cited: January 10, 2012.] http://www.econ.msu.ru/cmt2/lib/a/1178/file /Postnikova.pdf.

UNCERTAINTY OF THE INFORMATION IN ANALYSIS OF THE ENVIRONMENTAL AND ERGONOMIC RISK OF EQUIPMENT FOR ENVIRONMENTAL PROTECTION

Plamen M. Manev Lyubomir V. Vladimirov
University of Ruse, Bulgaria

The purpose is to analyze the uncertainty of information analysis in environmental and ergonomic risks arising from the operation of facilities for environmental protection. For its implementation are solved two problems. Firstly it is analyzed the uncertainty of the information environment. Then it is revealed the unclarity in the use of the conceptual apparatus.

Key words: information, risk, uncertainly, vagueness.

The information insecurity envelopes all spheres of the public life. Most often it is interpreted as uncertainty, unclarity and even inadequacy. It can be seen as ambiguity, suspicions, problematic, using fuzzy and/or alternating linguistic apparatus and more. So defined the information environment carries a vague, unverified, and the fuzzy and occasional character – all the elements of an insecurity. The use of this information in the

process of building different models, including models of risk, can cause any serious errors, incorrect results, and as a result - wrong decisions.

The purpose of the paper is to analyze the insecurity of the information environment and to insurance, seen as a stage in the complex process of risk analysis arising from the equipment for environmental protection. For its implementation it is necessary to solve the following tasks: 1) insecurity analysis of the information environment, 2) the disclosure of the unclarity, arising from the use of the conceptual apparatus.

The risk analysis is a complex and multi-component process, incorporating the definition and the identification of the risk elements. It is an integral part of risk management and, in turn, includes a number of components to be analyzed. The critical point in the procedure is to identify dangers and to define the likely scenarios of danger phenomena and events. The judgments about the severity of injury and probability of occurrence are based on it. On its fundament the different possible combinations of events leading to damage with specific weights and probabilities of occurrence and the realization is made and risk assessment.

For detailed identification of risk factors that generate dangers it is necessary to have a huge data base. It is a function of the nature of component data that have varying degrees of uncertainty, since they are random variables.

For the unsecurity analysis of information insurance in risk analysis from the operation of facilities for environmental protection, a system of defining and interpreting basic classes, categories, groups and units for risk uncertainty in measurements is developed [1]. The system includes definitions and interpretations of uncertainty taxonometric units. The two main types of insecurity were used and on them it is based a hierarchical structure. Two multi-component areas of insecurity are defined: Region I. Uncertainty and Region II. Uncertainty (n -meaningfulness). For the purposes of this study the constituent components are adapted to the problems of information security risk assessment from the operation of facilities for environmental protection.

In the hierarchy of information insecurity, the uncertainty has lowest level, and the reasons for their appearance is considered as a function of: 1) measurement of variables - environmentally and ergonomically danger phenomena, impacts, effects, 2) variability of the indicators over the time and space, and 3) linguistic errors in formalization of the dangers of facilities for environmental protection, 4) differences and discrepancies in the opinions between experts about the risk structure, 5) various methodologies to measure the environmental and ergonomic risk and the resulting variety of decisions; 6) inconsistent prioritization of the critical events occurring in the environment and the management of the equipment for environmental protection. These reasons spelled quantifiable indicators of uncertainty. The uncertainty of risk models should be considered, as modeling is widely used, and sometimes the only method of analysis and risk assessment.

The iinadequacy of the information when modeling the environmental and ergonomic risks is due to: 1) the variability and randomness of the processes in investigated facilities to protect air, water, soil and waste in their local ergonomic systems and their place in the global urban systems, 2) ignorance or incomplete

knowledge of the elements of the surveyed facilities, 3) incorrect formalization of the structure of the investigated systems, 4) subjective errors in analytical risk analysis, 5) the occurrence of insufficiently known natural phenomena. These discrepancies with the objectivity of critical phenomena, impacts and effects leads to inaccurate determination of the risks parameters, which deceives and leads to incorrect management decisions.

The unclarity (*n* -meaningfulness), in analogy to the uncertainty is the second factor in the information insecurity analysis and risk assessment of facilities for environmental protection. Its subjective component is associated with feeling, perception, and perception of risk. There are errors arising in the communication of subjects with different temperament and character. The information perceived as a danger in some situations may seem to other situations as safety. Consequently, priority ranking tasks for protective, corrective - reducing or compensative actions need to be rearranged, but their temporal ranges must be substantially changed.

All the concepts must be used in a clear and understandable to participants in the processes way. This can be done by just linguistic modeling of critical events having ecological and ergonomic nature. Therefore, the most important is risk - linguistics and its component the risk - lexis. The causes of unclarities in the information are generally associated with the use of fuzzy terminology and words that do not conform to conventional and specialized terminology used in the identification, analysis, evaluation, management and risk reduction. For a detailed presentation of the correct information it should be used linguistic diversity. Must be used words with precise meaning of natural language researchers. When using foreign words in the terminology, which inevitably required, they must be accepted in the theory of ecological and ergonomic risk. This is the way of creation of simple and approachable linguistic model of risk situations and events, including in the field of analysis and risk assessment of the operation of facilities for environmental protection.

The ways and methods of formalization of causality and the semiotics of risk are two other characteristics of the risk - linguistics. The ignorance or failure to comply with the rules of phraseological description of causality in the emergence and development of risk factors at the first and non-accepted, verification and testing of the basic risk items, syntactic rules and semantic rules and axiomatic in the second one are causes of linguistic ambiguity nature. As consequences of the above reasons it can be understand the analysis of the documentation describing originated and implemented critical events. In the documents, records, declarations, conclusions for accidents, anthropological and natural disasters and accidents have used phrases, expressions, phrases, and definitions that make information unusable and unfit. For a description of such events it should be used concepts, even out of context should be clear and precise and to prevent the manifestation of variety of meanings.

In the present paper it is revealed in details the uncertainty of information when analyzing the risk from implementation of the equipment for environmental protection. The uncertainty in terms of the information environment and unclarity (*n* –mea-

ningfulness) arising from the use of specific terminology were considered. The critical nodes and the levels of hierarchical structure for defining and interpreting the major taxonomic classes, categories, groups and units of the insecurity in the analysis of environmental and ergonomic risk facilities for environmental systems were analyzed.

References

1. Vladimirov, L. Riskmetric in environmental security. Monograph. Varna, Varna Free University, 2009.

МЕТРИКИ ТЕСТИРОВАНИЯ – НЕОБХОДИМОСТЬ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ПРОГРАММНОГО ПРОДУКТА.

Сторож Оксана, ASEM

This article is about different metrics. A metric is a measure. A metric system is a set of measures that can be combined to form derived measures. Two main types of metrics are described, they are: initial metrics and determined metrics.

При проектировании и создании какого-либо продукта существует необходимость оценить его качество, т.е. степень соответствия присущих характеристик требованиям. Одним из требований, при проектировании программного продукта, как правило, является отсутствие ошибок в работе программы, но, как известно, устранить абсолютно все ошибки невозможно, в силу постоянно меняющейся внешней среды и соответственно постоянно меняющихся требований, но их количество должно быть сведено к минимуму. Для выявления ошибок необходимо проводить разного рода работы по тестированию качества продукта. А для принятия решения об окончании тестирования, необходимо использовать метрики тестирования и качества. Они позволяют оценить характеристики продукта, степень покрытия тестами функциональности и другое.

Согласно международному стандарту ISO 14598: Метрика - это количественный масштаб и метод, который может использоваться для измерения. Можно выделить два основных типа метрик: метрики первичные, метрики вычисляемые [1]. Первичные метрики – это те, которые накапливаются в результате тестирования, например, количество найденных багов, время, затраченное на прогон тестового сценария, стоимость тестирования и т.д. они являются основой для анализа тенденции. Вычисляемые метрики используются для непосредственной оценки качества продукта, а также для оценки эффективности самого процесса тестирования. В таблицах ниже приведены некоторые примеры упомянутых видов метрик и их описание.

Таблица 1

Первичные метрики

Название метрики	Описание метрики
Количество найденных багов (Opened Bugs)	Позволяет косвенно оценить квалификацию разработчиков, а также используется для расчета затрат, необходимых на устранение, найденных дефектов.
Непроверенные тест кейсы (Not Run Test Cases)	Данная метрика позволяет обратить внимание на те функциональности продукта, которые не могут быть проверены и выявить причины. Например, она может указывать на плохое описание требований в проектной документации, на неквалифицированность тестировщика, на некачественную работу разработчика и др.
Количество переоткрываемых багов (Reopened Bugs)	Если от релиза к релизу значение метрики увеличивается, то это может означать, что требования к функции понимается по-разному разработчиком и тестировщиком, тестировщие не точно описал дефект, разработчик некачественно исправляет дефект.
Количество багов по приоритету (Bugs by Priority)	Большое количество багов с высоким приоритетом может указывать на неверное понимание требований разработчиками.
Время тестирования (Time of testing)	Эта метрика широко применяется при планировании различных видов тестирования и разработке бюджета. Временные затраты напрямую зависят от сложности системы, опыта проектировщиков, разработчиков и тестировщиков, от детальности требований и их документированию.

Кроме описанных в таблице метрик существует еще огромное количество [2]: удачно и неудачно пройденные тест кейсы (Passed/Failed Test Cases), открытые/ закрытые/ переоткрытые/отклоненные дефекты (Opened/ Closed/ Reopened/ Refused Bugs), количество дефектов по приоритету/серьезности/важности для бизнеса (Bug Priority/Severity/Business Importance), объем тестирования, стоимость тестирования и другие.

Таблица 2

Вычисляемые метрики

Название метрики	Описание метрики
Удачно пройденные / Неудачно пройденные тест кейсы в процентном соотношении (Passed/ Failed Test Cases)	При условии, что всегда найдется хотя бы 1 баг, значение метрики от релиза к релизу должно стремиться к бесконечности. Если значение не увеличивается, значит необходимо обратить внимание на квалификацию команды разработчиков.
Отклоненные/открытым багам (Rejected/Opened Bugs)	Если в процентном соотношении количество отклоненных багов велико, это может означать, что разработчики и тестировщики по разному трактуют описание функции с «дефектом». Либо тестировщик не очень точно описал проблему, разработчик не желает или не может исправить проблему, либо не считает это ошибкой.
Плотность ошибок	Эта метрика показывает отношение общего числа дефектов в программном продукте к количеству строк в исходном коде. На основе отслеживания динамики изменения значения этой метрики, делают вывод о необходимости продолжения работ по тестированию или их прекращению.
Полнота тестирования	Метрика указывает на готовность продукта к выходу на рынок. Она высчитывается как отношение планируемого тестового набора к полному тестовому набору введенному в программу на данный момент. На практике это сделать достаточно сложно, поскольку эта процедура

	является очень громоздкой. Также требования к продукту могут со временем меняться и соответственно могут появляться все новые тесты, а старые могут постепенно становится неактуальными.

Необходимо отметить, что вычисляемых метрик гораздо больше первичных, поскольку в зависимости от вида продукта, от функционала, назначения и других критериев для каждой информационной системы вычисляемые метрики выводятся индивидуально, хотя существуют и общие, необходимые для оценки качества любого продукта.

Вывод

Существует несколько классификаций метрик. На мой взгляд, наиболее удачной является разделение их на вычисляемые и первичные метрики. В зависимости от проекта, менеджеры имеют возможность выбрать и рассчитывать те, которые являются наиболее подходящими для проекта. Метрики важны при определении качества, момента окончания тестирования или момента, когда проект может быть представлен пользователям, для выявления различных ошибок тестирования и проектирования и другое.

Литература:

1. Рахманов, Тимченко «Метрики в современном тестировании». Научно технический вестник СПбГИТМО (ТУ). Выпуск 10. 2003г.
2. http://www.protesting.ru/qa/metrics.html - электронная статья «Метрики по обеспечению качества»

SECURITATEA CIBERNETICĂ ŞI SECURITATEA NAȚIONALĂ. CAZUL REPUBLICII MOLDOVA

Alexanru BURUC, Dan NISTOR
Academia Militară a Forțelor Armate „Alexandru cel Bun"

*The daily activities taking place in any country are nowadays critically dependent on a stable and secure cyberspace, particularly those touching on the economic and national security dimensions. However, cyber crimes and cyber attacks have increased dramatically in the last few years, highlighting the need for governments around the world to take necessary measures in order to protect its citizens, their businesses, the national economy and the critical national operations. That is why this essay presents an overview of the concept of **cyber security**, the main cyber threats and their implications for national security strategies, revealing the level of importance given to this dimension of the national security, the current regulations and resources identified for this sector.*

Introducere

Lumea în care trăim devine din ce în ce mai interdependentă, iar acest lucru se datorează în mare parte evoluțiilor din domeniul tehnologiei informației şi comunicațiilor. Această interdependență crescândă generează numeroase avantaje, cât şi dezavantaje, având în vedere faptul că instituții publice şi companii private au devenit aproape în

totalitate dependente de sistemele informatice pentru a îndeplini activități importante. Aşadar, guvernele de peste tot în lume trebuie să se pregătească pentru a face față unor provocări noi care pot apărea în spațiul cibernetic, deoarece viața de zi cu zi a oricărui cetățean, economia națională, precum şi securitatea națională a oricărui stat depind în prezent de stabilitatea şi securitatea spațiul cibernetic.[1]

Securitatea cibernetică a fost în scurt timp implicată de la disciplina tehnică la un concept strategic. Globalizarea şi internetul a dat indivizilor, organizațiilor, şi națiunilor o nouă putere incredibilă, bazată pe dezvoltarea tehnologiilor de rețea. Pentru fiecare – studenți, soldați, şpioni, propagandişti, hackeri, şi teroriști – adunarea de informații, comunicațiile, diverse fonduri şi relațiile publice sau digitizat şi revoluționalizat.

Corelația securitate cibernetică – securitate națională

În consecință, conflictele militare şi politice la moment au o dimensiune cibernetică, dimensiunea şi impactul căreia sunt dificile de prezis, şi lupta în spațiul cibernetic poate fi mai importantă decât evenimentele ce au loc pe un camp de luptă de pe suprafața terestră. Ca şi teroriştii, hackerii au găsit success hackerii au găsit succesul în mass-media hype pură. Ca şi în cazul armelor de nimicire în masă, este dificil să te răzbuni asupra unui atac asimetric.

Națiunile sunt într-o dependentă crescîndă de sistemele complexe şi tehnologiile informaționale. În cele mai multe cazuri, Tehnologiile de comunicații şi informatică au acțiuni directe asupra securității naționale şi economice care de obicei şi sunt subiecte ale dezmembrării de la o mulțime de factori atît generați în cadrul națiunii cît şi din afara hotarelor acesteia. Liderii guvernelor şi din sectorul privat se confruntă cu riscuri şi vulnerabilități cibernetice. Această incertitudine se datorează complexității şi interconectivității tehnilogiei implicate pentru suportul sistemelor critice.

Asigurînd securitatea şi vitalitatea economică înseamnă că națiunea dată trebuie să administreze securitatea cibernetică în concordanță cu considerațiile economice, sociale şi politice. Inclusiv în cadrul strategiei de securitate cibernetică se stabilesc capacități de management al incidentului național de securitate a computerelor.

De obicei această capacitate poate lua forma unei sau a amai multor echipe de răspuns la incidentele cu caracter cibernetic (informațional).[2]

Dezvoltarea rapidă a tehnologiilor moderne de informații şi comunicații – condiție sine qua non a edificării societății informaționale – a avut un impact major asupra ansamblului social, marcând adevărate mutații în filozofia de funcționare a economicului, politicului şi culturalului, dar şi asupra vieții de zi cu zi a individului.

Practic, în prezent accesul la tehnologia informației şi comunicațiilor reprezintă una dintre premisele bunei funcționări a societății moderne. De fapt ținta atacurilor cibernetice va fi infrastructura sistemului cibernetic (fig. 2) care este vulnerabil la diverse acțiuni întreprinse.

---

[1] http://www.caleaeuropeana.ro/securitate-securitate-cibernetica-national-romania-cepe

[2] Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability

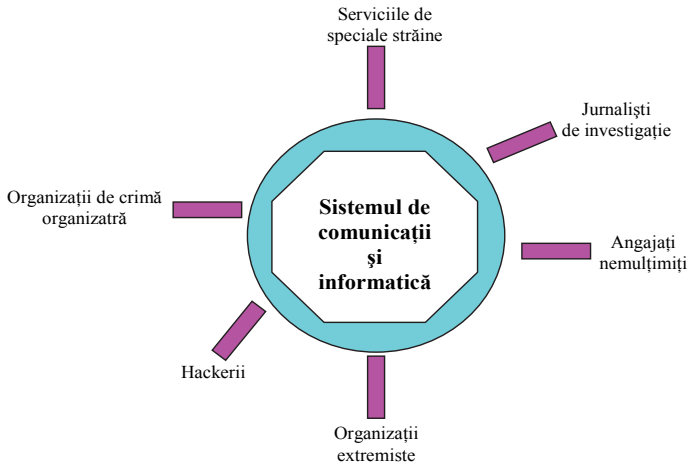

Figura nr. 1. **Surse de amenințări cibernetice aupra securității naționale**[1]

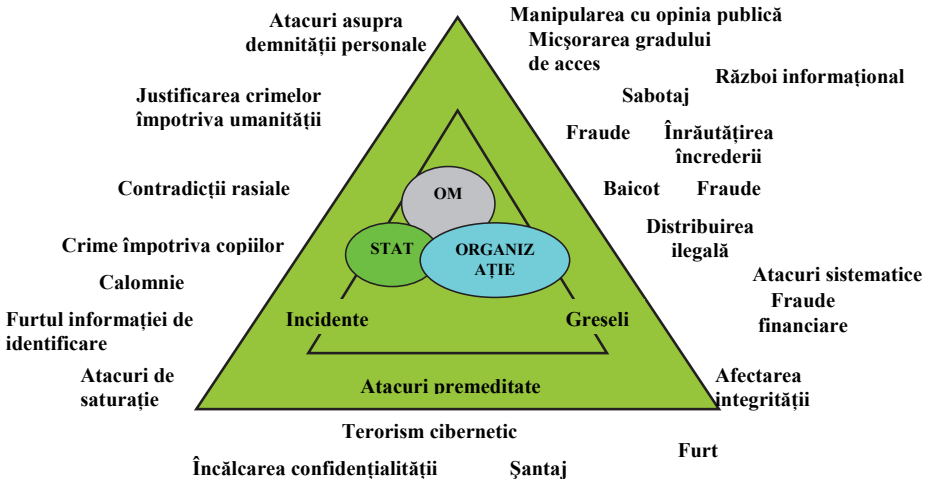

Figura nr. 2. **Ţinte şi surse ale riscurilor cibernetice**

Spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând atât deopotrivă, oportunități de dezvoltare a societății informaționale bazate pe cunoaştere şi riscuri la adresa funcționării acesteia (la nivel individual, statal şi chiar cu manifestare transfrontalieră).

Cu cât o societate este mai informatizată, cu atât este mai vulnerabilă, iar asigurarea securității spațiului cibernetic trebuie să constituie o preocupare majoră a tuturor actorilor implicați, mai ales la nivel instituțional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu.[2]

---

[1] ITU national cybersecurity strategy guide, Dr. Frederick Wamala (Ph.D.)

[2] Strategia de securitate cibernetică a României (proiect)

Astfel în cadrul Republicii Moldova s-a format centrul pentru securitatea cibernetică[1] care asigură securitatea informațională a autorităților administrației publice în spațiul cibernetic prin intermediul colectării şi analizei informației ce ține de atacuri cibernetice, precum şi întreprinde măsuri urgente şi eficiente de protecție a resurselor informaționale.[2]

Tabelul Nr. 1

Serviciile acordate de către centrul de răspuns la incidentele de securitate cibernetică (CERT (Computer Emergency Response Team)

Proactive	Reactive	Support
• Anunțuri privind evenimente din domeniu. • Anunțuri privind amenințări nou-identificate pe plan național şi internațional. • Cercetare şi informare privind noutățile tehnologice în domeniu. • Realizarea, la cerere, de auditări de securitate sau teste de penetrare. • Buletine de securitate.	• Alerte şi atenționări privind apariția unor activități premergătoare atacurilor • Gestiunea incidentelor la nivel național, în cooperare cu celelalte echipe • Diseminarea rezultatelor investigațiilor incidentelor de securitate cibernetică, cu respectarea prevederilor acordurilor de cooperare încheiate cu partenerii.	• Analize de risc aplicate la nivel local şi la nivel național privind infrastructurile cibernetice • Planificarea asigurării funcționării continue şi a recuperării în caz de dezastre; • Pregătirea echipelor de tip de răspuns la atacul cibernetic , a echipelor de audit în domeniul securității rețelelor, cu prioritate a celor incluse în infrastructura critică națională

Totodată, credem că este necesar de a se aborda un nivel mai ridicat de securitizare a infrastructurii digitale, deoarece la nivel mondial atacurile cibernetice sunt din ce în ce mai frecvente şi mai complexe. De aceea, Republica Moldova a avut în vedere anumite obiective care între timp au fost îndeplinite.

Infrastructuria critică şi sarcinile CERT (Computer Emergency Response Team)

Sarcinile de dirijare cu riscurile cibernetice, ce ar trebui să se soluționeze pentru asigurarea securității cibernetice a infrastructurii critice în conformitate cu А. А. Кононов, А. В. Сичкарук sunt:

1. constituirea unor structuri model şi tipizarea obiectelor infrastructurii critice;
2. stabilirea categoriilor după pericole pe baza modelelor de referință ale riscurilor. Evaluarea riscurilor de încălcare a securității cibernetice;
3. Construirea profilelor de bază de protecție (în acest context „profil de protecție" se are în vedere toate cerințele în ceea ce priveşte securitatea cibernetică) pe categorii funcție de baza normativ juridică existentă;
4. Controlul calității după cerințele:
   a. adecvat;
   b. închiderea „completă" a celor mai periculoase, amenințări şi a posibilelor riscuri cibernetice;

[1] Hotărîrea Guvernului Nr. 746 din 18.08.2010

[2] http://cert.gov.md/desprecsc.html

c. verificarea la consistenţă;
d. lipsa de redundanţă;
e. lipsa efectului distructiv.

5. concretizarea profilelor de protecţie pe obiecte şi pe grupuri de obiecte;
6. aducerea profilelor de protecţie actuale la nivelul cel mai superior;
7. concentrarea regulată periodică a datelor de îndeplinire a profilelor de protecţie;
8. prelucrarea informaţiei în timp real în ceea ce priveşte cerinţele de securitate;
9. aprecierea riscurilor de încredere a securităţii cibernetice. Identificarea vulnerabilităţilor, „locurilor înguste", combinaţiilor periculoase, formarea şi justificarea programelor naţionale şi regionale, măsuri şi acţiuni de măsuri a securităţii cibernetice;
10. Controlul de către o comisie de inspecţie a veridicităţii datelor prezentate de satisfacere a securităţii cibernetice.[1]

În cadrul proiectului Strategiei Naţionale de Securitate a Republicii Moldova se evidenţiază că pornind de la creşterea rolului tehnologiilor informaţionale în domeniul securităţii statului, instituţiile abilitate vor întreprinde acţiuni pentru asigurarea securităţii şi administrării eficiente a sistemelor informaţionale naţionale atât la nivel juridic, cât şi funcţional prin reducerea factorilor principali de risc, precum atacurile pe reţea (cybercrima) viruşii informatici, vulnerabilitatea softurilor, neglijenţa sau rea-voinţa utilizatorilor şi conectarea neautorizată a persoanelor terţe.[2]

În acest sens, o atenţie importantă trebuie acordată infrastructurii critice (IC), prin care se înţelege acele elemente materiale (echipamente, instalaţii, lucrări de artă, capacităţi de transport etc.), organizaţionale (reţele de transport, sisteme energetice, producţie şi distribuţie, produse petroliere şi gaze naturale etc.) şi informaţionale (fluxuri şi reţele de transmisii de date, procedure etc), vitale pentru buna desfăşurare a vieţii sociale şi susţinerea evoluţiilor economice, într-un climat stabil de securitate. Agresiunile pot fi realizate ca urmare a unor fenomene naturale (cutremure, inundaţii, alunecări de teren etc) sau ca urmare a unor acţiuni umane, accidentale sau intenţionate, cu o formă făţişă sau mascată, factorul risc fiind datorat stabilităţii şi lipsei de flexibilitate ale infrastructurilor critice. Vulnerabilităţile IC sunt împărţite în funcţie de proprietăţi, întâlnind astfel vulnerabilităţi acceptabile, critice sau inacceptabile, înţelegând totodată prin vulnerabilităţi la adresă IC incapacitatea protejării sistemului de securitate în dauna calamităţilor naturale, a accidentelor sau a penetrării de către surse exterioare.[3]

Observăm astfel faptul că statul tinde să nu rămână singurul subiect în ceea ce priveşte accesul la putere prin intermediul cyber-spaţiului, întrucât din ce în ce mai multe corporaţii sau ONG-uri pot acţiona liberi pe internet, cu atât mai mult cu cât dispun de o tehnologie proprie

---

[1] Задачи управления киберрисками и кибербезопасностью критических инфраструктур национального масштаба;

[2] Proiect Strategia Securităţii Naţionale a Republicii Moldova;

[3] http://geopolitics.ro/implicatii-ale-dezvoltarii-cybers-spatiului-asupra-securitatii-nationale-ii;

şi foarte avansată, profitând în acelaşi timp de presiunea civică la care statul este supus pentru a face publice cât mai multe date. Această creştere a actorilor poate duce către escaladarea unor conflicte ca urmare a unor posibile interese şi/sau viziuni diferite.

Concluzii

La moment există o tendință majoră ca țările lumii să se alieze pentru a asigura securitatea cibernetică.[1]

După noi tendința este una sănătoasă atît timp cît acest fel de amenințări sunt prezente în fiecare din națiuni. Comunul acord de a descuraja atacurile cibernetice reprezintă o forță de neînvins.

Ca urmare a acaparării serviciilor financiare, de informare, de socializare, de educație ş.a., internetul devine cea mai importantă componentă a infrastructurii critice (IC), fapt ce face din securizarea sectorului IT o prioritate de bază privind securitatea multor state ale lumii.

În ceea ce priveşte gestionarea amenințărilor cibernetice, acestea tind să treacă cât mai mult din zona militară către cea de intelligence.

Măsurile destinate operaționalizării Sistemului Național de Securitate Cibernetică trebuie armonizate cu eforturile pe dimensiunea protecției infrastructurilor critice, respec tiv cu evoluția procesului de dezvoltare a capabilităților de tip CERT (Computer Emergency Response Team).

În varianta optimă, Sistemul Național de Securitate Cibernetică (SNSC) trebuie să dispună de o structură flexibilă, adaptativă, are să înglobeze apabilități de identificare şi anticipare, resurse şi proceduri operaționale de prevenire, reacție şi ontracarare şi instrumente pentru documentare şi sancționare a autorilor atacurilor cibernetice.

Un recent raport al companiei de software antivirus Kaspersky Lab a arătat că Moldova este una din țările cele mai expuse riscurilor cibernetice, chiar în acest moment patru sisteme informatice ale Executivului, Ministerului Apărării şi ambasadelor moldoveneşti fiind atacate de un virus foarte puternic, numit „Octombrie Roşu", care țintește cu precădere țări din fostul bloc sovietic.[2]

Acesta fapt prezintă încă odată argumentul că Republica Moldova ar trebuie să se mobilizeze în ceea ce priveşte securitatea cibernetică pentru a nu păți ca şi în cazul Estoniei.

Este necesară implementarea, la nivel național, a unor standarde minimale procedurale şi de securitate pentru infrastructurile cibernetice, care să fundamenteze eficiența demersurilor de protejare față de atacuri cibernetice şi să limiteze riscurile producerii unor incidente cu potențial impact semnificativ.

Bibliografie

1. http://www.caleaeuropeana.ro/securitate-securitate-cibernetica-national-romania-cepe/, accesat la 25.02.2013;
2. ITU national cybersecurity strategy guide, Dr. Frederick Wamala (Ph.D.), CISSP p.16;

[1] http://www.fluxdestiri.info/2012/08/guvernele-lumii-se-aliaza-pentru-securitatea-cibernetica

[2] http://www.europalibera.org/content/article/24880817.html

3. Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, John Haller, Samuel A. Merrell, Matthew J. Butkovic, Bradford J. Willke. Iunie 2010, pag. 1-2;
4. Strategia de securitate cibernetică a României (proiect), pag. 3;
5. Hotărîrea Guvernului Nr. 746 din 18.08.2010 "Cu privire la aprobarea Planului Individual de Acțiuni al Parteneriatului Republica Moldova – NATO actualizat";
6. http://cert.gov.md/desprecsc.html, accesat la 25.02.2013;
7. А. А. Кононов, А. В. Сичкарук, К. В. Черныш, Задачи управления киберрисками и кибербезопасностью критических инфраструктур национального масштаба, p.100 – 102;
8. Proiect Strategia Securității Naționale a Republicii Moldova din 21.10.2011;
9. http://geopolitics.ro/implicatii-ale-dezvoltarii-cybers-spatiului-asupra-securitatii-nationale-ii, accesat la 05.03.2013;
10. http://www.fluxdestiri.info/2012/08/guvernele-lumii-se-aliaza-pentru-securitatea-cibernetica/, accesat la 05.03.2013;
11. http://www.europalibera.org/content/article/24880817.html, accesat la 25.02.2013.

CRM В ОБЛАКЕ

Е.Згардан, С.Жук
Молдавская Экономическая Академия

CRM системы для работы с клиентами на сегодняшний день пользуются популярностью за счет развития тенденций к полной автоматизации бизнес-процессов компаний. Современные системы управления взаимодействием с клиентами позволяют повысить уровень продаж, обеспечивают оптимизацию маркетинговых стратегий, улучшение уровня облуживания клиентов путем сохранения персональных данных и истории операций с ними, модернизации бизнес-процедур и анализа их результатов. Информация в современном мире представляет огромнейшую ценность и зачастую приносит огромные прибыли компании. Защита данных от несанкционированного доступа со стороны конкурентов или других посторонних лиц является необходимым условием для надежной и эффективной работы любой фирмы. Безопасность в CRM системах также играет далеко не последнюю роль.

CRM системе для работы необходима интеграция во внутренние системы компании: получение доступа к различной коммерческой информации о клиентах, базам данных, истории операций, совершенных клиентами. Подобные сведения являются «лакомым кусочком» для конкурентов. Поэтому, **безопасность в CRM системах** должна быть на высшем уровне, особенно в плане защиты информации.

На данный момент облачные технологии пользуются все большей популярностью в связи с желанием повысить оперативность решения бизнес-задач и более эффективно управлять бизнес-процессами.

Термин "облако" подразумевает под собой инфраструктуру серверов и устройств хранения данных, предоставляющих мгновенный круглосуточный доступ и объединенных в одно информационное пространство.

Ваши данные, хранящиеся в облаке, многократно дублируются, распределяются и хранятся на разных носителях, что минимизирует потери информации.

Рассмотрим ряд факторов, которые чаще всего являются причиной потери данных или несанкционированного доступа, и сравним классическое серверное хранение данных и облачное.

1. Кража данных

Практически всем сотрудникам компании известно, где находится корпоративный сервер, и какая информация на нем хранится. Теоретически, его можно выкрасть, информацию можно скопировать, к серверу можно получить доступ по локальной сети и удаленно.

В случае с облаком никто не знает, где конкретно хранятся ваши данные, к ним невозможно получить физический доступ.

2. Порча оборудования

Если вы храните данные на локальном сервере или на своем компьютере, вы не застрахованы от выхода оборудования из строя, особенно жестких дисков. Если у вас налажена система дублирования информации и сохранения резервных копий, это приведет к остановке работы на 1-2 дня, в иной ситуации вы потеряете данные безвозвратно.

В облаке все построено таким образом, что потеря данных из-за поломки оборудования невозможна. Все оборудование проходит регулярную проверку, а данные многократно дублируются на различных серверах.

3. Изъятие информации правоохранительными органами

В случае хранения данных в облаке никто не сможет прийти и опечатать ваш сервер. А функция "красной кнопки" позволит вам, в случае необходимости, моментально заблокировать доступ к облачным данным сразу для всех сотрудников компании.

4. Кибератака – взлом данных

Кибератаки и промышленный шпионаж – это страх, пришедший из голливудских сценариев, в которых все подростки мечтают получить доступ к базе данных ООО "Ромашка".

Как правило, каждая кибератака – это солидный бюджет. Чаще всего целью атак является дестабилизация работы публичных web-сайтов. Если атака совершается на аккаунт в приватной зоне, система моментально реагирует и блокирует его, сообщая о попытке взлома правообладателю и, если требуется, меняет реквизиты доступа, оставляя злоумышленников ни с чем.

На данный момент в Молдове, сравнительно мало компаний, сферой деятельности которой является CRM в облаке. Мы являемся представителями компании Cred-Info, компания основанная в 2009 году, которая осуществляет внедрение CRM системы.

В некоторых **CRM системах для работы** необходимы специальные электронные ключи, которые представляют собой небольшое устройство (и, между прочим, совсем недорогое), выполненное в виде брелока и содержащее уникальный код. Электронный ключ подключается к USB-порту компьютера. Он выдается всем клиентам компании, которые приобрели товар или заказали услугу и является идентификатором личности клиента для дальнейших заказов.

Следующий подход характерен для крупных и многофункциональных CRM-систем уровня Oracle Siebel. Он заключается во включении в систему всех процедур информационной безопасности, которые можно реализовать. Такой путь позволяет обеспечить максимальную безопасность данных в системе, особенно при реализации многопользовательской работы в приложении. Можно скрывать данные одного пользователя от других, гибко разделять права на чтение, запись, изменение информации, собирать статистику работы каждого пользователя, строить динамические профили поведения, что позволяет обнаружить подозрительную активность пользователей. Например, можно своевременно выявить попытку скачать базу данных клиентов или ознакомиться с контактами большого количества записей из БД, то есть - выявить случай, когда сотрудник обращается за рабочий день к сотне записей, хотя всегда работал только с десятью.

Но далеко не все необходимые процедуры защиты информации можно реализовать внутри CRM-системы. Например, реализация в приложении антивируса или межсетевого экрана смысла не имеет. Тем не менее, эти средства защиты необходимо использовать для того, чтобы защитить приложение от атак извне и заражений внутри сети. Конкретный набор дополнительных средств защиты необходимо определять в каждом конкретном случае, он будет зависеть от общей архитектуры сети, от архитектуры CRM-системы, от разделения прав пользователей и типов обрабатываемой в ней информации.

Сочетая вышеперечисленные методы, мы получим третий подход к защите информации в CRM - комбинированный. Он предусматривает компиляцию внешних средств защиты информации и процедур, встроенных в приложение и базы данных CRM. Этот подход в наибольшей степени распространен, поскольку является универсальным.

ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ И ЗАЩИТА ДАННЫХ

Галина Александровна Шелеляева
Гомельский государственный университет им. Ф. Скорины

Premises of application of security features of the electronic documents this in case of use, electronic document management. Problems simultaneous use of paper and electronic documents are revealed. Approaches to information security in automated data handling are considered.

В коммерческой деятельности сегодня электронным способом обрабатывается около 80% информации. По-прежнему основным носителем ее, сопровождающим все бизнес-процессы, остается документ.

Документ – это совокупность трех составляющих:

- носитель;
- форма;
- активизация определенной деятельности.

Именно некоторая деятельность и превращает данные в документ. Но документ перестает существовать, если в дальнейшем не подразумевает процедуры обработки. Форма документа тесно связана с характером дальнейшей деятельности, она порождает необходимость документов. При этом не существенен носитель информации, бумажный или электронный документ играют одинаковую роль в бизнес-процессах. В Республике Беларусь принят и успешно реализуется закон «Об электронном документе и электронной цифровой подписи», согласно которому «подлинный электронный документ приравнивается к документу на бумажном носителе, подписанному собственноручно, и имеет одинаковую с ним юридическую силу».

Электронные документы позволяют переместить центр тяжести компьютерной технологии с традиционных структурированных алфавитно-цифровых данных на потоки данных, дополненные большими объемами неструктурированного текста, изображений, звука, видео и графики. Такие документы смогут также включать гипертекстовые связи, переработанные OLE - объекты, текстовые объекты и реляционные данные. Электронный документ будет ограничен такими параметрами как его содержимое, структура данных, форматы и стандарты режима передачи и, самое важное, характер его использования.При изменении любого из этих параметров соответственно будет меняться документ. Он будет открытым, гибким, адаптируемым, многомерным.

За несколько лет концепция электронного документа получила свое развитие от обычного графического образа документа до идеи управления документами. Сегодня документ - это форма знакомого вида, обработка которой происходит с помощью последовательного применения тесно взаимосвязанных технологий в рамках так называемых Систем Управления Электронными Документами (СУД) или Electronic Document Management Systems (EDMS).

Электронный документооборот в коммерческой деятельности - это, в первую очередь, возможность (и необходимость) свободного обмена данными и документами с

партнерами по бизнесу. Следовательно, любой недобросовестный партнер может получить доступ и к внутренней конфиденциальной информации предприятия

Огромный управленческий эффект в самой ближайшей перспективе сулит переход от электронного документооборота в отдельных локальных офисных сетях к единой системе документооборота территориально распределенной системы организаций, которую можно с точки зрения документооборота рассматривать как один единый виртуальный офис.

Важно заметить, что в условиях активного перехода к электронному документообороту бумажный документооборот продолжает, и в обозримом будущем будет продолжать оставаться значимой составляющей документооборота. Следовательно, в этих условиях всегда будет возникать проблема одновременного управления бумажным и электронным документооборотом, сохранения целостности данных, защита их от несанкционированного использования и модификации.

В общем случае один и тот же документ может в течение всего своего жизненного цикла существовать в электронном и бумажном виде, причем иногда одновременно могут существовать бумажные и электронные экземпляры одного и того же документа. Таким образом, разделение контроля за бумажными и электронными документами вносит путаницу и, в конечном счете, приводит к потере контроля за документооборотом предприятия в целом. Главная задача здесь - естественным образом, в рамках единой системы, обеспечить контроль над всеми ипостасями документа, а также защиту информации независимо от ее носителя.

Именно электронный документ является основной угрозой информационной безопасности корпоративных систем и систем управления взаимоотношениями с клиентами (CRM-систем), т.к организация и технология защиты бумажных документов отработана веками, а аналогичные меры применительно к электронному документу часто неэффективны.

Обязательным для корпоративных и CRM-систем является требование обеспечение защиты данных. И это требование в большинстве систем выполняется за счет традиционных средств парольной защиты, разграничения доступа, межсетевой и антивирусной защиты.

Вместе с тем, анализ показывает явную недостаточность этих средств , так как они не учитывают наличие человеческого фактора - инсайдерной опасности, наличие таких каналов утечки информации как случайный несанкционированный доступ, перехват электронных документов, передаваемых по каналам связи и т.п.

Наиболее уязвимыми составляющими бизнес-среды являются каналы передачи данных, электронная почта, бизнес-приложения.

Нарушения нормального функционирования бизнес-процессов приводят к экономическим потерям при ведении электронной коммерции, наносится ущерб имиджу и репутации компании.

С целью снижения рисков больших финансовых потерь предприятия должны инвестировать средства в инструменты обеспечения безопасности и эти инструменты тем действеннее, чем реже они используются в бизнес-сообществе.

Помимо традиционных дешевых, хорошо известных как пользователям, так и злоумышленникам, появляется ряд средств, представляющих интерес именно для систем электронного документооборота.

К таким средствам относится, в первую очередь двух- и многофакторная аутентификация. Например, вход в систему возможен после ввода личного пароля и использования одноразового пароля, полученного по SMS на заранее зарегистрированный телефон. Громоздкость таких и аналогичных методов оправдывается их хорошей защищенностью в том числе и от пользователей, предпочитающих так называемые «слабые пароли».

Интересной технологией может быть голосовая аутентификация Значительное количество разработок в этой сфере имеется уже сегодня, проекты внедрения подобных механизмов уже описаны в литературе и использованы на практике. Это может быть аутентификация по ключевой фразе, аудио-пароли доступа к информации.

Помимо технологий, связанных с использованием биометрических аутентификаторов, имеются также программно-аппаратные решения, такие как автономные ключи для генерации одноразовых паролей, считыватели RFID-меток, криптокалькуляторы, программные и аппаратные жетоны (токены), электронные ключи различных типов - Touch Memory и ключ/смарт-карта, а также биометрические идентификационные карты.

SECURITATEA INFORMAȚIEI PERSONALE

Elena Paximadi, Ion Petroșișin
Academia Militară a Forțelor Armate „Alexandru cel Bun"

În prezent un rol important i se acordă securității informaționale. Codarea informației, în trecut şi în prezent, a dus la creşterea securității informaționale. Criptarea mapelor şi fişierelor a dat posibilitatea utilizatorilor de a-şi partaja informația de infractori informaționali.

Introducere

În societatea modernă, un rol tot mai important îl joacă calculatoarele şi toate mijloacele electronice de comunicare, de depozitare, şi de prelucrare.

Pentru a fi utilizate tehnologiile informaționale în diverse domenii, este necesar să se asigure siguranța şi fiabilitatea acestora. Sub noțiunea de securitate (în sensul cel mai larg), se subînțelege capacitatea sistemului de informații pentru a păstra integritatea şi eficiența de influențele accidentale sau deliberate externe. Utilizarea tehnologiilor informaționale a dus la dezvoltarea rapidă a diferitelor metode de protecție a informației: codarea şi criptografia.

La un singur calculator pot opera mai mulți utilizatori, fiecare avînd informația sa şi în acest caz securitatea informației este la cel mai mic nivel. Acest fapt a dus la necesitatea apariției parolei la calculator.

Codurile sunt o transformare care operează la nivelul cuvintelor sau frazelor.

Criptografia este arta şi ştiinţa ascunderii semnificaţiei unei comunicări împotriva unor intercepători neautorizaţi [2].

În sensul larg, codificarea poate fi, de asemenea, numită şi scanarea textului, imagini (informaţii este convertită de la o reprezentare vizuală în digitală), şi chiar introducerea textului de pe tastieră.

Conţinutul de bază

Necesitatea utilizării metodelor criptografice rezultă din condiţiile în care există stocarea şi schimbul de informaţii.

Cel mai simplu model de criptosistemă se poate de prezentat în aşa mod:

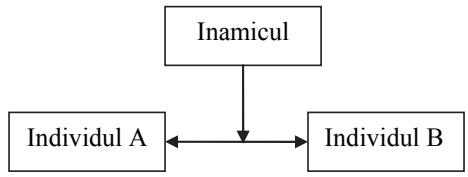

***Figura.1* Model de criptosistemă.**

De exemplu, în protecţia datelor stocate pe calculatorul dumneavoastră, puteţi presupune că utilizatorul A şi B – sunt 2 persoane de lucru. În acest caz, „canalul de informaţie" este un hard disk pe care sunt stocate datele.

Un model de codare este codul lui Cezar. Ce constă din literele alfabetului latin, fiecărei litere i se atribuie un număr din intervalul [0,25].

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

***Figura.2* Cheia pentru codul lui Cezar.**

Regulă de înlocuire poate fi descrisă după cum urmează: litera cu indicele *i* se înlocuieşte cu litera *i+3 (mod 26),* unde „mod 26" înseamnă restul împărţirii numărului *i+3* la 26.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

***Figura.3* Rezultatul aplicării codului lui Cezar.**

Este posibilă generalizarea codului lui Cezar, în care litera cu numărul *i* este înlocuită cu litera ce are numărul *i+k (mod 26)*.

În baza generalizării codului lui Cezar se crează o aplicaţie Excel cu 6 coloane în care se introduc formulele de calcul în conformitate cu expresiile din fig. 4.

	A	B	C	D	E	F
1	Caracterul	Indicele	K	I+k	Restul	Modificarea
2	a	0	5	=B2+$C$2	=MOD(D2,26)	=LOOKUP(E2,$B$2:$B$27,$A$2:$A$27)
3	b	1		=B3+$C$2	=MOD(D3,26)	=LOOKUP(E3,$B$2:$B$27,$A$2:$A$27)
4	c	2		=B4+$C$2	=MOD(D4,26)	=LOOKUP(E4,$B$2:$B$27,$A$2:$A$27)
5	d	3		=B5+$C$2	=MOD(D5,26)	=LOOKUP(E5,$B$2:$B$27,$A$2:$A$27)
6	e	4		=B6+$C$2	=MOD(D6,26)	=LOOKUP(E6,$B$2:$B$27,$A$2:$A$27)
7	f	5		=B7+$C$2	=MOD(D7,26)	=LOOKUP(E7,$B$2:$B$27,$A$2:$A$27)
8	g	6		=B8+$C$2	=MOD(D8,26)	=LOOKUP(E8,$B$2:$B$27,$A$2:$A$27)
9	h	7		=B9+$C$2	=MOD(D9,26)	=LOOKUP(E9,$B$2:$B$27,$A$2:$A$27)
10	i	8		=B10+$C$2	=MOD(D10,26)	=LOOKUP(E10,$B$2:$B$27,$A$2:$A$27)
11	j	9		=B11+$C$2	=MOD(D11,26)	=LOOKUP(E11,$B$2:$B$27,$A$2:$A$27)
12	k	10		=B12+$C$2	=MOD(D12,26)	=LOOKUP(E12,$B$2:$B$27,$A$2:$A$27)
13	l	11		=B13+$C$2	=MOD(D13,26)	=LOOKUP(E13,$B$2:$B$27,$A$2:$A$27)
14	m	12		=B14+$C$2	=MOD(D14,26)	=LOOKUP(E14,$B$2:$B$27,$A$2:$A$27)
15	n	13		=B15+$C$2	=MOD(D15,26)	=LOOKUP(E15,$B$2:$B$27,$A$2:$A$27)
16	o	14		=B16+$C$2	=MOD(D16,26)	=LOOKUP(E16,$B$2:$B$27,$A$2:$A$27)
17	p	15		=B17+$C$2	=MOD(D17,26)	=LOOKUP(E17,$B$2:$B$27,$A$2:$A$27)
18	q	16		=B18+$C$2	=MOD(D18,26)	=LOOKUP(E18,$B$2:$B$27,$A$2:$A$27)
19	r	17		=B19+$C$2	=MOD(D19,26)	=LOOKUP(E19,$B$2:$B$27,$A$2:$A$27)
20	s	18		=B20+$C$2	=MOD(D20,26)	=LOOKUP(E20,$B$2:$B$27,$A$2:$A$27)
21	t	19		=B21+$C$2	=MOD(D21,26)	=LOOKUP(E21,$B$2:$B$27,$A$2:$A$27)
22	u	20		=B22+$C$2	=MOD(D22,26)	=LOOKUP(E22,$B$2:$B$27,$A$2:$A$27)
23	v	21		=B23+$C$2	=MOD(D23,26)	=LOOKUP(E23,$B$2:$B$27,$A$2:$A$27)
24	w	22		=B24+$C$2	=MOD(D24,26)	=LOOKUP(E24,$B$2:$B$27,$A$2:$A$27)
25	x	23		=B25+$C$2	=MOD(D25,26)	=LOOKUP(E25,$B$2:$B$27,$A$2:$A$27)
26	y	24		=B26+$C$2	=MOD(D26,26)	=LOOKUP(E26,$B$2:$B$27,$A$2:$A$27)
27	z	25		=B27+$C$2	=MOD(D27,26)	=LOOKUP(E27,$B$2:$B$27,$A$2:$A$27)

	A	B	C	D	E	F
1	Caracterul	Indicele	K	I+k	Restul	Modificarea
2	a	0	5	5	5	f
3	b	1		6	6	g
4	c	2		7	7	h
5	d	3		8	8	i
6	e	4		9	9	j
7	f	5		10	10	k
8	g	6		11	11	l
9	h	7		12	12	m
10	i	8		13	13	n
11	j	9		14	14	o
12	k	10		15	15	p
13	l	11		16	16	q
14	m	12		17	17	r
15	n	13		18	18	s
16	o	14		19	19	t
17	p	15		20	20	u
18	q	16		21	21	v
19	r	17		22	22	w
20	s	18		23	23	x
21	t	19		24	24	y
22	u	20		25	25	z
23	v	21		26	0	a
24	w	22		27	1	b
25	x	23		28	2	c
26	y	24		29	3	d
27	z	25		30	4	e

***Figura.4* Formulele Excel de calcul.**

De asemenea se poate de criptat şi fişierele din mapă pentru a nu permite infractorului să efectuieze diferite operaţii cu informaţia din mapă. Acest lucru se pate de efectuat la calculatoarele ce au instalată sistema de operare Windows XP şi sitema de fişiere NTFS (*New Technology File System*) [1]. Edectuînd clic deapta pe fişierul necesar sau pe mapa necesară alegem opţiunea *Properties* apoi selectăm butonul Advanced şi în caseta apărută bifăm opţiunea *Encrypt contens to secure data*. Fişierele criptate se deosebesc de cele necriptate prin culoarea verede a denumirii fişierului.

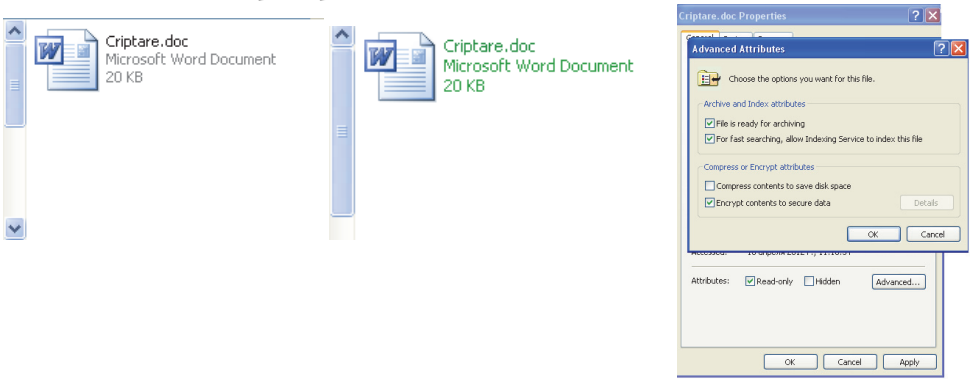

***Figura.5* Criptarea fişierelor.**

Un alt mod de protejare a informaţiei, este introducerea parolei fişierului, utilizînd opţiunea *General Options* din meniul *Tools*, introducînd parola şi confirmînd-o mai apoi.

În cadrul studierii temelor ce ţin de efectuarea calculelor pentru tragere, profesorii la crearea formulelor corecte, în aplicaţia Excel, protejează unele celule (pentru a nu da voie studenţilor să modifice valorile corecte), prin aplicarea opţiunii *Protection* din meniul *Tools*. Întîi de toate se deblochează toate celulele, selectînd toată foia de calcul, mai apoi din meniul

Format alege opțiunea *Cells/Protection* şi deblochează opțiunea *Locked*. Selectează informația necesară (acea informație ce trebuie blocată) şi din nou parcurge drumul din meniul *Format* alege opțiunea *Cells/Protection* şi blochează opțiunea *Locked* şi *Hidden*. De la opțiunea *Protection* alegem subopțiunea *Protect Sheet* şi pentru acest diapazon se va introduce parola pentru a nu da posibilitate altor utilizatori să introducă modificări.

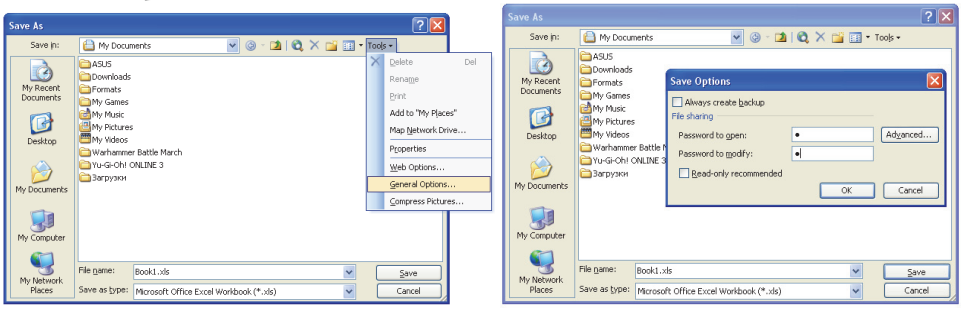

Figura.6* Utilizarea opțiunei *General Options.

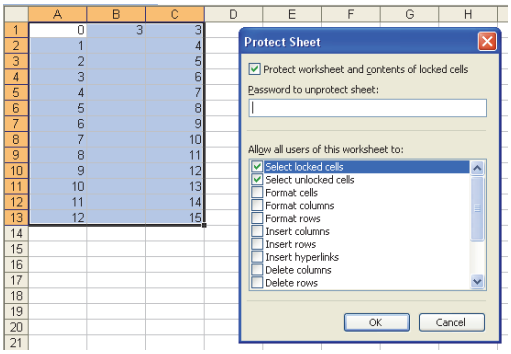

***Figura. 7* Introducerea parolei pentru celulele evidențiate.**

Concluzie

Informația - o resursă care trebuie protejată, de aceea într-un ritm mai rapid trebuie de a dezvolta echipamente de asigurare a siguranței informaționale mai complexe.

Dacă luăm în considerație informația ca o marfă, atunci securitatea informației poate duce la economii mari. Daunele care pot fi cauzate de protecția necorectă a informației duc la un cost enorm, decît protejarea corectă.

Expresiile matematice ce au fost introduse prin intermediul aplicației Excel pentru codul lui Cezar, dau posibilitate studenților să înțeleagă mai bine utilizarea calculatorului în aplicarea securității informaționale.

Referințe

1. http://ru.wikipedia.org/wiki/NTFS
2. OPREA, D. Potecția şi securitatea informațiilor. 2003. Iaşi, Editura „Polirom”

MĂSURILE SECURITĂȚII CIBERNETICE ÎN SOCIETATEA INFORMAȚIONALĂ

Claudia Hlopeanicov, Sergiu Munteanu
Academia Militară a Forțelor Armate „Alexandru cel Bun"

Potential of the information society is increasing due to technological development and multiple access paths. In this context, the proper course of business of security systems requires a functional IT system. IT security management systems are a key factor in the effective exercise of a company to protect data and conducting electronic transactions while the work of several institutions, businesses depend on their own computer system.

Among the main technical means implemented by companies whose business modern society, it could be mentioned that they can not perform optimally without a well-tuned system: antivirus, backup, training on the importance of implementing and tracking security measures.

Introducere

Societatea îmbrățișează din ce în ce mai mult tehnologia informației. Informația care până nu de mult avea la bază hârtia, îmbracă acum forma electronică. Informația pe suport de hârtie mai este încă rezervată documentelor oficiale, acolo unde este necesară o semnătură sau o stampilă. Adoptarea semnăturii electronice deschide însă perspectiva digitizării complete a documentelor, cel puțin din punct de vedere funcțional.

Acest nou mod de lucru, în care calculatorul a devenit un instrument indispensabil şi un mijloc de comunicare prin tehnologii precum poşta electronică sau Internetul, atrage după sine riscuri specifice. O gestiune corespunzătoare a documentelor în format electronic face necesară implementarea unor măsuri specifice. Măsurile ar trebui să asigure protecția informațiilor împotriva pierderii, distrugerii sau divulgării neautorizate. Cel mai sensibil aspect este acela de a asigura securitatea informației gestionată de sistemele informatice în noul context tehnologic.

Securitatea informației este un concept mai larg care se referă la asigurarea integrității, confidențialității şi disponibilității informației. Dinamica tehnologiei informației induce noi riscuri pentru care organizațiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea unităților de inscripționat CD-uri sau a memoriilor portabile de capacitate mare, induce riscuri de copiere neautorizată sau furt de date.

Lucrul în rețea şi conectarea la Internet induc şi ele riscuri suplimentare, de acces neautorizat la date sau chiar frauda.

Dezvoltarea tehnologică a fost acompaniată şi de soluții de securitate, producătorii de echipamente şi aplicații incluzând metode tehnice de protecție din ce în ce mai performante. Totuşi, în timp ce în domeniul tehnologiilor informaționale schimbarea este exponențială, componenta umană rămâne neschimbată. Asigurarea securității informațiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană.

Majoritatea incidentelor de securitate sunt generate de o gestiune şi organizare necorespunzătoare, şi mai puțin din cauza unei deficiențe a mecanismelor de securitate.

Este important ca organizațiile să conştientizeze riscurile asociate cu utilizarea tehnologiei şi gestionarea informațiilor şi să abordeze pozitiv acest subiect printr-o

conştientizare în rândul angajaților a importanței securității informațiilor, înțelegerea tipologiei amenințărilor, riscurilor şi vulnerabilităților specifice mediilor informatizate şi aplicarea practicilor de control.

Riscuri şi amenințări

Amenințările specifice spațiului cibernetic se caracterizează prin asimetrie şi dinamică accentuată şi caracter global, ceea ce le face dificil de identificat şi de contracarat prin măsuri proporționale cu impactul materializării riscurilor. În prezent, confruntările cu amenințările provenite din spațiul cibernetic la adresa infrastructurilor critice, având în vedere interdependența din ce în ce mai ridicată între infrastructurile cibernetice şi infrastructuri, precum cele din sectoarele financiar-bancar, transport, energie şi apărare națională. Globalitatea spațiului cibernetic este de natură să amplifice riscurile la adresa acestora afectând în aceeaşi măsură atât sectorul privat, cât şi cel public.

Posibilitatea ca sistemele informaționale computirizate ale unei instituții să fie insuficient protejate împotriva anumiți atacuri sau pierderi este numit de către Straub(1998) *risc de sistem.* Pe de altă parte, putem spune că riscul este considerat ceva subiectiv care se referă la un viitor care există doar în imaginație. Conform lui Turban (1996) *riscul* este defenit ca posibilitatea unei amenințări materializate.[7] Riscul este în contextul sistemelor informaționale computerizate, suma amenințărilor (evenimete care pot cauza daune), vulnerabilităților şi valoarea informațiilor expuse:

RISC = AMENINȚĂRI+VULNERABILITĂȚI+VALOAREA INFORMAȚIILOR

Informațiile stocate electronic au anumită valoare. Un incident care va afecta negativ informațiile stocate electronic va afecta şi individual instituția care depinde sau foloseşte informațiile respective. Reprezentarea schematică sugestivă a conceptelor privind securitatea sistemelor informaționale şi relațiile acestea este propusă în standardul CCITSE[1].

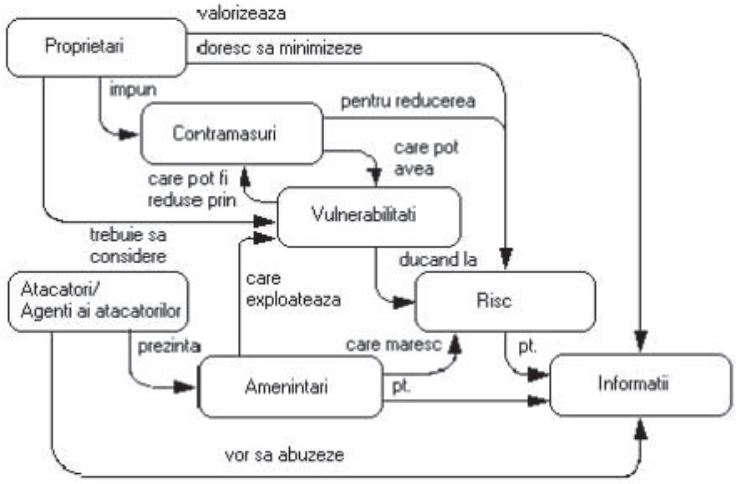

Figura 1. **Conceptele privind securitatea sistemului informațional.**

[1] *Common Criteria for Information Technology Security Evaluation.*

Un model al efectivității securității unui sistem informațional este propusă şi de către Kankanhali(2003). Conform acestui model angajamentul managerilor de vîrf, dimensiunea instituției, eforturile de disuasiune şi prevenirea acestora sunt consideraţi ca factorii cei mai importanți.[7]

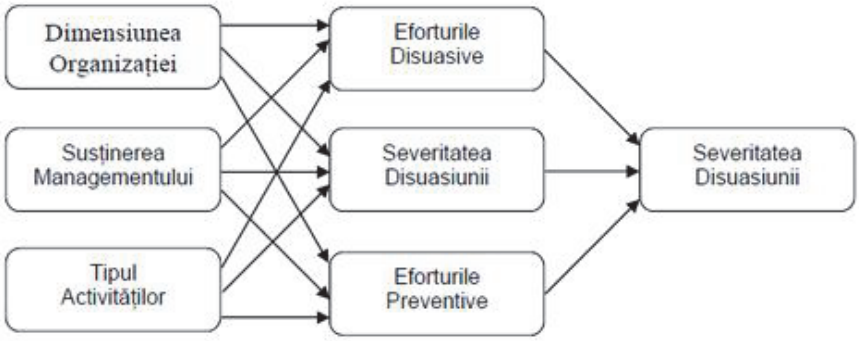

Figura 2. **Model al efectivității securității unui sistem informațional.**

Pentru evaluarea potențialului atacurilor posibile este necesar să fie înțelese expertiza, motivația şi intenția potențialilor atacatorilor. Un atacator care selectează sistemul în funcție de insecurității pe care acesta le prezintă este diferit de un atacator care selectează pentru atac un sistem anume, pentru a comite anumite fapte.

Amenințările la adresa spațiului cibernetic se pot clasifica în mai multe moduri, dar cele mai frecvent utilizate sunt cele bazate pe factorii motivaționali şi impactul asupra societății. În acest sens, putem avea în vedere criminalitatea cibernetică, terorismul cibernetic şi războiul cibernetic, având ca sursă atât actori statali, cât şi non-statali.

Principale persoane care generează amenințări în spațiul cibernetic sunt:

- persoane sau grupări de criminalitate organizată care exploatează vulnerabilitățile spațiului cibernetic în scopul obținerii de avantaje patrimoniale sau nepatrimoniale;
- terorişti sau extremişti care utilizează spațiul cibernetic pentru desfăşurarea şi coordonarea unor atacuri teroriste, activități de comunicare, propagandă, recrutare şi instruire, colectare de fonduri etc., în scopuri teroriste;
- state sau actori non-statali care inițiază sau derulează operațiuni în spațiul cibernetic în scopul culegerii de informații din domeniile guvernamental, militar, economic sau al materializării altor amenințări la adresa securității naționale.

Măsuri de securitate

Multe atacuri privind securitatea cibernetică provin din interiorul ei. La atacurile interne se referă furt de parole (care pot fi utlizate sau vândute), spionaj industrial, angajați nemulțumiți care tind de a cauza daune angajatorului, sau simpla utilizare necorespunzătoare. Majoritatea acestor încălcări pot fi soluționate cu ajutorul ofițerului de securitate a companiei, care monitorizează activitatea utilizatorilor rețelei.

Atacurile directe asupra rețelelor pot lua diferite forme, şi multe dintre acestea sunt posibile datorită modului în care operează suita de protocoale TCP/IP[1]. Fiecare protocol din suita TCP/IP comunică pe un anumit canal, numit *număr de port,* well-known port number. De exemplu, protocolul de transfer al hiper-textului, HTTP[2], operează pe portul 80, iar protocolul de transfer de fişiere, FTP[3], operează pe portul 21. Există, de fapt, peste 1.000 de numere de port binecunoscute şi fiecare din aceste porturi reprezintă o potențială cale pentru un atac la adresa rețelei dumneavoastră. Firewall-urile furnizează o strategie pentru blocarea acestor porturi.[1]

O altă modalitate prin care sunt concepute atacurile directe implică informații importante, cum ar fi numele de logare şi parolele, care sunt aflate de un cracker care foloseşte programe de spionaj, cum ar fi sniffer-ele de protocol. Un cracker poate sta în afara rețelei dumneavoastră, pe Internet, şi intercepta transmisii de date care pot oferi suficiente informații pentru un atac direct asupra rețelei interne.

Asupra unei rețele IP pot fi realizate o serie de tipuri diferite de atacuri:

- *spionajul electronic* (eavesdropping). Cunoscut şi sub numele de *adulmecați* sniffing sau *spionaj* (snooping), spionajul electronic reprezintă capacitatea de a monitoriza traficul din rețea, deoarece acesta este în format nesecurizat. în esență, cel care spionează foloseşte un fel de program de monitorizare a rețelei.
- *atacurile parolelor* (password attacks). Aceste atacuri sunt, de regulă, un rezultat al spionajului electronic. Din momentul în care cel care a spionat a reuşit să găsească un cont valid (deoarece aceste informații nu sunt întotdeauna protejate în rețeaua internă), atacatorul poate obține accesul la rețea şi poate afla informații cum ar fi utilizatori valizi, nume de calculator şi localizarea unor resurse. Acest lucru poate duce la modificarea, ştergerea sau re-rutarea datelor din rețea;
- *înşelarea adresei IP* (IP spoofing). Un atacator este capabil să îşi asume o adresă IP legală şi să obțină acces la rețea;
- a*tacurile de tip man-in-the-middle* (om *la mijloc)*. Atacatorul este capabil să monitorizeze, captureze şi să controleze date între dispozitivele emitent şi receptor;
- a*tacurile de tip denial-of-service (refuzarea funcționării).* Atacatorul capătă acces la rețea şi apoi trimite date nevalide serviciilor şi aplicațiilor din rețea, ceea ce determină ca aceste servicii de rețea să funcționeze inconsecvent sau să fie închise. Acest tip de atac se poate materializa, de asemenea, sub forma unei inundări cu date direcționate asupra unui anumit serviciu sau calculator, ceea ce determină o supraîncărcare şi o oprire a serviciului sau calculatorului. Acest tip de atac a fost folosit în mod repetat pentru a doborî site-uri web de pe Internet.

---

[1] Transmission Control Protocol/Internet Protocol.

[2] Hypertext Transfer Protocol.

[3] File Transfer Protocol.

Administratorii de rețea folosesc tot felul de strategii pentru a preveni aceste tipuri de atacuri. Ruterele securizate reprezintă o modalitate de protejare a rețelei interne, la fel ca firewall-urile.

O altă metodă implică implementarea securității protocolului internet (Internet Protocol Security, IPSec), care este o suită de servicii de protecție şi protocoale de securitate bazate pe criptografie ce pot fi folosite pentru securizarea rețelelor interne, rețelelor care folosesc soluții de conectivitate WAN[1] şi rețelelor care profită de avantajul soluțiilor de acces la distanță.

Securitatea cibernetică unei rețele, indiferent care este mărimea acesteia, va necesita, probabil, mai multe strategii. Aceasta înseamnă că trebuie să creați un plan de securitate pentru rețeaua dumneavoastră. După ce aveți un plan, îl puteți implementa, folosind instrumentele de securitate hardware sau software corespunzătoare. Securitatea rețelelor este, cu siguranță, un subiect foarte la modă şi extrem de important pentru activitatea oricărui administrator de rețea. Securizarea unei rețele nu este însă o sarcină uşoară. Chiar şi marile companii, cum ar fi Yahoo! şi Microsoft, au fost ocazional lovite de astfel de atacuri.[1]

Concluzii

În concluzie, pentru a trata toate aspectele referitoare la securitatea unei rețele trebuie abordate două aspecte protecția la atacurile din interior şi la atacurile din exterior. De asemenea, protecția unei rețele de calculatoare nu se realizează doar la nivel logic, al aplicațiilor, ci şi la nivel fizic, al securității echipamentelor. Un echipament, aflat într-o locație publică, în care au acces multiple catogorii de persoane, sunt mult mai suspectibile la atacuri la nivel fizic decât cele situate în locații cu control strict al accesului.

O bună practică ne învață că politicile de securitate trebuie aplicate la toate nivelurile ierarhice ale unei rețele de calculatore, nu doar la nivelul access, unde se regăsesc utilizatorii finali. De asemenea, utilizarea programelor de protecție antivirus şi firewall pentru protejarea calculatoarelor şi serverelor este necesară la orice nivel al rețelei de date.

Pe măsură ce instituțiile devin din ce în mai dependente de bună funcționare a sistemelor informaționale, problema securității devine din ce în mai iportantă.

Bibliografie

1. Joe Habraken – Rețele de calculatoare pentru începători, Editura BIC ALL 2002.
2. McClure Stuart, - Securitatea rețelelor, Editura Teora, 2002.
3. Emilian Stancu, Terorism şi Internet, în „Pentru Patrie", nr. 12/2000, p. 26.
4. Dumitru Oprea – Sisteme informaționale pentru afaceri, Editura Polirom, 2002.
5. Răzvan Daniel Zatu – Rețele de calculatoare în era Internet, Editura Economică, 2002.
6. Dorin Zaharie – Proiectarea obiectuală a sistemelor informatice, Editura DualTech, 2003.
7. http://www.securitatea-informatica.ro.
8. http://ro.wikipedia.org/wiki/Securitatatea_(calculatoare).
9. www.scibd.com.
10. www.bitdefender.ro

[1] Wide Area Network.

INFRACTIUNILE INFORMATIONALE SI SPIONAJUL INFORMATIONAL

Roman Gojan, Iulian Stan
Academia Militară a Forțelor Armate "Alexandru cel Bun"

Furtul informatiei

Adesea, Internetul este perceput că o vastă bibliotecă digitală. Numai World Wide Web –ul (www) oferă aproximativ un miliard de pagini cu date şi informaţii, iar cea mai mare parte a acestora sunt gratis. În acest fel, activiştii au la îndemînă un instrument util cu ajutorul căruia pot să localizeze documente cu caracter legislativ, declaraţii politice oficiale, analize şi comentarii pe diverse teme de interes, alte chestiuni cu relevanţă pentru misiunea lor. De asemenea, ei pot obține nume şi detalii de contact referitoare la factori de decizie din cadrul agenţiilor guvernamentale ori guvernelor pe care speră să le poată influența.

Activiştii pot identifica grupuri similare ori persoane cu aceleaşi preocupări şi adună informaţii referitoare la potenţiali suporteri ori colaboratori.

Există numeroase programe şi aplicaţii care ajută la colectarea de date şi informaţii, cum ar fi: motoarele de căutare, listele de distribuție e-mail, camerele de conversaţii online (chat) şi forumurile de discuţii. De asemenea, multe pagini de Web oferă chiar ele facilităţi de căutare în propriile baze de date.

În general, administraţiile cu iz totalitar recunosc beneficiile aduse de serviciile Internet în creşterea economică, însă percep libertatea cuvîntului în cadrul Reţelei ca pe o nouă ameninţare la adresa stabilităţii (securităţii) lor.

Falsificarea informatiei

Fapta de a introduce, modifica sau şterge, fără drept, date informatice ori de a restricționa, fără drept, accesul la aceste date, dacă fapta are ca rezultat obținerea de date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice.

- ***a) Obiect juridic special*** constă în relaţiile sociale referitoare la încrederea publică în siguranța şi fiabilitatea sistemelor informatice, la valabilitatea şi autenticitatea datelor informatice, a întregului proces modern de prelucrare, stocare şi tranzacționare automată a datelor de interes oficial sau privat.
- ***b) Obiect material*** este reprezentat de datele informatice asupra cărora îşi îndreaptă atenția făptuitorul. Datele informatice care apar pe monitor sau la imprimantă sub formă de caractere alfanumerice cu înțeles pentru utilizatori sunt reprezentate la „nivel fizic" (al maşinii de calcul) sau pe suportul de stocare de a înşiruire logică de stări „0" şi „1" corespunzătoare unor variaţii de tensiune.

Acționînd asupra acestor date (sau introducînd unele noi) este echivalent cu a acționa (prin intermediul procesorului) asupra înşiruirii de „0" şi „1" şi , implicit, asupra mediilor de stocare (Hard-Disk, floppy-disk, memorie flash, CD, DVD etc.).

- ***a) Subiectul activ*** (autorul) poate fi orice persoană responsabilă penal.

Manipulările frauduloase de acest gen sunt, în general, realizate de către inițiați în ştiința alculatoarelor ori de persoane care, prin natura serviciului, au acces la date şi sisteme informatice.

Participația este posibilă în toate formele sale: coautorat, instigare ori complicitate.

*b) **Subiectul pasiv***. În cazul acestei infracțiuni, subiectul pasiv va fi persoana fizică sau juridică prejudiciată în propriile interese şi față de care se produc consecințe juridice (de ordin patrimonial, moral ori social) în urma contrafacerii datelor informatice.

Subiect pasiv adiacent (secundar) va fi proprietarul, deținătorul de drept ori utilizatorul autorizat al sistemului informatic. Cu titlu de exemplu, falsificarea datelor informatice s-ar putea realiza sub următoarele forme:

- inserarea, modificarea sau ştergerea de date în câmpurile unei baze de date existente la nivelul unui centru de evidență informatizată a persoanei, unei bănci sau societăți de asigurări etc.
- prin acțiunea directă a făptuitorului asupra tastaturii ori prin copierea datelor de pe un suport de stocare extern;
- alterarea documentelor stocate în format electronic, prin modificarea sau ştergerea directă a cuvintelor etc.

Într-o abordare tehnică mai complexă, falsul informatic va lua una din următoarele forme:

- Simularea poştei electronice;
- Simularea hyperconexiunilor;
- Simularea Web-ului

Simularea EMAIL-ului

Poşta electronică pe Internet este deosebit de simplu de simulat, motiv pentru care, în general, mesajele email nu pot fi credibile în lipsa unor facilități cum sunt semnăturile digitale. Ca exemplu, să considerăm schimbul de mesaje între două hosturi Internet. Schimbul se produce folosind un protocol simplu care foloseşte comenzi cu caractere ASCII. Un intrus poate introduce cu uşurință aceste comenzi manual, conectîndu-se prin Telnet direct la portul Simple Mail Transfer Protocol (SMTP). Hostul receptor are încredere în identitatea hostului emițător, astfel că hackerul poate simula cu uşurință originea mesajului prin introducerea unei adrese a emițătorului diferită de veritabila adresă a hackerului. În consecință, orice utilizator fără privilegii poate falsifica sau simula mesaje de email.

Simularea Hiperconexiunilor

În secțiunile anterioare s-a discutat despre unele atacuri hacker împotriva comunicațiilor TCP şi Telnet. Această secțiune, care discută simularea hiperconexiunilor, precum şi următoarea, care detaliază simularea în Web, explică unul dintre atacurile folosite de hackeri împotriva calculatoarelor care comunică prin protocolul de transport pentru hypertext (HTTP). Hackerii pot construi atacuri asupra protocolului de autentificare a serverului Secured Socket Layer folosit la crearea de browsere şi servere de Web sigure, cum sunt cele ale firmelor Microsoft şi Netscape.

Aşa cum numele DNS sunt subiecte ale simulării DNS (adică un server DNS oferă o adresă de Internet falsă), la fel şi URL-urile sunt expuse simulării hiperconexiunilor, caz în care, o pagină indică un nume DNS fals al unui URL. Ambele forme de simulare duc la un alt site Internet decît cel dorit. Totuşi, simularea hiperconexiunilor este mai simplă din punct de vedere tehnic decît simularea DNS.

Dacă utilizatorul examinează meniurile browserului şi vizualizează sursa documentului sau informaţia despre document, va observa că identitatea autentificată a serverului nu este cea presupusă.

Simularea WEB-ului

Simularea Web-ului este un alt tip de atac hacker. La simularea Web-ului, hackerul creează o copie convingătoare, dar falsă a întregului Web. Web-ul fals este o reproducere exactă a celui veritabil, adică are exact acelaşi pagini şi conexiuni ca şi adevăratul Web. Cu toate acestea, hackerul controlează integral falsul Web, astfel încît întregul trafic de reţea între browserul victimei şi Web trece prin sistemul hacker.

La executarea unei simulări a Web-ului hackerul poate observa sau modifica toate datele trimise de la victimă la serverele Web. De asemenea, hackerul are controlul întregului trafic returnat de serverele Web către victimă. În consecinţă, hackerul dispune de multiple posibilităţi de exploatare. După cum am mai arătat, cele mai cunoscute metode de pătrundere într-o reţea sunt interceptarea şi simularea. *Interceptarea (sniffingul)* este o activitate de tip supraveghere, deoarece hackerul urmăreşte traficul de reţea în mod pasiv. *Simularea* este o activitate de intercepţie, deoarece hackerul convinge un host că este un alt host credibil, care poate primi informaţii.

Cheia atacului prin simularea Web-ului este ca serverul hackerului să se afle între victimă şi restul Web-ului. După cum am mai arătat, acest aranjament este cunoscut sub numele de atac prin intermediar.

Sabotajul informatic

Intrarea , alterarea , stergerea sau suprimarea de date sau de programe pentru calculator sau ingerinta în sisteme informatice în intentia de a impiedica fuctionarea unui sistem informatic sau a unui sistem de telecomunicatii.

Obiectul juridic: se refera la relatiile sociale în legatura cu dreptul de proprietate al proprietarului si utilizatorului de sistem informatic sau sistem de telecomunicatii pentru ca acesta sa functioneze corect, la parametrii proiectati, fara perturbatii produse prin actiune nefasta a unor infractori.

Subiectul activ: Poate fi orice persoana responsabila penal cu precizarea ca autorii , de regula, au cunostinte teoretice si practice în domeniul lucrului cu sisteme informatice.

Latura obiectiva: Elemental material consta intr-o actiune de interventie intr-un sistem informatic si anume de intrare, alterare, stergere sau suprimare de date sau de programe pe calculator sau ingerinta în sisteme informatice în intentia de a impiedica functionarea unui sistem informatic sau a unui sistem de telecomunicatii.

Latura subiectiva: Infractiunea se savarseste numai cu intentie , directa sau indirecta.

Spionajul informatic

Reprezinta activitatea de obtinere de date si informatii care constituie secrete de fabricatie (de creatie) în scopul folosirii lor pentru obtinerea unui avantaj material ilicit.

Altfel definit , prin spionaj informatic se intelege - obtinerea prin mijloace nelegitime sau divulgarea , transferul sau folosirea fara drept sau fara nici o alta justificare legala a unui secret commercial sau industrial în intentia de a cauza un prejudiciu economic persoanei care detine dreptul asupra secretului sau de a obtine pentru sine sau pentru altul avantaje economice ilicite.

Obiectul juridic: Il constituie apararea secretelor comerciale, violarile de secrete comerciale etc.

Obiectul material:Il reprezinta suporturile de informatii (discuri magnetice, flexibile, banda magnetica etc.)in care se afla inregistrate secretele comerciale si industriale.

Subiectul activ: Orice persoana responsabila penal, desi persoanele care faptuiesc trebuie sa cunoasca modul de lucru cu astfel de echipamente.

Latura obiectiva: Element al material consta intr-o actiune de obtinere de secrete comerciale si industriale cu urmarea imediata folosirea acestora pentru obtinerea unor avantaje materiale ilicite. Intre actiunea ca atare si urmarea imediata trebuie sa existe o legatura de cauzalitate.

Latura_subiectiva: infractiunea trebuie sa comisa cu intentie, directa sau indirecta, iar faptuitorul sa urmareasca realizarea unui prejudiciu economic sau de a obtine un avantaj economic illicit.

Accesul neautorizat

Constă în accesul fara drept la un sIstem sau o retea informatica prin violarea de securitate.

Obiectul juridic: Il reprezinta relatiile sociale referitoare la inviolabilitatea securitatii sistemului informatic .

Obiectul material: Consta în entitatile materiale care reprezinta sistemele sau retelele informatice

Subiectul activ: Poate fi orice persoana responsabila penal . Autorii unor astfel de infractiuni au denumirea de hakeri, care sunt experti în calculatoare si în retelele de calculatoare , familiarizati cu spargerea masurilor de securitate luate pentru protectia calculatoarelor sau a retelelor de calculatoare.

Latura obiectiva: Elemental material al infractiunii se realizeaza prin actiunea de intrare neautorizata (fara drept) intr-un sistem sau o retea informatica. Urmarea imediata consta în utilizarea acestor date cu scopul de a obtine un venit ilicit. Intre actiune si urmare trebuie sa fie o legatura de cauzalitate.

Latura subiectiva: Infractiunea de acces neautorizat se comite cu intentie directa sau indirecta . Forma de vinovatie din culpa exclude raspunderea penala pentru infractiunea de acces neautorizat.

Interceptarea neautorizata de informatii

Fapta care constă în interceptarea fara drept si cu mijloace tehnice de comunicatii cu destinatie , cu provenienta si în interiorul unui system sau al unei retele informatice .

Obiectul juridic: Il reprezinta relatiile sociale cu privire la dreptul fiecarei persoane la o viata privata neperturbata.

Obiectul material: Consta în suporturile materiale prin care se realizeaza comunicatiile.

Subiectul activ: Poate fi orice persoana responsabila penal.

Latura obiectiva: Constă într-o actiune de interceptare prin mijloace tehnice în vederea ascultarii continutului comunicatiilor , obtinerea continutului datelor , fie direct, accesand sistemul informatic si folosindu-l fie indirect, recurgand la procedee electronice de ascultare clandestina. Urmarea imediata consta în obtinerea informatiilor private si folosirea lor în scop propriu ilicit. Intreactiune si urmarea imediata trebuie sa fie o legatura de cauzalitate .

Latura subiectiva: Aceasta infractiune se comite numai cu intentie directa sau indirecta. Culpa nu este sanctionata.

Alterarea datelor sau programelor

Constă în actiunea de alterare în orice modalitate a datelor sau programelor pentru calculator.

Obiectul juridic : se protejeaza dreptul de autor cu privire la integritatea datelor sau programelor pentru calculator.

Obiectul material : il reprezinta suportul material (disc mobil, disc compact, disc dur, etc.) în care se afla inregistrate datele sau programele.

Subiectul activ : orice persoana care indeplineste conditiile cerute de legepentru a raspunde penal.

Latura obiectiva : elemental material este dat de alterare neautorizata de date sau programe pentru calculator cu urmarea imediata producerea de pagube proprietarului. Intre actiunea ca atare si urmarea imediata trebuie sa fie olegatura de cauzalitate.

Latura subiectiva : forma de vinovatie este cu intentie , directa sau indirecta. Culpa nu este sanctionata.

Tipuri de infractori

In evidentierea aspectelor de ordin criminologic, expertii în analiza infractionalitatii informatice propun luarea în considerare a patru categorii principale în care pot fi impartiti acesti indivizi, astfel:

- Hackeri
- Phreaks si Crackeri
- Traficantii de Informatii si Mercenarii
- Teroristii informatici si Cyber-extremistii

Dupa cum se poate observa, în lista nu este prezenta categoria de indivizi care folosesc mediul virtual sau tehnologia Hi-Tech pentru a obtine castiguri financiare ilicite.

Mass-media (si nu numai) obisnuiesc sa trateze aceasta categorie de infractori drept "cyber-criminali", "hackeri", "infractori digitali" etc. din considerente care tin mai mult de gradul de atractivitate si comercial al articolelor sau stirilor de presa, fara a realiza ca, în realizarea actului infractional, acesti indivizi nu sunt cu nimic mai presus de "colegii

lor de breasla" care comit furturi, talharii, delapidari, inselaciuni etc. Potrivit *Online Hacker Lexicon*, un **Hacker** il gasim în oricare din urmatoarele ipostaze:

- persoana pasionata de explorarea detaliilor sistemelor informatice
- persoana ca programeaza cu entuziasm si are performante notabile
- persoana demna de a fi apreciata (*the hack value*)
- persoana careia ii place provocarea / emulatia intelectuala de depasire creativa sau de evitare a limitarilor
- intrus care incearca sa descopere informatii precise cu multa curiozitate si insistenta

În functie de *modul în care abordeaza sistemele informatice*, putem identifica:

White Hat Hackers - hackeri care acceseaza neautorizat sisteme informatice, prin inlaturarea masurilor de securitate, insa nu cu motivatie infractionala declarata, ci cu intentia de a dovedi de ceea ce sunt în stare. Din punct de vedere criminologic, ei sunt constienti de rezultatele faptelor pe care le savarsesc, nu le urmaresc, sperand în mod "inexplicabil" ca acestea nu se vor produce.

Grey Hat Hackers - hackeri care actioneaza asupra sistemelor informatice în baza unei rezolutii mentale aflate la granita dintre etica si intentia criminala.

Ethical Hackers - sunt acei hackeri care isi dovedesc, organizat, abilitatile tehnice de penetrare a sistemelor informatice, insa doar în baza solicitarilor responsabililor cu securitatea IT din cadrul organizatiilor sau institutiilor interesate de descoperirea propriilor vulnerabilitati virtuale. Ei sunt, insa, obligati (prin contract) sa pastreze secretul asupra operatiunilor efectuate ori breselor de securitate identificate.

Script Kiddies - persoane, nu neaparat specialisti IT sau cunoscatori ai domeniului, care acceseaza neautorizat sisteme informatice folosind în acest sens anumite utilitare de sistem, programe sau aplicatii dedicate, cel mai adesea scrise (concepute) de profesionisti. Este cazul celor care incearca sa "sparga" parolele de acces în sistem sau asociate conturilor de posta electronica ori plaseaza în sistemele informatice vizate programe de interecetare a codurilor generate prin apasarea tastaturii (keyloggere).

Crackerii reprezinta acea categorie de "infractori virtuali" care isi propun si adesea reusesc sa acceseze sistemele informatice vizate, în principal prin violarea masurilor de securitate.

Odata intrați în sisteme, crackerii actioneaza, de cele mai multe ori, în sens distructiv, provocand pagube sau perturband grav functionarea tehnicii de calcul prin: introducerea de virusi, viermi sau cai troieni, prin furt ori distrugere de date informatice, restrictionarea accesului la resurse pentru alte categorii de utilizatori etc.

Phreaks - definesc acea categorie de cybercriminali care se concetreaza cu precadere asupra sistemelor de telecomunicatii cu unicul scop de a efectua convorbiri gratuite. (engl. **Phone bREAKS**)

Spre deosebire de hackeri sau crackeri, **traficantii de informatii**sau **mercenarii** se implica activ în comiterea de infractiuni cibernetice avand drept principal scop spionajul economic, politic ori militar dar si alte avantaje, precum: influenta, respect în bransa sau chiar castiguri financiare importante.

Acestia sunt preferati de persoanele sau organizatiile interesate intrucat prezinta "avantajul" disocierii rapide *angajat - angajator* în cazul unui esec.

Terorismul informatic (si, pe cale de consecinta, *teroristii informatici*) reprezinta inca un concept greu digerabil pentru marea majoritate a statelor. Nu exista nici macar o definitie unanim acceptata. Pana în prezent nu au fost identificate cazuri relevante, insa în perspectiva dezvoltarii acccentuate a tehnologiei informatiei si a cresterii gradului de dependenta a societatii si mediului de afaceri de infrastructura de comunicatii si IT ne putem astepta în viitor la o concretizare a acestui tip de amenintare.

Cyber-extremistii - acestia folosesc intens infrastructura de comunicatii si tehnologia informatiei, în special Internetul, pentru a initia sau coordona propagarea de idei care incita la ura pe temei de rasa, religie sau apartenenta sociala ori pentru a instiga mase de oameni la un comportament antisocial. Discutii aprinse exista inca pe marginea incadrarii în aceasta categorie si a celor care activeaza în spatiul virtual din convingere, care propovaduiesc "cuvantul" anumitor religii (culte, secte etc.) ori impartasesc/ disemineaza ideile unor grupuri de presiune (gen*luptatori pentru drepturile omului, activisti pentru protectia mediului, protectia animalelor* etc.) si care, intr-un anumit context dat, pot fi considerati de catre autoritati drept antisociali.

Exemple software pentru spionaj si infractiuni informationale

Mail Nukers.

Sunt programe care bombardează o căsuță de poştă electronică cu un număr mare de mesaje (care de obicei depăşeşte 10000). Acest bombardament duce la blocarea sau chiar pierderea unei căsuțe de e-mail. Majoritatea acestor programe au opțiuni care permit trimiterea de mail-uri anonime.

Net Nuke.

Acest program are o mulțime de versiuni, deşi toate au acelaşi efect şi mod de operare: trimit un pachet nedefragmentabil prin rețea, astfel încât când computer-ul țintă va încerca să-l defragmenteze, nu va reuşi decât să blocheze portul de rețea.

Concluzii

Expansiunea tehnologică şi scăderea prețurilor sistemelor informatice, crează on mod indirect posibilitatea diversificării modalităților de onfăptuire a ilicitului, extinderea valorilor şi relațiilor sociale puse on pericol, mărirea prejudiciilor şi creşterea exponențială a numărului de infractori virtuali.

De aceea este necesar ca on viitorul cît mai apropiat, să se poată vorbi despre apariția ştiinței dreptului penal informatic, pentru a onlocui aplicarea dreptului penal societății informatice, aşa cum este cazul acum. Dar pentru aceasta este nevoie de un efort conjugat, interdisciplinar.

Bibliografie

1. Constituția Republicii Moldova Publicat : 18.08.1994 în Monitorul Oficial Nr. 1 27.08.1994
2. Legea Nr. 112 din 22.05.2008 pentru aprobarea Concepției securității naționale a Republicii Moldova Publicat : 03.06.2008 în Monitorul Oficial Nr. 97-98

3. D. Oprea, *Protecția si Securitatea Informațiilor*, Ed. Polirom, 2003
4. C. Troncotă, *Neliniştile Insecurității*, Ed. Tritonic, 2005
5. V. Hanga, *Dreptul şi calculatoarele*, Ed. Academiei Rombne, 1991
6. Decizia Consiliului Uniunii Europene nr.375 privind combaterea pornografiei infantile prin
7. Internet, 9 iunie 2000;
8. Internet Crime Compliant Center (IC3) - http://www.ic3.gov/default.aspx.
9. National White Collar Crime Center (NW3C) http://www.nw3c.org/.
10. http://www.securitatea-informatica.ro.

ESTIMAREA CANTITATIVĂ ŞI CALITATIVĂ A RISCURILOR INFORMAȚIONALE

Rodica Bulai, drd UTM

This paper briefly describes the quantitative and qualitative risk assessment methods with attention on its advantages and disadvantages when applied in information security.

Estimarea riscurilor informaționale atrage după sine două abordări diametral opuse: cantitativă şi calitativă. Acestea sunt diferite prin natura metricii pe care o utilizează.

Abordarea cantitativă pune în aplicare două elemente fundamentale, şi anume probabilitatea ca un

anumit eveniment să aibă loc şi pierderea estimativă asociată cu acel eveniment.

Se recomandă ca pierderile să fie estimate pentru o perioadă de un an, astfel se poate determina:

- Pierderile Anuale Estimate însumând după categorii de amenințări: (*PAE_ai*),
- Pierderile Anuale Estimate însumând pe categorii de bunuri: (*PAE_bj*), şi
- Totalul Pierderilor Anuale Estimate pentru perechile bun/amenințare: *PAE*.

În ambele cazuri de calculare a pierderilor totale, pe categorii de amenințări sau pe categorii de bunuri, rezultatul trebuie să fie identic. Astfel, se poate genera o matrice amenințări/bunuri şi *PAE*-urile corespunzătoare fiecărui bun, respectiv, fiecărei amenințări şi *PAE-ul global*:

Matricea amenințări / bunuri

	Bunul b1	**Bunul b2**	**…**	**Bunul bn**	**PAE_ai**
Amenințarea a1	V1xE1	V2xE1	…	VnxE1	PAE_a1
Amenințarea a2	V1xE2	V2xE2	…	VnxE2	PAE_a2
…	…	…	…	…	…
Amenințarea am	V1xEm	V2xEm	…	VnxEm	PAE_am
PAE_bj	PAE_b1	PAE_b2	…	PAE_bn	**ΣPAE**

În această matrice, Vj este valoarea bunului bj, iar Ei - frecvența de producere a amenințării ai în decurs de un an.

Se identifică măsurile care pot duce la reducerea vulnerabilității față de amenințarea cea mai costisitoare. Întotdeauna se are în vedere că unele măsuri se pot aplica pentru mai multe categorii de amenințări ori pentru mai multe categorii de bunuri.

Selectarea măsurilor de control trebuie să se țină cont de realizarea următoarelor obiective:

- valoarea Rentabilității Investiției cât mai mare: $RI = r\_cxPAE\_a–C\_c$, unde C_c = Costul anual pentru aplicarea controlului c, r_c = indicele de eficacitate pentru controlul c și PAE_a = Pierderile Anuale Estimate pentru amenințarea a.
- minimizarea *PAE* (Pierderilor Anuale Estimate).

Avantajele abordării cantitative

- Aprecierea şi rezultatele sprijină o analiză statistică semnificativă, deoarece abordarea calitativă se bazează pe metrica şi procesele obiective independente substanțiale.
- Valoarea confidențialității, integrității şi disponibilității informației sunt exprimate în termini monetari cu analiza rațională . Aceasta facilitează înțelegerea pierderilor aşteptate.
- Luarea de decizii legate de bugetul securității informației este sprijinită de o bază credibilă de apreciere a costurilor/ beneficiilor pentru măsurile de atenuare a riscurilor.
- Performanța pentru managementul riscului poate fi urmărită şi evaluată cu uşurință.
- Riscul este mai bine înțeles, iar rezultatele de apreciere a riscului sunt deduse şi exprimate într-o manieră clară. Valoarea monetară, procentajele şi probabilitatea sunt estimate la cota anuală.

Dezavantajele abordării cantitative

- Pentru executarea unei aprecieri cantitative a riscului sunt necesare instrumente automatizate certificate şi o bază de cunoştințe asociată. Sunt de asemenea necesare eforturi manuale.
- Este necesară adunarea unei cantități considerabile de informație despre informația țintă şi mediul tehnologiilor informaționale utilizate.
- Cercetarea pericolului asupra populației şi a frecvenței pericolului trebuie să fie desfăşurate prin eforturile proprii ale utilizatorului, atunci când nu există o bază de cunoştințe relevantă.

Mulți experți susțin că o abordare pur cantitativă nu este practică datorită posibilului impact pe arie extinsă al unui incident şi dificultății de măsurare a unei valori numerice pentru mulți din aceşti factori. Prin urmare, poate fi necesară şi folosirea unei abordări de tip calitativ.

Aprecierea riscului de tip calitativ reprezintă procesul de evaluare a riscului pe baza analizei diferitelor scenarii care explorează impactul potențial şi posibil al diverselor incidente şi amenințări.

Majoritatea metodologiilor de apreciere calitativă a riscului utilizează un număr de elemente interconectate: amenințări, vulnerabilități şi bunuri. Astfel, riscul poate fi determinat prin: *R=Valoarea_bunului+Vulnerabilitate+Amenințare.*

Matricea de evaluare a riscurilor

	Amenințarea	**0**			**1**			**2**		
	Vulnerabilitatea	**0**	**1**	**2**	**0**	**1**	**2**	**0**	**1**	**2**
Valoarea bunurilor	**0**	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

De asemenea, este necesar de a se ține cont de câteva ipoteze foarte importante pentru estimarea calitativă a riscurilor, și anume:

1. Fiecare bun are valoarea sa și fiecare bun este vulnerabil sau nu.
2. În cazul în care un sistem este vulnerabil, există cel puțin o amenințare care poate fi realizată (amenințările și vulnerabilitățile depind unele de altele).
3. O amenințare are o anumită probabilitate de a fi realizată, în dependență de anumite circumstanțe.
4. O amenințare are anumite consecințe care depind de unele circumstanțe.

Bazându-ne pe ipotezele de mai sus, riscul poate fi calculat după următoarea formulă:

*R=Valoarea_bunului*Probabilitatea*Impactul*, unde

Probabilitatea=Vulnerabilitatea+Amenințarea.

Matricea modificată de evaluare a riscurilor

Amenințarea	**Probabilitatea**	**1**			**2**			**3**		
	Impactul (consecința)	**1**	**2**	**3**	**1**	**2**	**3**	**1**	**2**	**3**
Valoarea bunurilor	**1**	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36
	5	5	10	15	10	20	30	15	30	45

Avantajele abordării calitative

- Calculele sunt simple, de la sine înțelese, nu este necesară determinarea valorii monetare în ceea ce priveşte confidențialitatea, integritatea şi disponibilitatea informației.
- Nu este necesară estimarea costurilor măsurilor de atenuare a riscurilor recomandate sau calcularea costurilor/beneficiilor. Se adresează unei indicații generale a zonelor de risc semnificative.

Dezavantajele abordării calitative

- Aprecierea şi rezultatele riscului sunt în esență subiective atât în ceea ce priveşte procesul, cât şi metrica. Datele metrice independent obiective nu sunt utilizate.
- Percepția asupra valorii bunurilor țintă nu este dezvoltată pe o bază monetară obiectivă, ceea ce ar putea să nu reflecte valoarea efectivă supusă riscului.
- Nu este posibilă urmărirea performanței managementului riscului în mod obiectiv, din moment ce toate măsurile sunt subiective.

Cu toate acestea, nu este posibilă desfăşurarea unei aprecieri pur calitative a riscului. În realitate, cele două abordări au un caracter complementar, şi de aceea sunt recomandate de a fi, întotdeauna, puse în aplicare în combinație.

Bibliografie

1. Hrvoje Segudovic, *Qualitative risk analysis methodcomparison // http://www.infigo.hr/files/INFIGO-MD-2006-06-01-RiskAsses_ENG.pdf*
2. Ion I. Bucur, *Evaluarea și managementul riscurilor de securitate //* http://www.xanderzone.ro/cursurimaster/C-II-4.pdf.
3. Александр Астахов, *Искусство управления информационными рисками*, ДМК Пресс, Москва, 2010.

ТЕНДЕНЦИИ РАСПРОСТРАНЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дорошев Дмитрий, Корнеенко Ольга
УО «Гомельский государственный университет имени Франциска Скорины» (Гомель, Белоруссия)

In article attempt to carry out the analysis of threats of information security popular now is given. On the basis of reports of the leading companies in the field of information technology tendencies of distribution of the basic categories of threats are described.

В последние годы перед руководителями большинства компаний остро встал вопрос о сокращении издержек, в том числе и в сфере информационных технологий, где затраты некоторое время росли рекордными темпами. В конце 2008 года многие компании предпочли занять выжидательную позицию, сократив до минимума затраты на ИТ. Однако подобная стратегия не может быть долгосрочной, в связи с тем, что большинство компаний имеют серьезные ИТ-инфраструктуры, которые прочно интегрированы в бизнес, и для многих отказ от ИТ практически означает отказ от бизнеса.

Все ИТ-затраты условно можно разделить на три вида: затраты, ориентированные на поддержку, на обновления, на инновации. Очевидно, что без замены

вышедшего из строя оборудования, не обойтись, от расходных материалов тоже невозможно отказаться. Однако, многие проекты из категории «обновления», такие как переход на новые персональные компьютеры, обновление версий программ, могут быть отложены. При этом, как полагают аналитики, расходы на ИТ-безопасность потребуют дополнительных инвестиций.

Понять необходимость инвестиций в информационную безопасность в период урезания бюджетов подчас достаточно сложно. Отдача от таких инвестиций выражается не в том, что случилось и принесло прибыль, а в том, чего не случилось и что, предотвратило убыток.

Существуют количественные методики оценки возврата инвестиций от внедрения систем безопасности (ROI) [1]. Одну из них можно выразить формулой:

$$ROI = (C_1*N_1 + C_2*N_2 + C_3*N_3 + ... + C_n*N_n)/TIC,$$

где C_1 и C_2...C_n – средняя стоимость инцидента информационной безопасности;
N_1 и N_2...N_n – количество инцидентов информационной безопасности в год;
TIC – стоимость покупки и внедрения решения информационной безопасности.

Данную методику используют как для стоимостного, так и для качественного анализа угроз информационной безопасности. Для качественного анализа можно выбрать наиболее важные категории угроз (вирусные атаки, хакерские атаки, DDoS-атаки, интернет-мошенничество, инциденты информационной безопасности (IM-агенты), инциденты информационной безопасности по вине «мобильных» сотрудников, потери по причине несоблюдения требований, потери от деятельности инсайдеров, утечки данных) и изучить, какие из видов угроз имеют тенденцию к уменьшению, а какие – к увеличению.

Вирусы. В последнее время не наблюдается снижение темпов роста вредоносного программного обеспечения. Ежедневно появляются десятки тысяч новых и модификаций уже существующих вирусов. С 2000 года соблюдается экспоненциальный характер роста количества вирусных программ. Данный бизнес приобретает элементы групповой работы, присущие процессу написания сложного коммерческого программного обеспечения. Растет количество троянских программ, направленных на кражу информации о банковских аккаунтах. Киберпреступники продолжают проявлять повышенный интерес в поиске новых уязвимостей в популярном программном обеспечении, в первую очередь в MS Office и MS Windows, тем более что в странах СНГ остро стоит вопрос о лицензионном использовании данных программных продуктов.

Не следует забывать про рост атак на мобильные телефоны при параллельной их коммерциализации. Этот процесс становится следствием усиления конкуренции киберпреступников на технологическом уровне и их активной борьбы за увеличение числа зараженных компьютеров. По мере того как все больше устройств подключается к Интернету, количество угроз, связанных с проникновением в них вирусов, также растет.

Рост киберпреступности. Хакерские атаки, DDoS-атаки, интернет-мошенничество напрямую связаны с ростом киберпреступности. Особенно это заметно в период кризиса. Из-за нехватки легальных рабочих мест, актуальным становится нелегальный заработок, при этом происходит всё большая дифференциация киберпреступников, а каждая деятельность в зависимости от трудоемкости и опасности приобретает свою рыночную цену. По мере развития систем интернет-банкинга развитие получают фишинг, целью которого является получение доступа к конфиденциальным данным пользователей, и фарминг – автоматическое перенаправление пользователя на фальшивый веб-сайт. Подпольная киберэкономика становится международной. На черном киберрынке лучше всего продается информация о кредитных картах для доступа к банковским счетам и персональные данные граждан.

IM-агенты и социальные сети. Некоторое время назад в Интернет-пространстве широко обсуждалась тема жесткого контроля доступа в Интернет на работе. Однако концепция Web 2.0 свидетельствует, что общение с лучшими представителями сетевого сообщества – это огромный потенциал для компании. Запрещаемые одно время во многих компаниях программы Skype и различные мессенджеры уже активно используются в силу своей экономичности. А в социальных сетях «сидит» подавляющее большинство сотрудников как в рабочее так и в нерабочее время. Социальная активность сотрудников растет, и проконтролировать, где целевой, а где нецелевой web-доступ, очень сложно. Чем больше социальной активности – тем выше риск утечки информации. Кроме того, социальные сети становятся основной мишенью атак, так как содержат персональную информацию, которая может быть использована злоумышленниками.

«Мобильные» сотрудники. Известно, что с увеличением количества «мобильных» сотрудников вероятность инцидентов ИБ возрастает. Может расти количество командировок, в которые сотрудники едут с офисным ноутбуком. Офисные сотрудники могут переходить на режим работы из дома. Так что нередки случаи, когда офисный ноутбук становится домашним, а доступ к нему получает вся семья.

Соответствие требованиям и стандартам ИБ. В последние годы все больше отечественных компаний выходит на международный рынок, работает в тесной интеграции с западными партнерами, и их ИТ-инфраструктура все в большей степени подпадает под требования международных стандартов по ИТ-безопасности. Очевидно, что отсутствие у отечественных компаний систем безопасности международного уровня тормозит перспективы их сотрудничества с западными предприятиями. Необходим анализ существующих мер защиты и приведение их в соответствие с требованиями стандартов.

Инсайдеры. С точки зрения мотивов различают халатных, манипулируемых, обиженных, внедренных инсайдеров и т.д. Очевидно, что для перехода сотрудника из категории «лояльный» в категорию «инсайдер» более чем достаточно: увольнение, отпуск без содержания, отмена бонусов. Согласно опросам, в западных странах до 45% служащих готовы передать конкурентам корпоративную информацию в случае увольнения.

Все вышесказанное свидетельствует повышении риска инцидентов информационной безопасности. Следовательно, возможные потери от них будут расти быстрее, нежели стоимость внедрения решения информационной безопасности [2]. Можно утверждать, что важнейшим активом любой современной компании является информация. Как и всякий критически важный актив, информация нуждается в защите, а в случае ее утечки компания несет довольно серьезные убытки.

Литература

1. http://www.trainings.ru/library/dictionary/roi/
2. http://www.securelist.com/ru/analysis

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНВЕСТИЦИОННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

Ремезова Екатерина Максимовна,
Владимирский государственный университет
им. А.Г. и Н.Г. Столетовых, Россия
Дорохов Михаил Александрович,
Харьковский национальный экономический университет,
Харьков, Украина

The purpose of this article is research of a problem of the accounting of uncertainty in case of support of information security of acceptance of the investment decision. Based on results of the detailed comparative analysis of existing methods, possible ways of overcoming of their shortcomings by means of use of the device of the theory of fuzzy sets and in particular type-2 fuzzy sets are considered.

Важным условием стабильного функционирования и развития любого крупного предприятия является эффективная инвестиционная политика, которая ведет к увеличению объемов производства, росту доходов, а, следовательно, наращиванию экономического потенциала. Обширная практика проведения реальных прогнозных расчетов инвестиционного проекта свидетельствует о необходимости всестороннего учета различных видов неопределенности при оценке, планировании и управлении инвестиционными проектами.

Действительность такова, что влияние факторов неопределенности на рассматриваемые проекты приводит к нарушению информационной безопасности инвестиционной деятельности предприятия, которое приводит к неожиданным потерям, убыткам, даже в тех проектах, которые первоначально признаны экономически целесообразными для предприятия. Под информационной

безопасностью мы понимаем степень доверия к информации, которая представляется топ-менеджменту, полученной в результате аналитической подготовки инвестиционного проекта.

Учет неопределенности информации и его эффективность напрямую зависят от выбора инструментария, на основе которого будет обеспечиваться информационная безопасность решаемых предприятием инвестиционных вопросов. Этап обоснования и выбора инструментария, обеспечивающего приемлемую формализацию неопределенности и адекватное решение задач, возникающих при управлении реальными инвестициями, является крайне важным. Необоснованный и как, следствие, не правильный выбор, в основном, приводит к неадекватности созданных моделей, получению неверных результатов в процессе их применения и, соответственно, возникает недоверие к полученным результатам, и игнорируются выводы на их основе. Вследствие чего, и происходит нарушения информационной безопасности, которые в свою очередь ведут к необоснованному и зачастую избыточному расходованию финансовых средств, как самого предприятия, так и инвестора.

В настоящее время в экономической практике под ***неопределенностью*** понимается неполнота или неточность информации об условиях реализации проекта, в том числе о связанных с ними затратах и результатах.

Исходя из приведенного выше описания неопределенности, можно выделить следующие факторы, которые характерны для любого инвестиционного проекта и напрямую влияющие на информационную безопасность его реализации:

- неопределенность исходных данных;
- неопределенность внешней среды;
- неопределенность, связанная с характером, вариантами и моделью реализации проекта;
- неопределенность требований, предъявляемых к эффективности ИП.

Учитывая факт наличия неопределенности при проведении инвестиционного анализа, можно сделать вывод о том, что классические статистические методы, такие как *метод корректировки ставки дисконтирования (премия за риск); метод достоверных эквивалентов (коэффициентов достоверности); анализ чувствительности показателей эффективности; метод сценариев;* методы теории игр (критерий максимина, максимакса и др.); *построение* «дерева *решений»; имитационное моделирование* по методу *Монте-Карло,* окажутся неэффективными и дадут не объективные (неадекватные) результаты, что в должной мере не обеспечит соответствующую информационную безопасность и приведет к повышенному и неоправданному использованию инвестиций.

Для решения данной проблемы некоторыми исследователями предлагаются методы и модели оценки инвестиционных проектов в условиях риска и неопределенности на основе аппарата теории нечетких множеств, позволяющий сформировать полный спектр сценариев реализации инвестиционного проекта. При этом решение принимается не на основе нескольких оценок эффективности проекта, но

по всей совокупности этих оценок. Ожидаемая эффективность проекта не является точечным показателем, а представляет собой поле интервальных значений со своим распределением ожиданий, характеризующимся функцией принадлежности соответствующего нечеткого числа. А взвешенная полная совокупность ожиданий позволяет оценить интегральную меру ожидания негативных результатов инвестиционного процесса.

Разработанные в настоящее время различные алгоритмы оценки эффективности инвестиционных проектов в условиях неопределенности ориентированы в основном на нечеткие множества первого порядка. Проведя анализ известных алгоритмов оценки[1], а так же экономических условий реализации инвестиционных проектов, можно сделать вывод о том, что в ряде случаев нечеткие множества первого порядка не могут обеспечить получение наилучшего решения ввиду недостаточно обоснованного выбора параметров моделирования, а поиск эффективных решений сопровождается значительными временными затратами из-за необходимости выполнения многократных реализаций используемых методов, моделей и алгоритмов с целью выбора наилучших параметров. Так же нельзя не отметить тот факт, что при принятии инвестиционного решения возникают различные виды неопределенности, которые трудно описать с помощью нечетких множеств первого порядка. Это происходит из-за того, что при использовании нечетких множеств первого порядка необходимо точное задание границ функции принадлежности, что в свою очередь несет недопустимое модельное упрощение и к тому же некорректно снижает степень неопределенности относительно оцениваемого проекта.

Нечеткие множества второго порядка являются обобщением нечетких множеств первого порядка. Алгоритм оценки эффективности инвестиционных проектов на основе нечетких множеств второго порядка состоит из следующих этапов:

1. Инициализация — выбор исходной совокупности инвестиционных проектов.
2. Задание исходных параметров инвестиционных проектов на основе экспертных оценок с преобразованием их в интервальную форму.
3. Выбор вида функции принадлежности.
4. Задание параметров функции принадлежности.
5. Расчет значений критериев оценки на основе интервальной математики для НМ2 (значения α-срезов показателя эффективности).
6. Построение функций принадлежности для каждого ИП (строятся соответствующие пары значений на основе функции random).
7. Дефаззификация полученных нечетких результатов.
8. Выделение области нахождения наилучшего решения (использование методов Min и Max).
9. Нахождение наилучшего решения из выбранной области на основании компромисса между допустимыми рисками и прогнозируемым доходом.

[1] Зенчук А. И., Шашкин А. И. Нечеткая модель оценки инвестиционных проектов // Вестник ВГУ, серия: системный анализ и информационные технологии, 2008, № 1, С. 117-123

Таким образом, может быть решена актуальная на сегодняшний день задача обеспечения информационной безопасности финансового бюджетирования в условиях неопределенности, основанная на нечеткой параметризации исходных данных. Используя рассмотренный алгоритм, можно рассчитать требуемые показатели экономической эффективности инвестиционных проектов и по совокупности определить наиболее выгодный как для инвестора, так и для руководителя.

ОПЫТ ЕС ПО РАЗРАБОТКЕ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Юрчук Виталий Анатолиевич,
эксперт НПО "Центр исследования проблем регионального и международного сотрудничества" (Львов, Украина)

Over the last two decades, the Internet has had a tremendous impact on all parts of European society. Information and communications technology has become the backbone of economic growth. To outline the EU's vision in this domain and protect cyberspace from misuse the European Commission has developed proposal for a Cybersecurity strategy of the European Union.

Стремительные темпы развития Интернета превратили всемирную сеть в неотъемлемую часть мировой и европейской экономики. Согласно результатам исследования международной консалтинговой компании McKinsey Global Institute "Влияние Интернета на экономический рост и благосостояние общества" [1], активное использование компаниями малого и среднего бизнеса Интернет-технологий способствует ежегодному увеличению ВВП тринадцати крупнейших мировых экономик в среднем на 3,4%.

Параллельно с ростом уровня использования Интернета малым и средним бизнесом, в Европейском Союзе происходит активный процесс интеграции информационно-коммуникационных технологий (ИКТ) практически во все, в т.ч. стратегические, отрасли национальных экономик. Нарушение штатного режима функционирования информационных и сетевых систем на объектах стратегического значения может привести к катастрофическим последствиям.

Интернет-аудитория ЕС на сегодня составляет около 72% населения политической организации, а всемирная сеть рассматривается как неотъемлемая медийная площадка и средство коммуникации общества. Подтверждением этому может служить решение Федеральной судебной палаты ФРГ от 24 января 2013 года, согласно которому Интернет и электронная почта признаны в стране базовыми потребностями человека.

Активное использование Интернета органами государственной администрации, интеграция ИКТ в стратегические отрасли экономик превратили всемирную

сеть в новую сферу противоборства между государствами. Широкое использование всемирной сети коммерческими организациями и населением Евросоюза для управления финансовыми ресурсами привели к стремительному распространению трансграничных киберпреступных группировок и соответствующего увеличения уровня недоверия населения ЕС к Интернету. Согласно результатам исследования Европейской Комиссии, на сегодня около 40% Интернет-пользователей стран ЕС считают реальной угрозой возможность компрометации персональной информации в сети, а 38% опасаются проведений финансовых он-лайн транзакций [2].

В отличие от традиционных угроз европейской безопасности (например, международной торговли людьми, наркотиками и т.д.), противоправная деятельность в Интернете характеризуется рядом особенностей. В большинстве случаев источники кибератак невозможно отследить и установить, атаки проводятся быстро и скрытно. Отсутствие границ в виртуальном пространстве может привести к тому, что атака на одну из стран ЕС может нанести значительный ущерб для всей организации. Это обусловливает необходимость разработки новых механизмов противодействия киберугрозам.

В ходе выступления на Всемирном экономическом форуме в Давосе в январе 2013 года комиссар ЕС по цифровой политики Н.Кроес подчеркнула, что одной из самых распространенных ошибок есть неверное толкование кибербезопасности как исключительно технического задания [3]. Главным субъектом обеспечения безопасности киберпространства в интересах бизнеса и общества является государство, а деятельность по повышению уровня кибербезопасности должна происходить на всех уровнях и рассматриваться как стратегическая общеевропейская задача.

С целью создания системы кибербезопасности ЕС, основное внимание европейских органов уделяется вопросу разработки соответствующей нормативно-правовой базы. Несмотря на значительный прогресс в этом вопросе, готовность политической организации и отдельных стран-участниц к противодействию потенциальным киберугрозам остается недостаточной. Этот факт, в частности, подчеркивается в резолюции Европарламента "По вопросам киберзащиты и обороны" (Report on Cyber Security and Defence) № 2012/2096 (INI) от 22 ноября 2012 года [4]. В документе особо отмечается увеличение угроз от использования виртуального пространства террористическими организациями (кибертерроризм), которые обладают достаточным потенциалом для проведения кибератак с критическими для ЕС последствиями.

К основным недостаткам системы кибербезопасности Евросоюза относятся:

- отсутствие единой европейской системы реагирования на кибератаки, единых национальных стандартов, а также унифицированного категориального аппарата в сфере кибербезопасности;
- недостаточный уровень координации деятельности между наднациональными и национальными гражданскими и военными органами в сфере безопасности киберпространства;

- низкий уровень межгосударственного обмена информацией о киберугрозах;
- недостаточный уровень государственно-частного сотрудничества;
- значительная диспропорция уровня готовности к противодействию киберугрозам на национальном уровне. На сегодня только 10 из 27 стран ЕС отработали соответствующие национальные стратегии кибербезопасности;
- недостаточное финансирование мероприятий по противодействию киберугрозам.

С целью формирования общеевропейского подхода к улучшению уровня безопасности киберпространства 7 февраля 2013 года Европейская Комиссия представила "Стратегию кибербезопасности ЕС: открытое и безопасное киберпространство" [5]. В документе сформулированы пять стратегических приоритетов Евросоюза в сфере улучшения уровня безопасности киберпространства:

- достижение устойчивости информационных систем к киберугрозам;
- радикальное уменьшение уровня киберпреступности;
- разработка политики и создание потенциала в сфере кибероборонны в рамках Общей политики безопасности и обороны;
- разработка производственных и технологических ресурсов в сфере кибербезопасности;
- создание согласованной международной политики ЕС в сфере безопасности киберпространства.

Ключевым фактором улучшения уровня кибербезопасности рассматривается принятие "Директивы по безопасности сетей и информации". Документ предусматривает устранение существующего "добровольного реагирования" частного сектора на киберинциденты и введение механизма обязательного информирования национальных органов о фактах выявленных киберугроз. Предложенная норма будет распространяться на определенный перечень частных структур, включая организации банковской, энергетической, транспортной и т.д. систем, которые имеют стратегическое для безопасного функционирования ЕС значение.

Представленные Европейской Комиссией предложения вступят в силу после их рассмотрения Европейским Парламентом.

Таким образом, обеспечение кибербезопасности рассматривается Европейским Союзом как ключевой фактор дальнейшего экономического роста и улучшения благосостояния общества. В связи с этим, политическая организация ведет активную деятельность в направлении разработки необходимого нормативно-правового регулирования безопасности киберпространства.

Литература:

1) McKinsey Global Institute, The great transformer: The impact of the Internet on economic growth and prosperity [Электронный ресурс] – Режим доступа:

http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/the_great_transformer
2) European Commission, Cyber security report [Электронный ресурс] – Режим доступа: http://ec.europa.eu/public_opinion/archives/eb_special_399_380_en.htm
3) Neelie Kroes, Speech: EU Cybersecurity Strategy [Электронный ресурс] – Режим доступа: http://europa.eu/rapid/press-release_SPEECH-13-51_en.htm
4) European Parliament, Resolution on Cyber Security and Defence [Электронный ресурс] – Режим доступа: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2012-457
5) Cybersecurity Strategy of the European Union [Электронный ресурс] – Режим доступа: http://ec.europa.eu/information_society/newsroom/cf//document.cfm?doc_id=1667

SAFETY OF ELECTRONIC COMMERCE IN BULGARIA – SAFE OR RISKY METHODS OF WORK

Tsvetelin T. Borisov
Student,"D.A.Tsenov" Academy of Economics,
Svishtov, Bulgaria

In this report we review any possible attacks against the Internet electronic commerce and also we have listed some of the most common attacks and existing problems. At the same time this report will provide advice and recommendations for improving more safe usage of electronic systems.

With the advent of the new modern technology at the beginning of the XXI century in the field of electronic commerce, users of such systems are becoming a target of many abuses of their personal information. Each system is designed to promote and facilitate trade and payment, but to use it we have to provide lots of personal data (gender, age, residence, address, etc.). With this data, e-commerce systems are an easy target for possible attacks, the main goal of which is the personal information.

Most - frequent attacks in e-commerce, according to some authors (the online edition http://www.nlcv.bas.bg[1]) are:

Attack on the basis of predicting - online information is transmitted between computers via the so-called TCP / IP packets, called simply packets which to be able to move need two coordinates. The first coordinate is called IP address of the computer receiver of information and the second one is the unique serial (consecutive) number of the package.

[1] types of threads - http://www.nlcv.bas.bg/bulgarian/vidove.htm

Attack via copying – this attack is carried out by monitoring, reviewing and copying of any separate packet or sets of packets on the entire TCP stream for a specified period of time or when the necessary resources on the computer which is controlled by a hacker are available of total TCP traffic. In this way the full information of the entire network is gathered in one place, allowing in a relaxed environment to dismantle all packages, including the detection of certain passwords and procedural specifics.

Attack via camouflage - here the main idea is, that the hacker could masque himself/herself as a client and on his behalf (using his IP address) to start or continue the already started session with the server by sending synchronized packets. The next step is to carry out a series of actions aimed to preserve the server condition in which it is currently at the moment. By doing this in the most cases the server ignores the masking and although in most cases the attacker's computer can receive data from the server, or it can send data to it and this is a serious potential threat.

Recommendations to consumers using the Internet for e-commerce according to one of the most-secured online Banks, i. e. Piraeus[1]:

Protect the user's computer – in order to do that you have to install and use antivirus and antispyware software on line. It will protect you from viruses and spyware. Always keep monitoring if you have installed the latest version of the above programs and update them with the latest virus definitions. Remember, that new viruses appear every hour and not updated software may not be able to detect and block them.

The security in making online transactions by using additional identification scheme and certificates should be increased – There are additional methods of protection in any system which is used in the Internet, such as electronic certification systems and additional methods of identification. In most cases this kind of certificates are installed on your computer, which increase the protection level of security**.**

Proven methods of secure payment has to be used, for instance **such** as PayPal and shop only from traders registered in this system. If there is a problem with your good it can get some of your money back as a guarantee up to a certain value, according to the region in which you are located. The Bulgarian version of PayPal is called ePay. These systems are reliable, because after you sign up and your credit / debit card is verified shopping trader doesn't have access to its data or validator.

It is strongly recommended to avoid shopping from online stores which require payment by credit card, and in which you need to enter numbers and validator. If you decide to do that, collect all available information about the trader company (physical address, telephone numbers, etc.) and t keep it until you receive the ordered goods.

On the other hand except, usage of reliable systems on the Internet we have to care, about one of the most important things – the password. In the official website of Microsoft[2] you may find the following tips about the choice of a password:

---

[1] Advices for how to use internet safe - http://www.piraeusbank.bg/ecPage.asp?id=251005&lang=1&nt=96

[2] Microsoft - http://windows.microsoft.com/bg-bg/windows7/tips-for-creating-strong-passwords-and-passphrases

- To be at least eight characters long
- Not contain an username, real name or company name
- To be more than one word
- To be different from your previous passwords

In conclusion we can say that e-commerce unite a lot of technology within, offering a convenience for its users. We witness a boom in the IT field, which has its pros and cons. Therefore, it can be concluded that to solve the problems with the security of e-commerce we need to find a solution for the issues related to the protection of the technologies used for their realization.

References:

1. Types of threats - http://www.nlcv.bas.bg/bulgarian/vidove.htm
2. Tips for safe Internet use-http://www.piraeusbank.bg/ecPage.asp?id=251005&lang=1&nt=96
3. http://windows.microsoft.com/bg-bg/windows7/tips-for-creating-strong-passwords-and-passphrases

PREREQUISITES AND DISADVANTAGES IN E-COMMERCE

Boryana Todorova
Academy of Economics "D. A. Tsenov", Svishtov, Bulgaria

In our modern way of living, new technology is developing and it is everywhere around us. We can use it not only in the office or at home, but everywhere else outdoors. Web-based devices are perfect solution to be in touch with everyone and to run business in every point of the world. E-business and e-commerce nowadays are very easy and available way for shopping. Unfortunately, there are some problems which have to be solved in order to increase the number of e-shops consumers. Security in Internet is important way to secure your data and personal information and your system and technology.

The number of customers which use electronic services is increasing in every second. Emerging new technologies allow mobile and permanent access to web environment. This is a prerequisite to increase the need for electronic applications, sites, programs and communication systems. Internet clients are few because they are not informed about the countless opportunities that it provides. Although e-commerce is everywhere around us and it enters our customers habits as an available and easy way of shopping. According to Bulgarian E-commerce association it is expected a surge in 2011 about 50% in using e-shops. In comparison with the other members of European Union Bulgaria has very poor results of e-commerce, i.e. only around 2-4 % of Bulgarians are active clients of Internet shopping [1]. The main reason is psychological attitude and distrust in these systems.

The most popular way of shopping is the traditional way when you can see, touch and even try the goods. But now there are some new ways of trading and buying goods. For example, in the UK there are dedicated television channels and they offer only goods which you can buy via telephone. Another way is online shopping. But at the same time there are some problems which could arise when it comes to delivery. Many customers complain of goods' quality which turns out not to be the same as it was written in the offer, or it is not the same as it looks on the web site. Also some orders may have been lost during the delivery time. One of the problems in using e-shops in Bulgaria is that your order will be delivered only by courier and you must pay extra money which discourage customers. Fortunately, according to European customer centre in Bulgaria problems with delivery have significantly decreased, the goods recently are with good quality and without defects [2].

The problems indentified are distrust in local firms and manufactures, which offer usage of e-shops and e-services. Other disadvantages are: bad customer service; low quality products; long-period for delivery and lack of variety in payment process [1]. Products that we buy via Internet are not always with the same size, quality or origin, and this is a prerequisite not to use Internet as main source of goods. Payment process must assure clients about their resource security and they must feel free and safe in using e-shops. 85% of Bulgarian customers pay their money in cash when the delivery comes, and only 15 % think that Internet is safe enough to trust the system and provide their data.

In Bulgaria there are many opportunities in using e-shops and e-commerce. The problems which the country must solve are to make people trust and use Internet for shopping and to know that it is a safe place for their data and money. E-commerce allows rich variety of products, so you can choose the most comfortable time for yourself to shop, and also you can choose the way of payment. Distant access is one of the main functions of system components for complex security of information. It contains devices for identification and authentication, devices for authorized access of using a computer system, devices for event registration [2].

One of the threats when you use Internet as an alternative way of trading is the existing of viruses and security of personal information and data resources. There have been many cases in which we may think that the computer or another technology system has been infected by a virus when a client has used Internet. For crackers and hackers this is a good way to steal data from your computer and to abuse it. When it comes to money and transactions customers and e-shops providers must be more careful and this must be the safest place in web site. We had witnessed, or maybe even were victims, of criminal usage and stealing money from credit and debit cards. Bank accounts can be affected by thefts if websites do not offer adequate security [3].

There are methods such as encryption, digital signature and certification, which are common ways to provide security. The first method contains one or more algorithms for encrypting, keys which use those algorithms and systems for managing the keys. According to the method for encrypting in the very beginning the text is processed by those algorithms for encrypting and the keys are sent later to the correspondents.. This method has two very

important advantages - the key can be used with one algorithm for sending messages to people and if the key somehow became known then it can be changed without changing the algorithm. The second one, digital signature, is equivalent to the traditional signature, which is applied when the transaction is initialized and the information is not changed or destroyed. It can be used in two ways - with one secret key, which can be used by the two-parties or with two secret keys - one key for every single party. Electronic certificate is a digital document which connects the public key with certain consumer or application. This relation ties the identification of the person who possesses keys, which will be used for encrypting and signature [3]. These three methods are an important and irreplaceable way for ensuring the information will be not used improperly.

In conclusion we can argue that the e-business sets many challenges in front of corporations, firms and organizations in every world economy. Before Bulgarian economy and Bulgarian community the solution for these problems is related to many other different problems of economical, social, political, cultural, moral nature. The morality of using Internet and the security of personal information and data are the main reasons why the e-business is not a preferred way for shopping. Along with technology development e-commerce will be known and easy way to buy products and goods, due to its offering f a high variety of goods and an easy way of ordering them.

References:

1. Lukanov B., Which is the biggest problem in the development of e-commerce in our country? <http://www.biservalov.net/blog/problemi-na-elektronnata-targovia>
2. Annual Report European Consumer Center, Bulgaria, 2011
3. Kraev L., Kraeva V, Emilova P., E-Business, Faber 2009.
4. Pandev S., Ecommerce Threads & Solutions < http://www.ezinearticles.com/? Ecommerce- Threats-and- Solutions&id=884278>

Materialele Conferinței "Securitatea Informațională 2013"
sunt publicate în redacția autorilor.

Semnat pentru tipar 09.04.13.
Coli de tipar 7,80. Coli de autor 7,85.
Tiraj 25 ex.
Tipografia Departamentului Editorial-Poligrafic al ASEM