Библиографический список

1. Дегтярева, А. Методы идентификация личности по радужной оболочке глаза / А. Дегтярева, В. Вежневец // Компьютерная графика и мультимедиа. – [Электронный ресурс] – электрон. дан. – Вып. № 2 (6). – 2004. – Режим доступа: http://www.cgm.computergraphics.ru/content/view/61.
2. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. Монография. — Пенза: Изд-во Пензенского государственного ун-та, 2000. – 188 с.

PROBLEMS OF INFORMATION SECURITY

Kostadinka Cabuleva, *MSc*
Faculty of Economics, "Goce Delcev" University - Stip
(Republic of Macedonia)

We know that information security have economic impact on organizations. Collection, aggregation and access to information in today's organizations is based on innovation, which in turn create conditions for a positive feedback cycle of development. Speed and accuracy in the flow of information processes determine the rate of development and degree of certainty. Information security has as its sole purpose to protect the information resources of the organization, without being in conflict with the safety of staff, norms and generally accepted moral principles.

Information risk and the economics of managing security is a concern of private-sector executives, public policy makers, and citizens.[1] Information is an asset that, like other important business assets, adds value to the business of the company (organization) and therefore should be protected. Information security protects information from a number of threats in order to ensure continuity, to minimize damage to the company (organization) and to maximize return on investment and business opportunities.

Today, the reliability of information systems and services makes companies and organizations more vulnerable to security threats. The reasons are many but the basis is the very nature of cybercrime-they are more hidden and more complex, making their detection difficult. The company management should en-

[1] M. Eric Johnson "*Managing Information Risk and the Economics of Security*", Center for Digital Strategies Tuck School of Business at Dartmouth Hanover, NH, USA, 2008.

gage in the process of evaluation of resources for safeguards. Even in cases where the level of information security is clearly insufficient technical specialists have trouble justifying to senior management of the necessary funding. If the information is valuable in practice there is no threat to information assets of the company's potential losses are minimal (manual confirms it) and you can forget about security systems. However, if the information has a particular value, threats and potential losses are clear, then the budget (with the absolute conviction of this manual) should include funds for the security subsystem. Information security is ensured by a set of measures at each stage of the life cycle of information system, the value of specialized subsystem in the general form of the cost of design work, purchase and setup of software and technical resources, incl. internetwork screens, cryptographic tools, antivirus systems, means of authentication, authorization and administration costs to physical safety, staff training, management, maintenance and periodically update the system. It is interesting that the main causes of damage, especially in the financial sector are employees in the company followed by former employees, while the damages from outsiders are contributing much less. The types of attacks can be summarized in: stealing passwords - methods to obtain other user passwords; social engineering - the acquisition of information to which they have access; errors and black door (bugs and backdoors) - destination (use) of benefits through the use of systematic errors; opportunities for authentication - the use of defects (inconsistency and incompleteness) of the authentication mechanisms; errors (failures) in some protocols - protocols with errors in design and implementation; leaks - use of systems such as system signature (finger) or a named system (DNS) information needed by administrator or necessary for the functioning of the network, but which can be used for network attacks; denial of service - attempts to deprive consumers of the services of their computer system.

Also fraud by phone, online or by mail continue to grow and is on the rise. Such types of fraud where the true owner of the card is not present when the transaction shows an increase of 5 percent annually. Banks have reduced losses by two thirds of investment in new technology and upgrading systems for information security. Thus, the efforts of banks to fight criminals and frauds with credit cards and bank accounts are successful and show excellent results. In America banks cooperate with police, with special sections on financial fraud, but also invest in software and identification of fake websites that timely prevent abuse of the bank accounts of us-

ers (various benefits of lottery, offering online job offering rate for transferring money to your account various types of heritage). However, most studies show that 40 percent of banks do not report incidents to protect their reputation and trying internally to cope with problems.

In the modern market economy each firm is forced to work in conditions of fierce competition. When possible use by competitors of confidential information obtained in ways not entirely legitimate. This leads to obvious violations of rights of owner of industrial or intellectual property rights. Subject of harm may be know-how, trade and financial secretions, interference in the privacy of the citizen and the others. Security policy is the set of rules and practices that govern how an organization manages, protects and distributes information.

The problem of information security is the world's number one priority, and its solution should lead to maximum security for network resources with minimal impact on user access and productivity. Consequences of breaches of information security: loss of revenue; reducing investor confidence; reduce the confidence of customers; disclaimer consequences; deterioration of goodwill; loss or compromise of data; violation of business processes.

Price decisions against major security issues: - limiting functionality for improved security; -compromising the ease of use of the Internet; - need for investment of considerable human and financial resources.

References

1. Bogetoft, P., Damgaard, I., Jacobsen, T., Nielsen, K., Pagter, J. and Toft, T. "Secure Computing, Economy, and Trust - a Generic Solution for Secure Auctions with Real-World Applications," Report RS-05-18, Basic Research in Computer Science. 2005.
2. L. Jean Camp and Stephen Lewis "Economics of Information Security (Advances in Information Security)" Kluwer Academic Publishers, 2008
3. M. Eric Johnson, "Managing Information Risk and the Economics of Security" Springer, 2008
4. Mark Stamp, "Information Security – Principles and Practice", John Wiley & Sons, Inc., New Jersey, 2006;