2. Создание и внедрение комплексной системы защиты информации и информационных ресурсов, включающую в себя криптографическую и антивирусную защиту, систему межсетевого экранирования, подсистему аутентификации и идентификации при доступе, подсистему управления, доступом, подсистему защиты информационных систем при их интеграции между собой, а так же при подключении к внешним телекоммуникационным системам.
3. Создание системы аттестации объектов информатизации на предмет соответствия требованиям информационной безопасности.
4. Распределение полномочий между компетентными ведомствами в области организации и обеспечения информационной безопасности и создание реальных механизмов для реализации концепций и политик.

THE LEGAL BASIS OF INFORMATIONAL SECURITY IN FACE OF MODERN WORLD REALITY OR ONLY A MYTH

Michał MAZUR,
Institute of Political Studies and International Relations
(Cracow, Poland)

The article examines contemporary issues combined with the problem of legal basis of informational security. In this brief text author tries to underline some of the most important questions which arise from many attempts to create the sufficient legal model of information protection. The task seems obviously to be very hard but in the end it's not impossible.

1. Introduction

In modern world almost all critical aspects of people activity are supported by legal regulations. This matter has fundamental meaning for their stability and continuity. Generally when something is obvious it is much easier to obey, to comply with regulations.

Informational security, both real and legal, seems to be the first rate factor for the functioning of individuals, institutions and, in the first place, for political organisms which are independent states. For centuries one can point many examples where the effective information handling was essential for the final result of each scuffle.

Real informational security, mentioned above, must have, in every case, foundation. This foundation is legal regulation which is able to sanction effective security of identified data. Symptomatic, in this field, is statement that to keep a secret, silent is not sufficient [1].

2. Contemporary patterns and issues

Most of contemporary states rest their legislation, as regards informational security, on regulations focused around information defined as classified or secret. The other area, which is thought to be crucial, are the issues of state security, fundamental for every political authority. These are usually gathered by legislator in constitution or in the legal acts of the highest rank. Exceptions in certain states are capital planning practices within the government or agency-specific policies [2].

For example we can take Republic of Poland, where the foundation is act that specifies the protection of classified information or data. It determines the procedures and organization of this partly restricted state area [3]. One can enumerate some of act's aspects such as: classification of information in order of it's importance, access to specified types of data, the course of examine proceedings which let particular units to have opportunity to familiarize with classified information, the bureaucratic system which carries secret documents, and finally the physical protective means combined with IT services able to process information.

As one can see it is very specific field of legislation. The creators of this type system must know not only the unique character of informational security, but also must be familiar with nowadays IT threats which seem to be uncontrollable. Nevertheless it's almost impossible to compose such perfect network, able to stop criminal elements. Elements that attack with growing aggression due to the rising price of information in modern world.

The state informational security and its legal basis is not everything. It doesn't cover the whole scope of problems combined with this issue. On the other hand we have private sector, present and highly important in every country, which is also exposed to the same type of threats.

Access to stored information on computer databases has increased greatly. More and more companies store business and individual information on computer hard disks than ever before. Much of the information stored is highly confidential and not for public viewing. Its value is often higher than some fixed assets of particular company.

Many businesses are solely based on information. Personal staff details, client lists, salaries, bank account details, marketing strategies and sales information may all be stored on a database. Without this information, it would often be very hard for a business to operate. Information security systems need to be implemented to protect this information. But not only this. It is crucial to ensure that in case of emergency, in case of committed crime, the information will be properly secured and that each state will make sufficient efforts to protect valuable information with proper legal regulations. It is all because nowadays typical guarantees can be simply useless [4].

In highly networked IT society, IT trouble caused by one often even not significant company may possibly cause damages to the entire society. Therefore, ensuring information security in companies should be done not only to obey the law and to minimize its damage, but also to instill everyone the responsibility as a member of the society. Thus, the task of the government is also to value companies efforts to improve their information security. It can't be done without proper legal basis.

The same refers to online identity theft, in which confidential information is illicitly obtained through a computer network and used for profit. It is undoubtedly a rapidly growing enterprise. Credible estimates of the direct financial losses exceed much more than a billion dollars per year. Indirect losses are much higher, including customer service expenses, account replacement costs, and higher expenses due to decreased use of online services in the face of widespread fear about the security of online financial transactions. Increasingly, online identity theft is perpetrated using malicious software. It can be used to obtain many kinds of confidential information, including user names and passwords, social security numbers, credit card numbers, bank account numbers, and personal information such as birthdates and mothers' maiden names. In this field the number of legal acts is growing but there is still much to improve.

3. Summary

To summarise, there is none legal environment which fully protects information, which can assure the owner of particular data that it is safe and absolutely nobody can get access to check it. In case of information security is never ending process that requires constant monitoring, updates, research, investment and implementation of new technologies. But before everything the secret lies within the law system which is able to control all abuses. The perfect model simply can not be done. The role of each legislator is to try to gain such a level that will increase, as much as possible, probability of safety.

On the other side the punishment must be also quite severe. But here emerges another problem. To punish with pecuniary penalty or with insulating penalties. Consciousness of concrete society is crucial in this case.

Nevertheless, does every modern country has that kind of muscle to enforce the implementation of its own legal regulations, basis, in relation to informational security. For many reasons, some of them were mentioned above, it raises concerns.

Information security is becoming more demanding, as the skills involved become more complex and managerial. Experts who create protection models or systems must be aware of the enormity of obstacles which have to be surmount. Obviously it is not easy but also can't be left unsolved.

Bibliography

1. Claudel, *Journal 1904-1955*, PAX, Warsaw 1977
2. Abeles, Bartol, Batdorff, Hash, Rollins, Robinson, *Integrating IT Security into the Capital Planning and Investment Control Process*, NIST, Gaithersburg 2005
3. Namieśnik, Wesołowski, *Security and protection of data*, Gdańsk 2007
4. Kifner, *Security policy and the protection of information*, Helion Publishers, Warsaw 1999

О ТЕХНОЛОГИЧЕСКИХ АСПЕКТАХ ЕДИНОГО ГОСУДАРСТВЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Андрей САУЛЯК,

ЦГИР "REGISTRU" Министерства информационных технологий и связи Республики Молдова

Aspects of security at creation uniform system of paper and electronic state document circulation. Protection methods of electronic documents. Electrodigit Technology of Protection of the paper documents.

Построение единого государственного документооборота (ЕГД) кажется задачей невыполнимой или требующей несоизмеримых усилий. Но даже если она будет жестко-вертикально внедрена не факт, что она сможет существовать и поддержи-