THE IMPACT OF INFORMATION SECURITY UPON MODERN SOCIETY

Н. П. Шевцов
Научный руководитель преподаватель В. Н. Юрданова
Сибирский федеральный университет

> *"The era of sociotechnical systems is coming, and those of us who is able to integrate human and technical factors will be most fit for their time."*
>
> Edgar H. Schein (b. 1928)

Recently, Information Security has received a lot of attention in our societies and trade press in the Russian Federation in the USA and in EU. A current stage of society development is characterized by the increasing role of information sphere. It increasingly affects the state of political, economic, defense, personal security and other components in any modern society.

There are many different effects in positive and negative ways of information security technologies upon society in general and civil society organizations in particular. Information security mechanisms have the potential to act as enablers or disablers for the work of civil society groups. Recent increased emphasis on national security issues by state actors, particularly their initiatives, have resulted in legislative instruments that impinge upon the civil liberties of many citizens and have the potential to restrict the free flow of information vital for civil society actors.

In Russia and abroad the information field is formed by various means (mass-media, information security, public policy. Modern information technology, including information security as an integral and vital part of society management tool can significantly change not only the structure of relations, but also the lifestyle of people, their way of thinking, the mechanisms of family functioning, social institutions, government, etc.

In many regards, information security technologies are deployed for the improvement of society and are used to protect important, sensitive information from unwanted disclosure, modification or fabrication. An example is the use of cryptographic software tools that are used to protect sensitive and potentially incriminating information gathered by human rights field workers and investigators.

When discussing Information Security and its impact upon society, it is important to understand that technical approaches are not defining part of computer security and all main vulnerabilities were often created by humans that are commonly interconnected with protected information resources as well as to the Internet (WLAN) when it has a risk to be damaged or hacked.

The key goal of my paper is to explore some basic theoretical aspects and principles of Information Security during its action in society such as:
- Confidentiality, Integrity and Availability
- Human Factor (HF) as one of the basic defining part of Information Security (IS) in sociotechnical systems (STS)
- Legal methods (laws, instructions, regulatory documents etc.)
- Technical approaches (e.g. cryptography, firewalls)

Thanks to the informatization process the modern society is included in the global information space, becoming a part of it and becomes dependent on from information technologies and resources.

This space connects the world together and makes all the state information interdependent. Receiving large amounts of data bearing the knowledge, people at the same time get a lot of global dangers related to information security (e.g. information warfare, information terrorism, etc.). For example, information weapons act primarily on the consciousness of the subjects in order to manipulate them. Such negative information influences on the consciousness of the subject and as a result it can lead to a change in his outlook and values reorientation. Therefore, the problem of information security should be deep enough comprehended.

Information security is inherently an ethically neutral technology. The manner in which this technology is deployed determines the effects on society. As national security concerns receive more and more priority from a range of state actors the potential effects of information security technology on society become broader. Governments in most societies are increasingly stressing the risks that terrorism presents to society. The danger of this emphasis is that governments effectively 'paint themselves into a corner' whereby they need to be seen taking actions to counter the terrorism threat that they themselves have helped to promote.

One way of publicly taking action is to introduce measures, which are presented as high-technology solutions to security problems, such as the deployment of facial 10 recognition biometrics to aid airport security. The decrease in civil liberties, as well as the false sense of security that can result from such deployments needs to be carefully examined to ascertain, on balance, whether society is actually losing the freedoms that governments are meant to be protecting.

Information influence becomes the main instrument of managing people (instead of the usual physical) to the economy (e.g. economic sanctions), trade (e.g. credit card transaction processing), advertisements (financial pyramids), the political struggle, affecting the psyche rights, especially of certain social groups (e.g., teenagers), etc.

Therefore, one of the main elements that affect the life of modern society and the interests of national, public and personal safety, is information security.

Internet information field is generated by mass-media, search engines and public policy, lending itself to effect retouching, just as during the reign of Joseph Stalin retouched photos of public enemies.

Let me introduce just one example from the book by David King, "The Commissar Vanishes: The Falsification of Photographs and Art in Stalin's Russia" (Metropolitan Books, New York, 1997).

Fig. 1 Voroshilov, Molotov, Stalin, and Yezhov in 1937

Fig. 2 Nikolai Yezhov was arrested in 1938 and was executed in 1940

Such things often happen in the modern Internet: disappearing scientific articles, photos, music, which acquired the status of a state as "undesirable content". In this case, society has to face information isolation like the Iron Curtain. There are four ways to solve the problem: the first is to refuse and ignore all information resources in general, the second is to accumulate information saving it prior to one's removal from public access, the third is to prevent censorship and prohibition sole resources through strict public control and the fourth is your personal solution.

It is important to understand that from the standpoint of national security policy, with its respect to the government, information integrity field should be carried out despite all democratic requirements. Although this factors limit the freedom of citizens, but it is a guarantee of national security, future modern society is provided by information security.

References:
1. https://www.gov.uk/service-manual/making-software/information-security.html
2. http://www.cscan.org/presentations/14-10-09-OpeyemiOre.pdf
3. Carey-Smith, Mark T. & May, Lauren J. (2006) The Impact of Information Security Technologies Upon Society (http://eprints.qut.edu.au/6082/1/6082.pdf)