Information Aspect of Energy Security

S. Levinzon

Kaluga Branch of the Baumann Moscow State Technical University, Kaluga, Russia svlev34@gmail.com

In general, the algorithm for assessing the information aspect of energy security is fairly simple and includes certain stages [1], i.e. it is necessary to define energy security for evaluation purposes, characterize the energy system vital elements, identify their vulnerabilities, and interpret the obtained results in relation to the set goals.

When determining energy security, one can start from the Energy Sustainability Index of the World Energy Council (WEC). This index is valuable in that it (one of a few) attempts to account for the differences in the stand on of countries- importers and exporters of energy and the level of their economic development. The breadth of its scope must be pointed out as well: for example, in 2013, it gave estimates for 129 countries.

The component "Energy security" of the WEC Index includes 6 indicators of equal importance: the ratio of energy production to energy consumption, diversification of electricity generation sources, losses in networks as a percentage of electricity generation, average annual growth rate of the of energy consumption to GDP ratio for 5 years. In 2013, for the "Energy security" component value of 9.92, Russia was ranked second in the world (after Canada). Currently, this value slightly decreased [2].

The problem of energy security. According to the available forecasts, world energy consumption could increase by a third over the next 15 years, and by about 45% - in the coming 20 years [3]. Information security - protection of information and supporting infrastructure from accidental or deliberate natural

or artificial impacts, which can inflict unacceptable damage on subjects of information relations. Supporting infrastructure - systems of electricity, heat, water, and gas supply, air conditioning systems, etc., as well as maintenance personnel. Unacceptable damage - damage which cannot be neglected.

Energy security is characterized by three main factors: the ability of the fuel and energy complex to ensure a sufficient supply of affordable and high-quality fuel and energy resources (FER); the ability of the economy (as an FER consumer system) to rationally (carefully) consume energy and, therefore, limit its demand. In [3], information terrorism is defined as a special form of violence, which is a deliberate and targeted data attack by a terrorist organization or individual terrorists or threat to use such an attack in order to force the government to fulfill political, economic, religious and other goals. This form of violence is accompanied by an emotional pressure on society to generate fear, panic, loss of confidence in the government and create political instability.

The term "information terrorism" is more general than "cyber-terrorism"; it encompasses the use of a variety of methods and means of information pressure on different aspects of human society (physical, information, cognitive, social) [4]. With that, it is possible to distinguish between the following main types: information-psychological terrorism – control of the media to spread disinformation, rumors, demonstrate the power of terrorist organizations; pressure on operators, developers, representatives of information and telecommunications systems through violence or threats of violence, bribery, etc.; information technology terrorism – damage to individual physical elements of the information environment of the state; interference generation, use of special programs to stimulate control systems destruction, or, on the contrary, external terrorist control of technical objects, biological and chemical means of destruction of the element base, etc.

For decades, the information security industry has evolved under the same scenario: as soon as a new virus appeared, developers immediately came up with an antivirus - in the endless pursuit of the hackers, in a hopeless attempt to get ahead of cybercriminals' thought. The time has come when the rules began to change: the new code encryption technology promises to make hackers' lives as hard as possible . Currently, the fight against hackers in many countries (especially in EU, USA, Asia and Russia) goes on with "varying success". Banking systems are constantly hacked; hackers get access to users' personal information; "compromising information" on political figures is published; local power systems are disrupted; materials of political parties are laid out in open access; and much more .

Neutralization of hackers (individuals and teams) occurs mostly in two directions: protective systems are constantly being improved, and hackers are identified, captured in various countries and subjected to punishments up to criminal prosecution. As the saying goes, the show is not over yet, the battle continues.

List of references

1. Левинзон С.В. Энергобезопасность. Вчера, сегодня, завтра. 400с.pdf.URL:https://monographies.ru/files/S.V.Levinzon.Jenergobezopasnost.pdf (12.09.2017).

2. Энергетический бюллетень № 28,сентябрь 2015. URL: http://ac.gov.ru/files/publication/a/6397.pdf (14.09.2017).

3.Баранов Н.А.Проблемы национальной безопасности и пути их разрешения. URL: http://nicbar.ru/nazbez_lekzia2.htm (03.09.2017).

4. Информационные войны и информационный терроризм. URL: http://www.ereading.club/chapter.php/1013635/74/Chrezvychaynye_situacii_socialnogo_haraktera_i_zaschita_ot_nih.html (04.08.2017).