Control of social networks in the 21 century

Salomatina V.D., Chumakova A.V.

Tyumen State University, Tyumen, e-mail: vika2000.salomatina@yandex.ru

The social sites these days are gaining a lot of popularity with almost all of the educated youth using one or more of the social networking sites. They 'have played a crucial role in bridging boundaries and crossing the seas, bringing all people at a common platform where they can meet likeminded people, find old friends and communicate with each other.' [1; 89] The increased use of social networking sites has become an international phenomenon in the past several years. Through these websites everyone connect with 'their peers, share information, reinvent their personalities and showcase their social lives [5; 3]. Many people have internet on their phone and a touch of a button check their mails, their Facebook, movie times, their bank balances etc. Some people argue that the use of social sites in the workplace leads to better employee productivity such as higher morale and other argue that the use of social networking sites in the workplace regulate in loss of labour productivity due to time wasted at work (Wavecrest, 2006). In today's world Facebook, Twitter, Myspace are common websites for people to meet and make acquaintances.[4]

Of course, Internet is a very convenient and efficient source of information. It is 'is by far the most popular source of information and the preferred choice for news ahead of television, newspapers and radio' [2]

The main Internet - users contingent is the Youth Environment. Young people are active users of the global network receiving the lion's share of information from the Internet - space. The Internet surrounds them everywhere as they easily go into the global network with various gadgets and devices. An important factor in this case is the fact that the worldview of young people is still at the stage of development. Therefore the Internet with its spectrum of opinion and views, the prevalence of ideas of different meaning and content can present a real danger. This judgment is particularly true for those portals and Internet sources that are designed to spread the idea of extremist and terrorist shares.

Of particular concern is the use of existing information resources-the global Internet by international terrorism. In particular, terrorist groups increasingly use the latest information technologies and the Internet to disseminate propaganda and information exchange, to attract financial resources and to plan terrorist attacks.

Via the Internet criminals can arrange the place of terrorist attacks. Various Internet programs provide very wide opportunities for all Internet users without exception, providing open access to satellite imagery and maps of any terrain and thus allowing terrorists to plan more carefully their actions. Subsequently, many countries try to improve their legislation proposing new bills and making new laws to protect their people from threat connected with Internet.

Thus, on July 29, 2017, the President of the Russian Federation signed two federal laws that prohibit the anonymous use of online messenger applications and detail the procedure for blocking access to websites recognized by the Russian authorities as prohibited.

Federal Law No. 276-FZ of July 29, 2017, on Amendments to the Federal Law on Information, Information Technologies, and Information Protection came into force on November 1, 2017. This law 'prohibits owners of information and telecommunications networks and information resources (websites, website pages, information systems, and programs for computers and electronic equipment) to provide access to websites and information resources that are designated as "resources with restricted access" by the Federal Service for Supervision in the Field of Communications, Information Technology, and Mass Media (Roskomnadzor). The Law requires Roskomnadzor to create a national information database of online resources and services to which access is prohibited in Russia.' [3]

Federal Law No. 241-FZ of July 29, 2017 on Amendments to Articles 10(1) and 15(4) of the Federal Law on Information, Information Technology and Information Protection prevents the anonymous use of instant messaging online.

The ability of U.S. authorities to search for terrorist suspects through online surveillance is expanding. Such surveillance can be carried out using the Carnivore online surveillance system developed and used by the FBI, which allows tracking visits to Web pages and correspondents by electronic correspondence, in some cases If there are extraordinary circumstances-without a warrant issued by the court, but only with the approval of the prosecutor's office. In addition, providers, telephone companies or credit organizations are required to provide the state with information about the consumer of their services without a court order for the seizure, if the FBI claims that such information is necessary for Authorized investigation of international terrorism or covert intelligence activities, provided that such an investigation against a U.S. citizen is conducted only in view of his activities protected by the First Amendment to The U.S. Constitution (this amendment enshrines the freedom of religion and political freedoms of citizens: words, seals, associations, demonstrations and manifestations).

Thus, the American authorities have been given ample opportunities to "electronically" control and listen to telephone conversations both citizens of their country and foreigners, allowing them to collect a huge amount of information under Counter-terrorism and foreign intelligence.[6]

Based on the above, we can once again see that the problem of the spread of terrorism on the Internet grows every day. There are new ways of influencing and recruiting people, there is a huge number of services that are aimed at facilitating and destroying the boundaries of communication between people around the world. Unfortunately all these programmes are not used by terrorists for peaceful purposes.

In this regard, today it is necessary to make new laws and rules against the world threatterrorism in the Internet. It is necessary to unify national legislation in the sphere of protection of critical infrastructure from cyber terrorism.

References:

- 1 Fiona Homer. The perfect handover: an innovative approach to report the impact of a combined handover process on inpatient wards in the United Kingdom a quasi-experimental study. // 26th World Nursing Education Conference 2017. Available at: <a href="https://books.google.ru/books?id="https://books.google.ru/books.google.ru/books?id="https://books.google.ru/boo
- $\underline{SytzgAhXQMJoKHcwECNkQ6AEwBXoECAkQAQ\#v=onepage\&q=bridging\%20boundaries\%20}\\ and \%20crossing\%20the\%20seas\&f=false$
- 2. Internet most popular information source: poll. // Available at: https://www.reuters.com/article/us-media-internet-life/internet-most-popular-information-source-poll-idUSTRE55G4XA20090617
- 3. Russia: New Legislation Restricts Anonymity of Internet Users. Available at: http://www.loc.gov/law/foreign-news/article/russia-new-legislation-restricts-anonymity-of-internet-users/
- 4. Social Media and Social Networking Sites. Available at: https://www.bartleby.com/essay/Social-Media-And-Social-Networking-Sites-F3F7GAT36YKW
- 5. Waleed Mugahed Al-Rahmi, Mohd Shahizan Othman The Impact of Social Media use on Academic Performance among university students: A Pilot Study // Journal of Information Systems Research and Innovation. Available at:
- $\underline{https://seminar.utmspace.edu.my/jisri/download/G_FinalPublished/Pub12_SocialMediaAcademicP}\\ \underline{erformance.pdf}$
 - 6. Carnivore Details Emerge. Available at: https://www.securityfocus.com/news/97