A SOFTWARE TOOL FOR INCREASING EFFECTIVENESS OF COUNTERING OF ANTI-UKRAINIAN PROPAGANDA ON INTERNET

Kolodiazhnyi I., Dorenskyi O.
Central Ukrainian National Technical University, Kropyvnytskyi

Significant progress and dissemination of information technology, the global nature of mass communication systems have led to the creation of a global information space that forces the world community, each state to navigate and adapt itself into the modern information environment quickly. In this context, the world community has realized that international information security is a problem, the solution of which significantly affects the existence of mankind. That is, with the development and spread of ICT into all spheres of vital importance, the issues of information security recognized in our country as one of the most important components of national security, as a multi-level problem of state information policy, become more significant. Persuasion methods got powerful development during the 20th century. Propaganda, which has a large arsenal of such methods, stimulates socio-political activity of citizens, showing them specific directions and tasks of activity, indicating the ways and means of solving the problems they are facing. According to the public information of the Security Service of Ukraine, hostile propaganda is actively implemented through social networks. Ukraine implemented an approach to resist propaganda in social networks, personal special economic and other restrictive measures (sanctions). The essence is to prohibit the Internet providers to provide an access to Russian-made Internet services: Vkontakte, Odnoklassniki, and many others. However, as practice shows, the approach to ensure the information security of the state proved ineffective. After all, the blocked websites are still among top 10 mostly visited sites in Ukraine, as users actively use VPN, Tor, Opera and other ways to bypass the lock [1].

The aim of the work is to increase the effectiveness of resistance of the separatism propaganda and anti-Ukrainian ideology that are spread on Internet by implementation and use the software of Tor entry nodes and servers of VPN providers blocking.

The main function of the developed software system is blocking of the Tor entry nodes, servers of VPN providers and sites with information about bypass of blocking. Blocking is done by blacklisting resources. The user is redirected to the local host every time he trying to access a forbidden resource [1-2].

The software is intended for use by Internet Service Providers. ISPs install the software on their servers. The requirements of using the software are minimal: employees must have a basic level of computer skills in order to create, delete and edit data in the database.

The software works like this. A web resource request is sent to the ISP server. The domain name request is accepted by the system and checks whether the domain name is present in the database. If the domain name is present in the

database, then the system returns a DNS response which contains a local server address by using an implemented DNS server.

The “blacklist” database contains illegal IP/URLs. GUI is provided for the working with database. The first thing to do is enter the password, if the password is entered correctly - the main menu is displayed, otherwise the message about the wrong password is displayed. The main menu has the functions to add a domain name and IP, search for a domain name, delete a domain name, upload the records, display the information about the developer.

The protection of the database is ensured by the block cipher DES, the basis of which is the Faustel scheme with corresponding parameters. The implementation of DES can be done in three steps: 1) the fixed initial IP permutation is applied to the input block; 2) 16 rounds are performed, which include operations to modify the input parameters; 3) the final permutation is applied to the result of the 16th round.

Thus, it is shown in the work that despite the introduction in Ukraine of the prohibition on Internet providers to provide an access to Internet users to Russian-made Internet services, which are means of spreading propaganda of separatism and anti-Ukrainian ideology, part Ukrainians are still using them, bypassing the blocking with VPN, Tor, etc. the way. Therefore, it is proposed the software tool that will prevent access to the forbidden web resources by blocking of the addresses of incoming Tor nodes and VPN provider servers. It will allow to increase the effectiveness of resistance of the separatism propaganda and anti-Ukrainian ideology on Internet, including social networks.

Developed software can be used not only in the context of hybrid warfare by providers, but also when necessary to restrict access to resources that are inappropriate in the workplace. For example, by private firms that can entrust the software installing to their administrators.

REFERENCES

1. Kolodiazhnyi I., Dorenskyi O. Increasing Effectiveness of Countering of the Separatism Propaganda and Anti-Ukrainian Ideology in Social Networks. Інформаційні технології в соціокультурній сфері, освіті та економіці : міжнар. наук.-практ. конф. студ. і молодих учених, 18–19 квіт. 2019 р., м. Київ : матеріали конф. Київ : КНУКіМ, 2019. С. 279-280. URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/8941/1/ITCKC_Kyiv_2019_279-280.pdf

2. Колодяжний І. О., Доренський О. П. Методологічні засади підвищення ефективності протидії антиукраїнській пропаганді в соціальних мережах. Інформаційні технології – 2019 : VI всеукр. наук.-практ. конф. молодих науковців, 16 трав. 2019 р., м. Київ / Київський університеті імені Бориса Грінченка. Київ, 2019. С. 53-54. URL: https://fitu.kubg.edu.ua/images/stories/Departments/kitmd/zbirnuk/zbirn_tez_materialiv_konf_IT_2019.pdf