

# METHODOLOGY OF COUNTERACTION OF SOCIAL ENGINEERING ON OBJECTS OF INFORMATION ACTIVITY

Lishchuk I., Sokolov V.

*Borys Grinchenko Kyiv University, Kyiv, Ukraine*

There are many sources of threats to enterprise information and cybersecurity. Enterprise personnel are always involved in the storage and processing of information. Therefore, it is important to consider the human factor as a real existing vulnerability in the information security of the enterprise.

Usually for the convenience of people, most public Wi-Fi networks are left open, making them a good place to conduct various attacks. This fact is what inspired this study.

The aim of the work is to prepare a reasonable method of raising the level of personnel's awareness in the issues of social engineering methods counteraction.

The scientific novelty of the work consists in the development of the method of the staff awareness management in the questions of counteraction to the methods of social engineering.

In the sphere of information security the term “social engineering” is used to describe the science and art of psychological manipulation. According to the statistics of Infowatch analytical center, 55% of losses related to information security violations caused by employees who were influenced by social engineers.

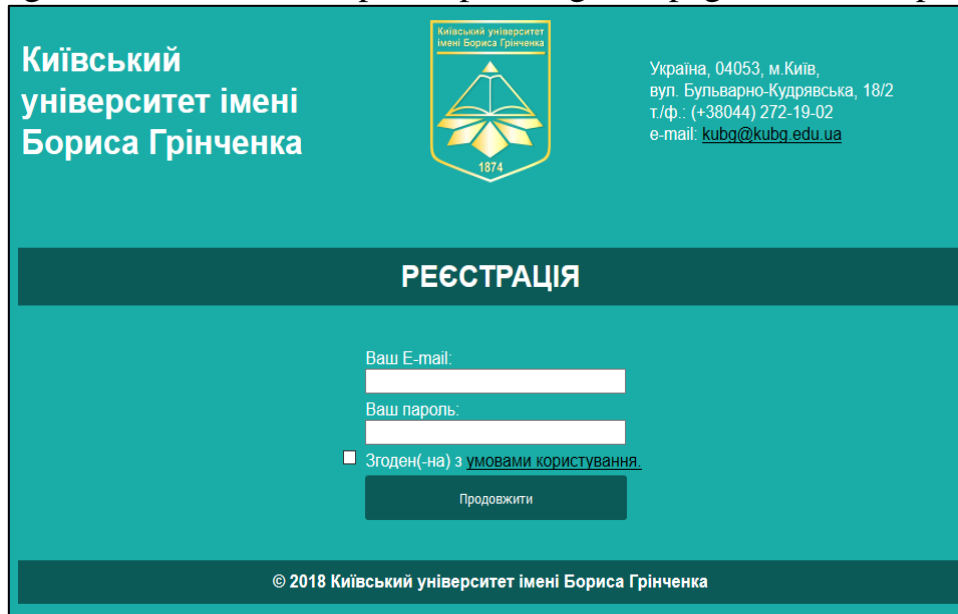
So, the following equipment was chosen for the test stand: Raspberry Pi 3 Model B, SanDisk MicroSDHC 16Gb Class 10 Trust PowerBank 10,000 mAh, Tp-Link TL-WN722N v3.



Three profiles of higher education institutions (HEIs) were selected as part of the experiment:

- Humanitarian (Boris Grinchenko Kyiv University, Kyiv).
- Technical (State University of Telecommunications, Kyiv);
- Mixed (National University “Lviv Polytechnic,” Lviv).

According to each of them, a separate phishing web page was developed.



Київський  
університет імені  
Бориса Грінченка

Київський університет  
імені Бориса Грінченка

Україна, 04053, м. Київ,  
вул. Бульварно-Кудрявська, 18/2  
т./ф.: (+38044) 272-19-02  
e-mail: [kubg@kubg.edu.ua](mailto:kubg@kubg.edu.ua)

РЕЄСТРАЦІЯ

Ваш E-mail:

Ваш пароль:

Згоден(-на) з [умовами користування](#).

Продовжити

© 2018 Київський університет імені Бориса Грінченка

Statistics of the ease with which users share their address and even passwords are shown in the figure 1. The trend shows an increase in the percentage of submitted personal data of humanitarian students, but still the trust in unknown open networks is high enough among students of technical universities. The high percentage of password input is due to the introduction of non-existent passwords.

Because of experiments, it is visible that awareness of user's even technical specialities is not enough; therefore, it is necessary to pay special attention to working out of techniques of increase of level of awareness of users and decrease in quantity of potential attacks to objects of information activity.

## REFERENCES

1. Sokolov, V. Y., Kurbanmuradov, D. M. (2018). "Method of Counteraction in Social Engineering on Information Activity Objectives." *Cybersecurity: Education, Science, Technique* 1: 6–16. <https://www.doi.org/10.28925/2663-4023.2018.1.616>.
2. Dashko, D. A., Meshkov, V. I. (Apr. 2013). "Social Engineering from the Point of View of Information Security," In V Ukrainian Conference "ITBtaZ," 1–2.
3. InfoWatch. (2017). "Modern Threats Emanating from Information Systems," 1–12.
4. Shatkovsky, M. O. (2015). "The Influence of Social Engineering on the Information Security of Organizations," 1–4.