**Haborets O. A.**
PhD, Associate Professor of the Department of Operational-search Activities and Information Security of
Donetsk State University of Internal Affairs,
Kropyvnytskyi, Ukraine
ORCID: 0000-0001-7791-6795
**Chernobrov V. M.**
Cadet of the Faculty of Training Specialists for Criminal Police Units,
Donetsk State University of Internal Affairs,
Kropyvnytskyi, Ukraine

# SOCIAL ENGINEERING AS A MEANS OF INFLUENCE ON PEOPLE CONSCIOUSNESS

Social engineering is the use of psychological manipulation techniques to influence people's behavior and beliefs. It is a tactic that has been used throughout history to manipulate and control individuals or groups, whether in the context of politics, marketing, or other fields.

One of the most important aspects of social engineering is the ability to influence people's consciousness. This can be done through various techniques, such as persuasion, coercion, deception, and manipulation. These techniques can be used to influence people's beliefs, attitudes, values, and behaviors, and ultimately shape their consciousness.

For example, political leaders may use social engineering to manipulate the public's perception of their policies or to persuade voters to support their agenda. Advertisers may use social engineering to influence consumer behavior by appealing to their emotions or creating a sense of urgency. Similarly, cult leaders may use social engineering to control their followers by creating a sense of dependence and loyalty.

One of the most powerful tools of social engineering is the use of technology, such as social media platforms, to disseminate propaganda and manipulate public opinion. These platforms are designed to exploit human psychology, by using algorithms that tailor content to individual preferences, and by creating echo chambers that reinforce existing beliefs and biases.

Social engineering methods are often used on the internet to manipulate individuals into divulging sensitive information or performing actions that benefit the attacker. The internet provides an ideal platform for social engineering, as it allows attackers to remain anonymous and reach a large audience.

One common social engineering method used on the internet is phishing. Phishing involves creating a fake website or email that appears to be from a legitimate source, such as a bank or social media platform. The attacker then tricks the victim into entering their login credentials or other sensitive information, which the attacker can use to access the victim's accounts or steal their identity.

Another social engineering method used on the internet is baiting. Baiting involves creating a fake file or download that appears to be valuable or interesting, such as a free software download or movie. When the victim downloads the file, it installs malware or other malicious software that can be used to steal information or control the victim's computer.

Social media platforms are also frequently used for social engineering. Attackers may create fake profiles or use social media to spread false information or propaganda. They may also use social media to gather information about their victims, such as their interests, friends, or location, which can be used to craft a more convincing attack.

To protect against social engineering on the internet, it is important to be vigilant and skeptical of requests for information or actions. Always verify the authenticity of websites or emails before entering sensitive information, and be cautious when downloading files or clicking on links. It is also important to keep software up to date and to use antivirus software to protect against malware and other threats. Additionally, be cautious about the information shared on social media, and limit the personal information that is publicly available.

It is important to be aware of the potential dangers of social engineering and to be vigilant against its manipulative tactics. This can be done by developing critical thinking skills, questioning sources of information, and seeking out diverse perspectives. By being aware of social engineering tactics, we can protect ourselves from manipulation and make informed decisions based on our own values and beliefs.