Таким чином, для запобігання та вирішення проблем в галузі кібербезпеки, необхідно постійно проводити діагностування систем шляхом проведення спеціальних тестів, використання спеціалізованого обладнання та залучення кваліфікованих фахівців, які зможуть усунути причини можливих вразливостей. Також важливо пам'ятати, що ми всі знаходимося в одному великому мережевому просторі, тому навіть звичайний співробітник або військовослужбовець може стати жертвою будь-якого вірусу, що може призвести до зараження на всіх рівнях. Тому, одним із ключових аспектів кібербезпеки є проведення навчань з працівниками з метою запобігання та протидії кібератакам.

Список використаних джерел:

1. Стратегія національної безпеки України, затверджена Указом Президента України від 12.02.2007 No105/2007в редакції Указу Президента України від 8.06.2012 року No 389/2012. [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/105/2007.

2. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 No 96.Офіційний вісник України. 2016. № 23.

3. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року. [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19.

4. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. / В. А. Ліпкан, Ю.Є. Максименко, В. М. Желіховський. Київ: КНТ, 2020. 280 с.

Shaets E.O.
Cadet of the Faculty of Training Specialists for Criminal Police Units, Donetsk State University of Internal Affairs

Haborets Olha Andriivna
PhD, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs

SOCIAL ENGINEERING AS A METHOD OF SHAPING PEOPLE'S CONSCIOUSNESS

Social engineering employs psychological manipulation techniques to shape behavior and beliefs, a tactic evident throughout history in various contexts like politics and marketing.

Central to social engineering is the capacity to influence consciousness, achieved through persuasion, coercion, deception, and manipulation. These methods impact beliefs, attitudes, values, and behaviors, molding consciousness itself. Political leaders might employ social engineering to sway public opinion or garner support for their policies, while advertisers may leverage it to sway consumer behavior by tapping into emotions or urgency. Similarly, cult leaders can use social engineering to foster dependence and loyalty among followers. Technology, notably social media, amplifies social engineering's reach, with platforms tailored to exploit human psychology through algorithmic content curation and the creation of echo chambers that reinforce existing beliefs and biases.

Social engineering techniques are frequently deployed online to coerce individuals into revealing confidential data or undertaking actions advantageous to the perpetrator. The internet serves as an optimal medium for social engineering due to its capacity to preserve anonymity and reach a broad audience. A prevalent online social engineering tactic is phishing, wherein perpetrators fabricate counterfeit websites or emails resembling authentic sources like banks or social media platforms. Subsequently, they deceive victims into disclosing login credentials or other confidential data, enabling access to the victim's accounts or identity theft.

Another technique of social engineering utilized on the internet is baiting, which entails creating a deceptive file or download masquerading as valuable or intriguing, such as a free software or movie download. Upon downloading, the victim unwittingly installs malware or other malicious software enabling the perpetrator to pilfer information or assume control of the victim's computer. Social media platforms are also frequent targets for social engineering endeavors. Perpetrators may fabricate fake profiles or disseminate false information or propaganda via social media. Furthermore, they may exploit social media to gather information about their targets, including their interests, connections, or whereabouts, to craft more convincing attacks.

To mitigate the risks of social engineering online, it is imperative to remain vigilant and skeptical of requests for information or actions. Always verify the legitimacy of websites or emails before divulging sensitive information, and exercise caution when downloading files or clicking on links. Keeping software updated and employing antivirus software can also safeguard against malware and other threats. Additionally, exercise discretion regarding information shared on social media and limit the personal information publicly accessible.

Awareness of the potential hazards of social engineering and maintaining vigilance against its manipulative tactics is crucial. This entails cultivating critical thinking skills, scrutinizing sources of information, and seeking diverse perspectives. By recognizing social engineering tactics, individuals can shield themselves from manipulation and make informed decisions aligned with their values and beliefs.