6. SpringerLink. Human factors in cybersecurity: An interdisciplinary review. – Режим доступу: https://link.springer.com/ Threatscape. The Human Factor in Cyber Security. – Режим доступу: https://www.threatscape.com/

7. The Guardian. Qantas cyberattack: staff error leads to data exposure. – Режим доступу: https://www.theguardian.com/

Yarotska Anastasiia Stanislavivna
Student of academic group 301_SPS,
Institute of Law and Psychology, NAIA

Scientific supervisor:
Pakrysh Oleksandr Yevheniiovych
Candidate of Technical Sciences,
Associate Professor, Associate Professor of the Department of Information Technologies, Institute of Law and Psychology, NAIA

PSYCHOLOGICAL TYPES OF CYBERCRIMINALS

In the modern world, where almost every person has easy access to the Internet, and it is not limited to a home desktop computer, new ways of illegal, criminal behavior are opening up, and therefore, with the advent of the Internet, cybercriminals have appeared in our lives. According to the definition of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", a cybercrime is a socially dangerous guilty act in cyberspace and/or with its use. A cybercriminal, accordingly, is a person who committed such a crime.

As each type of illegal behavior in cybercrime has a certain collective profile of the offender, I propose to examine it from several points of view: the general characteristics of the cybercriminal (who are these people and what controls them), psychological types of cybercriminals by motivation for committing crimes and by approaches to illegal activities in cyberspace. I chose to characterize psychological types by their type of activity.

The general profile of a cybercriminal begins with the same general criminal craving/desire to obtain a benefit that is impossible (or difficult) to obtain in a law-abiding way. However, by the nature of the diversity of cyberspace, these benefits are radically different. A cybercriminal is primarily attracted by anonymity, invisibility in an infinite number of Internet connoisseurs. As in the real world, a person who wants to commit a crime is attracted to remaining unexposed, and ultimately unpunished.

Messengers do not leave fingerprints in the conventional sense, and when committing a virtual crime, you do not have to look into the eyes of the people you are robbing, psychologically this aspect can have a calming effect on a potential criminal and lower the threshold forcommiting the crime. "No one will recognize me here", "They won't be able to find out who I am", and "They can't get me back", this is how I would summarize the main ideas when describing the choice process of cybercrime over another type of crime [1].

With technological development, forced authorization on popular sites, applications, and search engines is increasingly coming to the virtual world, and anonymity has become more difficult to maintain. To do this, the criminal needs at least an initial level of knowledge in information technology. Thanks to specialized browsers (such as Tor, for example) and software that can be customized (operating systems such as Linux, Ubuntu), a cybercriminal can still achieve maximum anonymity. Therefore, in order to engage in cybercrime, it is worth having a large amount of knowledge and technical capabilities. From a psychological point of view, a person who wants to commit a crime, seeks anonymity and achieves it – sends a fairly clear message: it can be assumed that a person is not very socially adapted to a certain level, or at least perceives society with detachment, has a fairly developed level of awareness of technology and has money driven motives.

According to the motivation for committing crimes in cyberspace, offenders can be divided into: scammers, identity thieves, cyberterrorists, stalkers, hacktivists and hobby hackers.

Scammers and identity thieves mainly operate with the desire to get monetary gain, in one way or another: scammers trick people for money, and identity thieves steal personal information and use it to steal money, or resell this information to data brokers. This type of cybercriminal is characterized primarily by selfishness, some degree of immorality, greed for power.

Cyberterrorists operate mainly with DDoS attacks, thanks to such massive attacks, it is possible to leave without information, for example, banks, government agencies, enterprises of any type, due to oversaturation and temporary shutdown of servers. Usually, during or after a massive DDoS attack on software, information remains in danger, and this is followed by data theft. Cyberterrorists usually do not work alone, as they are often sponsored by organizations or specific stakeholders. Psychologically, these are most likely very closed individuals or groups of people who are morally gray, and despite their prejudices, often work under the auspices of customers. If this is a group of cyberterrorists, then most likely their style of activity will converge with hacktivists.

Stalkers, like offline stalkers, are looking for information about a specific person or group of people, their goal is to collect information and directly monitor the activities of the object. Stalking and stalking often have a characteristic for it obsessive nature, sometimes sexually determined.

Hobby hackers are amateur enthusiasts who engage in cybercrime mainly not for reward, but to satisfy their interest or ego. For a hacker's hobby, it is not necessary to steal or break something, for them it is enough to know that this system can be hacked, and hack it. It is logical to expect that first of all this person will be self-centered, primarily love technology, and will orient first and foremost on their own individual goals in criminal acts.

Hacktivists (hackers-activists) use criminal methods to influence the state of events in political terms, achieve the termination of a service, or steal information for distribution to the public. Like ordinary activists, hacktivists tend to have a strong sense of justice, or its violation.

According to the main approaches to illegal activities in cyberspace, criminals can be described as white hats, black hats and gray hats.

"White hat" hackers are known as "ethical hackers". They have the same experience and knowledge as black hats, but organizations legally allow them to "hack" their systems.

White hats test security weaknesses and vulnerabilities in IT systems before black hats can exploit them. The white hats then patch up all the loopholes they have discovered. In this way, their proactive hacking prevents the actions of black hats or minimizes the damage that black hats can cause. A white hat in itself does not mean criminal activity, but can operate on illegal software, or not request acsess properly.

"Black hats" are dangerous, highly skilled and motivated by personal and financial gain. They hack with malicious intent and use their knowledge of programming languages, network architecture, and network protocols.

Black hats illegally infiltrate networks to compromise or stop an organization entirely. They hack into accounts to delete, modify, or destroy sensitive data. They also organize small and large-scale phishing attacks and other cybercrimes.

"Gray hats" border between black hats and white hats. While their motives are usually good, they still engage in technically illegal hacks like black hats do.

For example, a gray hat sees that a bank has just updated an app. It can intentionally (but illegally) hack into a system to find potentially vulnerable spots.

Instead of committing a hack, gray hats alert system administrators to flaws so that they can be fixed before the black hat takes advantage.

White, black, and gray hats can be characterized, respectively, by the desire to do good, evil, or something in between [2].

In terms of personality profile, Black Hats are usually highly intelligent and technically gifted. Studies often indicate that they may exhibit traits associated with the "Dark Triad" (Manipulative, Psychopathy), as well as a high propensity for risk and thrill-seeking. Their potential victims range from ordinary citizens with valuable data to large corporations, financial institutions, and government organizations that have weaknesses in their cyber defenses [3].

Cybercrime is evolving due to a combination of several key factors: high financial profitability, the rapid development of technology and the growth of computerization of society, as well as the low level of awareness of many users.

References:

1. Marleen Weulen Kranenbarg, Jean-Louis van Gelder, Ard J. Barends, Reinout E. de Vries. 2023. “Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets.” // Computers in Human Behavior. Volume 140. March 2023. https://doi.org/10.1016/j.chb.2022.107576 .

2. Межа між кіберзлочинністю та етичним хакінгом — 15 типів хакерів, які вам потрібно знати у 2023 році [Electronic resource]. URL: https://10guards.com/ua/blog/2023/06/20/the-thin-line-between-cybercrime-and-ethical-hacking-the-15-types-of-hackers-you-need-to-know-in-2023/ (date of application 10.10.2025).

3. Truong Jack Luu, Binny M. Samuel, Michael Jones, J.C. Barnes. 2025. “Exploring how the Dark Triad shapes cybercrime responses” // Personality and Individual Differences. Volume 244. October 2025. https://doi.org/10.1016/j.paid.2025.113250 .

Жицька Валерія Олегівна
Студентка н.гр. 117 СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

СТАН ТА ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

В наш час особливо, під час воєнного стану в Україні, дуже важливим є кібербезпека громадян і країни в цілому. Тому в роботі було розглянуто деякі проблеми кібербезпеки в Україні і шляхи їх усунення. Було проаналізовано проблеми в процесі створення безпечного кіберпростору в Україні, встановлено, що одним із можливих шляхів до створення безпечного кіберпростору є розвиток відповідної освіти в Україні.