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

THE PROBLEM OF APPLICATION OF PROFILING IN CYBER POLICE ACTIVITIES

Profiling in cyber police activities refers to the process of analyzing large amounts of data to identify patterns and characteristics that are indicative of criminal behavior or cyber threats. This information is then used to create a profile of potential suspects or threats, which can help law enforcement agencies to focus their investigations and resources more effectively.

However, the use of profiling in cyber police activities raises a number of ethical and legal concerns, particularly in relation to privacy and data protection. One of the main concerns is the potential for profiling to result in unjustified discrimination against certain groups, such as racial or ethnic minorities. This is because profiling often relies on identifying certain characteristics that are associated with criminal behavior, and these characteristics may be disproportionately present in certain groups.hat profiling is used ethically and effectively.

Another concern is the accuracy of profiling techniques, particularly when it comes to predicting future criminal behavior. Some critics argue that profiling can be unreliable and may result in false positives, where innocent people are wrongly identified as potential suspects. This can lead to unwarranted surveillance or even arrest, which can have serious consequences for the individuals involved.

There are also concerns around the transparency of profiling techniques, and the potential for these methods to be abused or used for political purposes. It is important for law enforcement agencies to be open and transparent about the profiling techniques they use, and to ensure that they are subject to appropriate oversight and accountability measures.

There are a number of different types of profiling techniques that may be used in cyber police activities. These include:

Behavioral profiling: This involves analyzing patterns of behavior or activity to identify potential threats or suspects. For example, law enforcement agencies may analyze patterns of online activity to identify individuals who are engaging in criminal behavior or who may be planning to commit a cyber attack.

Psychological profiling: This involves analyzing personality traits and other psychological characteristics to identify potential threats or suspects. This can be particularly useful in cases where the perpetrator of a cyber attack may be difficult to identify, such as in cases of anonymous online threats.

Demographic profiling: This involves analyzing demographic data, such as age, gender, or ethnicity, to identify potential threats or suspects. However, this type of profiling is controversial due to concerns around discrimination and bias.

While profiling can be a useful tool for cyber police activities, there are a number of ethical and legal concerns that must be taken into account. These include concerns around privacyand data protection, as well as concerns around discrimination and bias.

In order to address these concerns, law enforcement agencies must ensure that they are transparent about the profiling techniques they use, and that these techniques are subject to appropriate oversight and accountability measures. They must also ensure that they are collecting and analyzing data in a manner that is consistent with relevant privacy and data protection laws and regulations.

Overall, while profiling can be a valuable tool for cyber police activities, it must be used in a manner that is consistent with ethical and legal standards, and that respects the rights and privacy of individuals.

Haborets Olha Andriivna
PhD, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs
Chernobrov Violetta Volodymyrivna
cadet of the faculty of training specialists for criminal police units of Donetsk State University of Internal Affairs

THE USE OF AUTOMATED INFORMATION SYSTEMS IN OPERATIONAL AND INVESTIGATIVE ACTIVITIES

Automated information systems have become increasingly prevalent in operational and investigative activities conducted by law enforcement agencies, intelligence services, and other government bodies. These systems enable the efficient and effective collection, processing, and analysis of large volumes of data, which can be used to inform operational strategies and support investigations.

Automated information systems (AIS) are computer-based tools that can store, process, and transmit data in a way that improves the efficiency and effectiveness of operational and investigative activities.

In operational activities, AIS can be used to support tasks such as data entry, record keeping, report generation, and communication. For example, in law enforcement, AIS can be used to manage criminal databases, track incidents, and issue alerts to officers in the field. In emergency services, AIS can be used to manage dispatch and track resources. In healthcare, AIS can be used to manage patient records and schedule appointments.

In investigative activities, AIS can be used to support tasks such as data analysis, evidence collection, and case management. For example, in law enforcement, AIS can be used to search databases for information on suspects, analyze patterns in crime data, and manage evidence. In healthcare, AIS can be used to track outbreaks and analyze medical records for evidence of fraud or abuse.

The use of AIS in operational and investigative activities has several benefits, including increased efficiency, accuracy, and accessibility of information. However, it is important to ensure that the systems are secure and that access to sensitive