

Макаринська Анна Вадимівна

курсантка 1-го курсу факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ, рядова поліції

Лунгол Ольга Миколаївна

доцентка кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ, кандидатка педагогічних наук

MODERN DIGITAL TECHNOLOGIES IN CRIMINAL ANALYSIS

Modern digital technologies are increasingly being used in criminal analysis to help law enforcement agencies investigate and solve crimes. Here are some of the key technologies used in this field:

1. **Big Data Analytics.** Big data analytics tools can help process vast amounts of data, such as social media activity, CCTV footage, and mobile phone records, to identify patterns and connections that may be relevant to a criminal investigation.

2. **Artificial Intelligence (AI).** AI-powered tools can help law enforcement agencies analyze data and detect patterns that would be difficult or impossible to detect with traditional methods. For example, AI algorithms can be used to analyze crime scenes and identify potential suspects based on factors such as physical characteristics and behavioral patterns.

3. **Digital Forensics.** It involves the collection and analysis of digital data, such as computer hard drives and mobile phone records, to uncover evidence that may be relevant to a criminal investigation.

4. **Geographic Information Systems.** GIS technology can be used to map crime data and identify patterns and trends in criminal activity. This information can be used to inform law enforcement strategies and allocate resources more effectively.

5. **Facial Recognition.** This technology can be used to identify suspects in CCTV footage and other images, helping law enforcement agencies to track and apprehend criminals more effectively.

6. **Predictive Policing.** Uses data analysis and machine learning algorithms to identify areas and times where crime is likely to occur, allowing law enforcement agencies to allocate resources more effectively and prevent crime before it happens.

Big Data Analytics is a key technology used in criminal analysis to process large amounts of data that can help investigators identify patterns and connections that may be relevant to a criminal investigation. Criminal activities generate massive amounts of data, including CCTV footage, mobile phone records, social media activity, financial transactions, and more. This data can be analyzed to identify potential suspects, predict future criminal activity, and aid in the investigation and prosecution of criminal cases.

The process of big data analytics in criminal analysis involves several steps, including data collection, data processing, data analysis, and visualization. The first step is to collect the relevant data, which can come from a variety of sources, such as

crime reports, witness statements, and surveillance footage. This data is then processed to remove any irrelevant information and to convert it into a format that can be easily analyzed.

Once the data has been processed, the next step is to analyze it using various statistical and machine learning techniques. These techniques can be used to identify patterns and connections in the data, such as links between suspects, times and locations of criminal activity, and more. For example, data analysis may reveal that a group of suspects frequently communicates with each other through a particular social media platform or that a particular location is more likely to be targeted by burglars during certain times of the day.

Visualization is also an important aspect of big data analytics in criminal analysis. Visualizing the data can help investigators to identify patterns and connections more easily and to communicate their findings to others more effectively. This can include using charts, graphs, and other visual representations of the data.

One of the benefits of big data analytics in criminal analysis is that it can help law enforcement agencies to identify potential suspects more quickly and accurately. For example, data analysis may reveal that a particular vehicle was present at the scene of a crime, which can be used to identify the owner of the vehicle and potentially link them to the crime. Big data analytics can also be used to predict future criminal activity, allowing law enforcement agencies to allocate resources more effectively and prevent crime before it occurs.

However, there are also concerns about the use of big data analytics in criminal analysis, particularly around privacy and data security. It is important that law enforcement agencies are transparent about how they are collecting and using data and that appropriate safeguards are in place to protect the privacy of individuals. Overall, big data analytics is a powerful tool for criminal analysis, but it must be used responsibly and ethically to ensure that it does not infringe on individual rights or perpetuate biases.

Digital forensics is an important technology used in criminal analysis to investigate and analyze digital data that may be relevant to a criminal investigation. Digital data can include electronic documents, emails, social media activity, computer hard drives, mobile phone records, and more. Digital forensics can help investigators uncover evidence that may be crucial to solving a crime or prosecuting a suspect.

The process of digital forensics in criminal analysis typically involves several steps, including data collection, analysis, and reporting. The first step is to collect the digital data that may be relevant to the investigation. This can include seizing electronic devices, such as computers or mobile phones, and creating a forensic image of the device to preserve the original data. The forensic image is a copy of the device's contents that is analyzed and searched for evidence while preserving the original data.

Once the digital data has been collected, the next step is to analyze it. This can involve using specialized software tools and techniques to recover deleted data, analyze internet activity, trace communication between individuals, and more. Digital forensics can also help identify potential sources of digital evidence that may be relevant to the investigation. For example, analyzing a suspect's mobile phone may reveal GPS data that can be used to track their movements or communications with other individuals

that may have been involved in the crime.

The final step in the process of digital forensics in criminal analysis is to report the findings to the appropriate authorities. This may involve creating a detailed report of the digital evidence that has been uncovered and presenting it to law enforcement agencies or the court. The report may also include expert testimony from digital forensics analysts who can explain the techniques used to analyze the data and the conclusions that were drawn from it.

Digital forensics is a powerful technology that can help investigators to uncover important evidence in criminal investigations. It can also be used to support the prosecution of suspects by providing digital evidence that can be used in court. However, it is important that digital forensics is used ethically and responsibly, and that appropriate safeguards are in place to protect the privacy of individuals. Additionally, digital forensics experts must be properly trained and qualified to ensure that the evidence they uncover is accurate and reliable.

Overall, these digital technologies are making a significant impact in the field of criminal analysis, helping law enforcement agencies to work more effectively and efficiently to solve crimes and protect the public.

Список використаних джерел

1. Schoppa C. 3 Ways AI Technology Helps Solve Crime. AI Time Journal. URL: <https://www.aitimejournal.com/how-ai-technology-helps-solve-crime/> (Дата звернення: 25.03.2023).

2. Garfinkel S. L. Digital Forensics. American Scientist. URL: <https://www.americanscientist.org/article/digital-forensics> (Дата звернення: 27.03.2023).

3. Samanidou V. Current Challenges and Future Research Areas for Digital Forensic Investigation. Journal of Forensic Toxicology & Pharmacology. Vol: 10 Issue: 4. 2021. Pp. 125 – 136.

4. Rafay A. Investigation and recovery of materials by Digital forensics. Journal of Computer Engineering & Information Technology. 10:4 DOI: 10.37532/jceit.2021.10 (4).265.

5. Criminal Justice. The growing role of technology in the Criminal Justice field. 2018. URL: <https://www.purdueglobal.edu/blog/criminal-justice/growing-role-technology-criminal-justice/> (Дата звернення: 25.03.2023).