

Чайківський І.

аспірант,

Західноукраїнський національний університет,

Логін В.С.

студент ПД-31 юридичного факультету

Західноукраїнський національний університет

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ ДЛЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

У сучасному світі інформаційні технології відіграють ключову роль не лише в повсякденному житті, а й у сфері забезпечення національної безпеки. З розвитком цифрових технологій стрімко зростає і кількість кіберзлочинів, що створює нові виклики для органів, відповідальних за правоохоронну діяльність.

Кіберзлочинність охоплює широкий спектр правопорушень: від несанкціонованого втручання в роботу комп'ютерних систем до поширення шкідливого програмного забезпечення, фінансового шахрайства, торгівлі людьми та дитячої порнографії через мережу Інтернет. Згідно з даними Європолу (2024), кіберзлочинність визнана однією з головних загроз для безпеки громадян ЄС.

Аналогічні висновки містяться у звітах ООН та Інтерполу. В Україні, згідно з аналітикою Департаменту кіберполіції Національної поліції України, за 2023 рік кількість зареєстрованих кіберзлочинів зросла на 18% у порівнянні з попереднім роком. Така динаміка вимагає від правоохоронців не лише постійного вдосконалення технічного арсеналу, але й підвищення рівня кваліфікації персоналу.

Одним з основних інструментів протидії кіберзлочинності є впровадження автоматизованих систем аналізу великих масивів даних,

використання штучного інтелекту для ідентифікації кіберзагроз та формування баз підозрілої активності. У сфері цифрової криміналістики активно застосовуються технології блокчейн-трасування, цифрового збереження доказів, а також спеціалізоване програмне забезпечення (наприклад, EnCase, FTK, Autopsy).

Однак, виникають і значні виклики: правове регулювання таких технологій часто не встигає за їх розвитком, а на міжнародному рівні відсутній єдиний підхід до кваліфікації та розслідування кіберзлочинів. Крім технічних, актуальними залишаються і кадрові проблеми. В умовах постійної цифровізації суспільства правоохоронні органи потребують фахівців з глибокими знаннями в галузі інформаційних технологій, цифрової безпеки, аналізу даних та криптографії. Формування міжвідомчої співпраці між поліцією, СБУ, кібердепартаментом, судовими експертами та приватним сектором стає ключовим у забезпеченні ефективної відповіді на кіберзлочини. Науковий і практичний інтерес становить також проблема доказування у кіберпросторі.

Належне документування, фіксація та збереження цифрових слідів — це складне завдання, що потребує спеціальних процедур та засобів, аби забезпечити допустимість доказів у суді. Отже, розвиток інформаційних технологій створює як нові інструменти для правоохоронців, так і нові сфери ризику.

Ефективна протидія кіберзлочинності можлива лише за умови комплексного підходу: вдосконалення нормативно правової бази, підвищення рівня технічного забезпечення, професійної підготовки кадрів та міжнародного співробітництва.

У цьому контексті правоохоронна діяльність трансформується з реактивної у проактивну, зосереджену на попередженні та профілактиці цифрових загроз.

Список використаної літератури:

1. Європол. (2024). *Internet Organised Crime Threat Assessment 2024* (IOCTA 2024).
2. Департамент кіберполіції Національної поліції України. (2023). Аналітичний звіт про стан кіберзлочинності в Україні. Київ.
3. Chertoff, M., & Simon, T. (2016). The Impact of the Dark Web on Internet Governance and Cyber Security. Global Commission on Internet Governance.
4. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.
5. Al-Khouri, A. M. (2012). Combating Cybercrime: A New Challenge for Law Enforcement Agencies. International Journal of Law and Information Technology, 20(1), 59–77.
6. United Nations Office on Drugs and Crime (UNODC). (2023). Comprehensive Study on Cybercrime.
7. Raghavan, S. (2020). Artificial Intelligence and Law Enforcement: Opportunities and Challenges. Journal of Cybersecurity Research, 5(2), 45-60.
8. Інтерпол. (2023). Annual Cybercrime Report 2023.