solve serious crimes. Improving the research system directly depends on the future of all of us.

Список використаних джерел

1. Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці : матеріали міжнар. «круглого столу» (Харків, 12 груд. 2019 р.) / редкол.: В. Ю. Шепітько (голов. ред.), В. А. Журавель, В. М. Шевчук, Г. К. Авдєєва. Х. : Право, 2019. 164 с.

2. Sampson B. Case Study – The Forensic Analysis of a 3D Printed Firearm. AFTE 49th Annual Training Seminar: Conference proceedings, Charelston, WV, USA, June 3–8, 2018, pp. 48.

Кукса Ю., здобувач ступеня вищої освіти Національної академії внутрішніх справ
Керівник з мови: ***Могилевська В.***

INFORMATION SECURITY IN INDIA

Cyber security is concerned with making cyberspace safe from threats, namely cyber-threats. The notion of "cyber-threats" is rather vague and implies the malicious use of information and communication technologies (ICT) either as a target or as a tool by a wide range of malevolent actors. At the present stage, Cyber security has become an integral aspect of national security. Moreover, its area of influence extends far beyond military domains to cover all aspects of a nation's governance, economy and welfare [1].

There are about 1.5 billion people in India and almost everyone uses the Internet for all their needs, ranging from shopping to banking, studying to storing data, cyber crimes have also increased in proportion to usage. Currently, the Information Act, 2000 is the primary law for dealing with cybercrime and digital commerce in the country. The Act was first formulated in 2000, and then was revised in 2008 and came into force a year late. The Information Technology (Amendment) Bill, 2008 amended a number of sections that were related to digital data, electronic devices and cybercrimes.

In the Information Technology Amendment Act, 2008, cybersecurity is exercised under sections 43 (data protection), 66 (hacking), 66A (measures against sending offensive messages), 66B punishment for illegally possessing stolen computer resources or communication devices), 67(protection against unauthorised access to data), 69 (cyberterrorism), 70 (securing access or attempting to secure access to a protected system) and 72 (privacy and confidentiality) among others.

The National Technical Research Organisation is the main agency designed to protect national critical infrastructure and to handle all the cybersecurity incidents in critical sectors of the country. Additionally, the

Indian Computer Emergency Response Team (CERT-In) is responsible for incident responses including analysis, forecasts and alerts on cybersecurity issues and breaches [3].

The Indian military, central police organizations, law enforcement agencies and others are deficient in manpower, for software and hardware aspects integral to this field. Moreover, there is a growing demand for professionals in Artificial Intelligence (AI), BlockChain Technology (BCT), Internet of Things (IoT) and Machine Learning (ML). According to several estimates there is a need for at least three million cybersecurity professionals today. India doesn't have the 'active cyber defence' like the EU's General Data Protection Regulation (GDPR) or US' Clarifying Lawful Overseas Use of Data (CLOUD) Act.

Unlike the US, Singapore, and the UK where there is a single umbrella organisation dealing in cybersecurity, India has several central bodies that deal with cyber issues, and each has a different reporting structure. Further, each state government has its own Cyber emergency Response Team (CERT).[1] India lacks indigenisation in hardware as well as software cybersecurity tools. This makes India's cyberspace vulnerable to cyberattacks motivated by state and non-state actors.

Challenges such as growing Chinese influence in Indian telecom space, social media is becoming a powerful tool for dissemination of "information" making it difficult to differentiate fact from fake news. [2]

National Security Imperative: The change in military doctrines favouring the need to raise cyber commands reflects a shift in strategies, which include building deterrence in cyberspace. The need for a competent cyber security infrastructure as part of national security was first emphasized by the Kargil Review Committee 1999. Increasing Importance of Digital Economy: The digital economy today comprises 14-15% of India's total economy, and is targeted to reach 20% by 2024.

Added Complexity: With more inclusion of artificial intelligence (AI), machine learning (ML), data analytics, cloud computing and Internet of Things (IoT), cyberspace will become a complex domain, giving rise to issues of a techno-legal nature. Data is referred to as the currency of the 21st century and due to its bulk creation owing to India's population, several international companies (Google, Amazon etc.) are trying to have access to it. Given this there are issues related to data sovereignty, data localisation, internet governance, etc. Thus, there is a need to build strong cyber security architecture.[1] Given all the shortcomings, Prime Minister Narendra Modi this summer proposed to prepare a draft National Cyber Security Strategy 2020, which provides for the creation of secure cyberspace in India.

New challenges include data protection/privacy, law enforcement in evolving cyberspace, access to data stored overseas, misuse of social media platforms, international cooperation on cybercrime & cyber terrorism, and so on [4].

Список використаних джерел

1. «Cyber Security Framework In India», 2020. URL: https://www.drishtiias.com/daily-updates/daily-news-editorials/cyber-security-framework-in-india.
2. «Cyber-security Challenges in India», 2019. URL: https://www.jigsawacademy.com/cyber-security-challenges-in-india/.
3. «The current state of cyber security in India», 2018. URL: https://opengovasia.com/the-current-state-of-cyber-security-in-india/.
4. «Why India needs a strong cybersecurity policy soon», 2020. URL: https://www.expresscomputer.in/security/why-india-needs-a-strong-cybersecurity-policy-soon/62440/.

Левковець А., здобувач ступеня вищої освіти
Національної академії внутрішніх справ
Консультант з мови: ***Лопутько О.***

PROBLEMATIC ISSUES OF DETERMINING MISCONDUCT IN THE CRIMINAL LAW OF UKRAINE

The impetus for fruitful work on the reform of criminal and administrative-tort legislation was initiated by the Concept of reforming the criminal justice of Ukraine, approved by Presidential Decree of April 8, 2008 No. 311/2008, which among other things proposed to humanize criminal legislation defendants), to limit the scope of imprisonment sentences, replacing them with, for example, penalties. Divide criminal offenses into crimes and criminal offenses. One of the directions of introduction of the Institute of Criminal Offenses is the exclusion from the system of legal responsibility of administrative responsibility for the act or omission, which infringes on public order, property, rights and freedoms of citizens, established the procedure of administration and enforcement of such offenses as criminal offenses in the law on criminal liability. But such a path is unacceptable in advance because of the even greater criminalization of both the law and society as a whole [1].

On April 24, 2019, the Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on Simplifying Pre-trial Investigation of Certain Categories of Criminal Offenses" was published in the Voice of Ukraine newspaper. The relevant Law comes into force on January 1, 2020. The most fundamental changes to the criminal law are the introduction of a criminal misdemeanour, which can be punished by a fine of not more than three thousand tax-free minimum incomes, or other punishment unrelated to imprisonment. It is also envisaged to pay off the criminal record immediately after serving the sentence that committed the crime. The imposition of responsibility for the offense led to a change in the classification of crimes according to the degree of gravity (Article 12), since in fact the offenses under the new Law refer to crimes of small gravity. In turn, crimes by severity will be divided into non-serious, serious and