development, so far in cases of different categories addresses the institution of jurors, which already exists over a hundred years. It is the jurors who decide the question of the guilt of certain persons, and it is they who, first of all, need to prove it [2].

Thus, the process of reforming the criminal procedure in Great Britain significantly affected the principles of proof that, along with the basic principles, include special, inherent only British criminal procedure, traits. However, due to the growth and complication of the mechanisms of organized crime, British forensic scientists are in dire need of data extraction principles from the mass of precedents and detailed scientific analysis each of them, in order to determine the focus of the entire criminal process in the framework of the investigation of organized criminal activity.

Moreover, in addition to the already developed theories and conclusions, scientists insist on the fact that the British scientific community is facing an acute the need to highlight and new principles and mechanisms of the process evidence that could respond quickly and effectively to difficulties arising during the investigation of an organized criminal activity, as well as serve to establish objective truth on business.

Список використаних джерел

1. Gunn M., Bailey S.H. Smith and Bailey on the Modern English Legal System, Oxford, 2012. C. 123–125.

2. Jacobs A., Masset A. Manual of Penal Proceeding. London, 2010. C. 67.

Ряба А., курсант Національної академії внутрішніх справ
Консультант з мови: *Богуцький В.*

TERRORIST INCITEMENT ON THE INTERNET

The internet is an astoundingly robust and dynamic instrument for all manner of communications. It is a platform for an array of webpages, blogs, chatrooms, virtual groups, news media, political forums, advertisement options, cybersleuth sites, revenge spaces, shaming discussion groups, incitement networks, and much more. While many pages on the internet are devoted to civil discourse, others are dedicated to calumnious activities. Along with newspapers and university websites, there are others engaged in cybershaming1 and cyberbullying [1].

Of even greater social, political, and cultural consequence is the slew of websites committed to the spread of hate against various groups, and in its darkest crevasses are terrorist websites dedicated to inciting violence, recruiting like-minded individuals, and indoctrinating others on the use of political, religious, and otherwise ideological violence. Terrorist speech on the internet poses a threat worldwide. The realm of communications has vastly expanded the delivery of constructive and destructive information. Groups who seek to alter governments' policies and religious practices through havoc, violence, and intimidation are among those who exploit the

cross-border nature of internet protocols and electromagnetic packets. In addition to open propaganda on forums such as YouTube and Facebook, terrorists have increasingly exploited "darknets" to obfuscate and anonymize their activities through networks like Tor, I2P, and Freenet [2]. While all of these are benign tools useful for confidential interactions, privacy, and other legitimate purposes, international criminals-terrorists, counterfeiters, drug dealers, and arms dealers among them – exploit these tools for nefarious purposes.

Terrorist organizations' increasingly diverse use of digital devices vastly expands their reach beyond the scope of traditional modes of communication-conversations, pamphlets, or couriers. The challenge facing government agencies and thinktanks is how to formulate policies, statutes, standards, and regulations for digital platforms that are likely to safeguard the public, while maintaining the constitutional standards of protected speech and privacy.

The internet differs in part from traditional communications because of the great distances that often exist between online speakers and their audiences. Rarely will a statement posted on the internet present an imminent threat of harm. However, traditional spatial and temporal considerations of imminence are insufficient for policy-makers to address internet-based terrorist incitement. Online speech likely will not present any clear or present danger-except in the rare circumstance in which the target of inciteful comments is immediately proximate to the speaker, as if, for instance, an inflammatory message was sent to someone in the immediate vicinity of the sender. Many terrorist threats, calls for recruitment, and virtual meetings are made from remote locations, often from countries other than the location of the audience. Even threats to life and physical well-being might be made to instigate others to take action at some ambiguously designated opportune time.

However, internet companies regularly fail to monitor their communication networks. Reasons they assert for this failure include a robust protection of free speech, the need for fast-paced innovation, the ambiguity of the meaning of hate speech, a commitment to avoid censorship, and the sheer volume of digital information streamed on social networks. A considerable part of this reasoning is fueled by partisan economic interests aimed to increase profits and minimize expenses.

Yet terrorists do not simply speak in symbolic terms but aim to illicit action and trauma. Terror speech seeks to terrorize listeners and to induce criminal conduct. To deal with these threats, a model is needed to deal with hybrid speech. That model has three qualifications: First, the speaker must call for criminal, physical violence.96 Second, the intended victim must be aware of the threat. Lastly, the threat must be real, not abstract. If these are met, government would be allowed to suppress the nonspeech, coercive terror.

Список використаних джерел

1. Alison Virginia King Constitutionality of Cyberbullying Laws : Keeping the Online Playground Safe for Both Teens and Free Speech. URL:

https://www.researchgate.net/publication/291154413 (last visited Oct. 27, 2020).

2. The Internet Organised Crime Threat Assessment (IOCTA) 2016. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (last visited Oct. 27, 2020).

Савчук А., курсант Національної академії внутрішніх справ
Консультант з мови: ***Лопутько О.***

MODERN MECHANISMS FOR ENSURING INFORMATION SECURITY (FOREIGN EXPERIENCE)

There is a widespread belief among the scientific community that the United States is a leader in information security.

The United States is an example of an established democracy in which a high level of cooperation between civil society and government is an integral attribute of socio-political relations. As already mentioned, the trend of involving non-governmental institutions in management and organizational processes is also present in the information security sector. It can be stated that such steps are one of the defining directions of the US government's security policy. Regulations governing information security in the United States include the National Security Act, the Information Security Management Act, and the Cybersecurity Research and Development Act, and the Freedom of Information Act. Analysing the US legislation in the field of information security, it can be stated that special emphasis is placed on the involvement of non-governmental actors and cooperation with civil society institutions. At the same time, American lawmakers pay special attention to the use of advisory bodies [1].

In general, the main US programs and strategic documents on information security, as well as regulations are characterized by one unifying factor: they all argue that the state in modern conditions is not able to withstand all types of threats in the information sphere, and therefore needs cooperation. both at the international level (with other states) and at the non-state level (with civil society institutions). In particular, one of the main normative documents in this area, the Federal Law on Information Security Management, provides for the functioning of the Advisory Council on Information Security and Confidentiality advisory board) at the National Security Agency (§ 304). The above-mentioned normative document envisages the involvement of representatives of the public sector (representatives of non-governmental organizations, research institutes, universities, "think tanks", etc.) in the work of the advisory council. The main purpose of the council is public control over the work, establishing effective interaction of these bodies with the public sector [2].

In particular, in the framework of the "International Cyberspace Strategy", which was adopted by the Decree of the President of the United