outweigh the costs. In some cases, this may be seen as the inevitable cost of doing business in these particular markets and the criminality becomes normalised. Challenges include:

- Maintaining existing standards of integrity in public and private sector decision-making and avoiding complacency. The perception that New Zealand is corruption free may result in under-investment in internal controls, resulting in underidentification of risks and incidences of bribery and corruption

- Responding appropriately to incidents of corruption and ensuring that allegations are dealt with in appropriate forums (e.g. Courts as opposed to employment disciplinary processes). Treating corruption as an employment matter may downplay the seriousness of the incident and can contribute to perpetuation of the problem.

- Changing perceptions of criminality, promotion of whistleblowing and reporting of incidents of corruption

- Gaps in legal frameworks Actions underway to improve prevention and disruption of bribery and corruption include:

- Amending bribery and corruption offence provisions to align these with international standards and increase penalties for improved deterrence and criminal proceeds recovery

- Progressing ratification of UN Convention Against Corruption.

Список використаних джерел

1. Strengthening New Zealand's resistance to organized crime. An all-of-Government Response/ August 2011.

2. Who experiences crime? URL: https://www.justice.govt.nz/justice-sector-policy/research-data/nzcass/survey-results/who-experiences-crime/.

Хандій К., курсант Національної академії внутрішніх справ
Консультант з мови: ***Драмарецька Л.***

PROVIDING INFORMATION SECURITY

In the conditions of modern global and regional information confrontations, destructive communicative influences, spread of information expansion and aggression, protection of the national information space and guarantee information security are becoming a priority strategic objectives of modern states in the system of global information relations [1, p. 28].

The principal provision of the Constitution of Ukraine (Law, 28.06.1996 №254к/96-ВР) in this area is art.17 that states, "The protection of the sovereignty and territorial integrity of Ukraine, provision of its economic and information security are the most important functions of the state, a matter of the whole Ukrainian nation" [2].

One could attempt to find some answers in the Law "On Information" (Law, 02.10.1992 №2657-XII), which regulates relations

connected to information, the main aspects of state policy in the area, the right to information, its guarantees, establishes types of information, etc. [3]. However, the law is silent on the definition of information security.

Information security is an integrated component of national security. It is considered a priority function of the state. Information security, on the one hand, provides quality comprehensive information to citizens and free access to various sources of information, and on the other hand - it controls the spread of misinformation, promotes the integrity of society, preserves information sovereignty, counteracts negative information and psychological propaganda and protects national information space from manipulation, information wars and operations.

Attention to the problems of ensuring information security of Ukraine is due to anti-Ukrainian influences, which promote the ideas of separatism, violence, national enmity and are attempts to destroy Ukraine's national identity, interethnic harmony, encroach on the constitutional order of Ukraine, territorial integrity [1].

Information aggression and media fake epidemic spread worldwide have caused a serious need for responding to these phenomena in Europe at a global level.

The European Parliament became imbued with the approval of its own resolution on combating anti-European propaganda spread throughout the EU and reflected the basic principles of this counteraction in the Document called "EU strategic communication to counteract propaganda against it by third parties" adopted on November 23, 2016.

Following the example of the European Parliament and responding to the challenges of today in Ukraine, the Decree of the President of Ukraine № 47/2017 of February 25, 2017 approved the Doctrine of Information Security of Ukraine (hereinafter – the Doctrine). The Doctrine defines the national interests of Ukraine in the information area, the threats to their implementation, the directions and priorities of the state policy in the information area.

The Doctrine is based on the principles of respect for the rights and freedoms of citizens, respect for human dignity, protection of legitimate interests of individuals, of society and of the state, ensuring the sovereignty and territorial integrity of Ukraine.

The following bodies are directly involved into the implementation of the Doctrine: The National Security and Defence Council of Ukraine; the Cabinet of Ministers of Ukraine; the Ministry of Information Policy of Ukraine; the Ministry of Foreign Affairs of Ukraine; the Ministry of Defense of Ukraine; the Ministry of Culture of Ukraine; the Ukrainian State Film Agency; the National Council of Television and Radio Broadcasting of Ukraine; the State Committee for Television and Radio Broadcasting of Ukraine; the Security Service of Ukraine; the intelligence agencies of Ukraine; the State Service of Special Communications and Information Protection of Ukraine; the National Institute for Strategic Studies.

The priorities of the state policy on ensuring information security are:

- creation of an integrated information system of evaluating threats and rapid responding to them;
- legislative regulation of a mechanism of finding, fixing, blocking and deleting from the information landscape of the state, in particular, from the Ukrainian segment of the Internet, the information that threatens lives or health of Ukrainian citizens, promotes war, ethnic and religious hatred, invasive change of the constitutional system or violation of the territorial integrity of Ukraine;
- designation of mechanisms for regulation of operation activities of telecommunications companies, printing companies, publishers, broadcasters, TV and radio centers and other enterprises, institutions, organizations, cultural institutions and the media, and using of local radio stations, creation and development of structures responsible for information and psychological security, especially in the Armed Forces of Ukraine, based on the practice of NATO member states;
- development and protection of the technological infrastructure for ensuring information security of Ukraine;
- development of digital broadcasting, prevention of influence on its infrastructure of entities associated with the aggressor-state;
- building an effective and efficient strategic communications system;
- development of mechanisms for cooperation of the state with civil society in addressing the information aggression against Ukraine;
- strengthening capacity of the security and defense sector to counter specific information operations aimed at invasive change of the constitutional system, any violation of the sovereignty and territorial integrity, undermining the defense capacity of Ukraine, demoralization of the staff of the Armed Forces of Ukraine and of other military force, worsening of the socio-political situation;
- prevention of free circulation of information products (printed and electronic) primarily originated from the territory of the aggressor-state that contain propaganda of war, ethnic and religious hatred, invasive change of the constitutional system or any violation of the sovereignty and territorial integrity of Ukraine, provoking riots;
- conducting by the intelligence agencies of Ukraine of campaigns on promotion and protection of the national interests of Ukraine in the area of information, countering external threats to the state information security outside Ukraine;
- prevention of the use of the state information [4].

Thus, in the contemporaneous conditions of uncontrollable development of information technologies the presence of various informative threats became an integral part of the public reality. Contemporary informative risks have a strong influence on all spheres of social life and affect the national interests as well. The experience of Ukraine that got into the conditions of external military-informative

aggression can be an example in this context. The solution of the complex problem of information security will allow to protect the interests of society and the state, as well as to guarantee the rights of citizens to receive comprehensive, objective and high-quality information.

Список використаних джерел

1. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії сучасним інформаційно-психологічним впливам. *Львівська політехніка.* 2016. URL: ena.lp.edu.ua:8080/bitstream/ntb/37314/1/7_31-36.pdf.

2. Конституція України: Закон України від 28.06.1996 No 254к/96-ВР № 30. *Верховна Рада України*. С. 141. URL: http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

3. Про інформацію: Закон України від 2 жовт. 1992 № 48. *Відомості Верховної Ради України.* С. 650. URL: http://zakon3.rada.gov.ua/laws/show/2657-12.

4. The Doctrine of Information Security of Ukraine: The Decree of the President of Ukraine № 47. 2017. URL: https://rm.coe.int/doctrine-of-information-security-of-ukraine-developments-in-member-sta/168073e052.

Хмелюк Ю., курсант Національної академії внутрішніх справ
Консультант з мови: *Василенко О.*

CORRUPTION IN POLICE FORCES AND FIGHTING IT IN THE WORLD

Police corruption is a specific form of police misconduct designed to obtain financial benefits, personal gain, career advancement for a police officer or officers in exchange for not pursuing or selectively pursuing an investigation or arrest or aspects of the thin blue line itself where force members collude in lies to protect other members from accountability. One common form of police corruption is soliciting or accepting bribes in exchange for not reporting organized drug or prostitution rings or other illegal activities.

Another example is police officers flouting the police code of conduct in order to secure convictions of suspects–for example, through the use of falsified evidence. More rarely, police officers may deliberately and systematically participate in organized crime themselves. In most major cities, there are internal affairs sections to investigate suspected police corruption or misconduct.

Accurate information about the prevalence of police corruption is hard to come by, since the corrupt activities tend to happen in secret and police organizations have little incentive to publish information about corruption. Police officials and researchers alike have argued that in some