2. European Counter Terrorism Centre (ECTC) at Europol and counter terrorism related information sharing. URL: http://www.statewatch.org/news/2015/nov/eu-councileuropol-ECTC-14244-15.pdf.
3. Contre la radicalisation, la France cherche encore sa voie. URL: https://www.la-croix.com/France/Securite/Contre-radicalisation-France-cherche-encore-voie-2016-03-21-1200748144.

***Савельєва А.,***
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
*Консультант з мови:* **Драмарецька Л.**

## CYBERCRIME POLICY IN SPAIN

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal [1].

Nowadays, the use of information technology has no limits. The virtual space takes over everything from the real one in a row, including crime in its new forms and manifestations. Cybercrime includes various types of crimes committed using a computer and the Internet. The object of cybercrimes is personal data, bank accounts, passwords and other personal information.

The guiding principle of the National Cybersecurity Strategy in Spain is ensuring the appropriate coordination and cooperation among all the public authorities and also involving the private sector and citizens when necessary. The investment in prevention is growing in order to reduce the possibility of the citizens to become a victim of any kind of crime [2].

Today cyberattacks harm not only individuals and legal entities, but also states. Every year, hundreds of events of various levels are held around the world to discuss current cyber security issues. Cybercrimes can include all crimes against computer systems and data (for example, intentional access to a computer system or its part; intentional damage, destruction, deterioration, changing or hiding computer information). Also, cybercrimes can include intentional actions related to the violation of copyright and related rights, the implementation of intentional illegal actions related to the production, offering or providing access, distribution of child pornography, intentional actions that lead to the loss of property of another person through any input, changes, destruction or concealment of computer data.

The Spanish authorities listed the following main trends with regard to current cybercrime:

- sexual exploitation of children on the Internet;
- online fraud (Payment fraud);
- cyber-attacks;
- online criminal markets;

- the convergence of cybercrime and cyberterrorism;
- cross-cutting crime factors, mainly social engineering techniques and cryptocurrencies [2].

The prevention is a fundamental pillar. There are many initiatives and good practices in terms of awareness-raising campaigns within schools, training of practitioners and mass media campaigns:

- giving a coordinated and efficient answer to issues related to the security of both minors (schools and their environments) and the rest of groups of Spanish population (the elderly, tourists, vulnerable groups of people, etc.);
- fostering the awareness of the society about police resources for crime prevention and victims' protection;
- enhance the trust of society in the National Police and the development of proactive behaviour to reveal the situations and crimes of which they may be victims;
- collaborating with other public institutions with responsibilities in this area [2].

It is impossible to completely protect yourself from cyber-attacks. However, following at least the minimum-security rules for online behavior will significantly increase the chances that you will not be hacked. Security rules include not downloading software from untrusted sources; use antiviruses to work with computers; do not open files and letters from suspicious sources; do not click on suspicious links.

According to recent data, more than 13 thousand legal proceedings for cybercrime took place in Spain, most of them corresponding with fraud or crimes against sexual freedom. Despite this, about 60 percent of the Spanish population took measures to improve their safety when surfing online in recent years. Crimes against intellectual property also deserve special attention, not only because of the large losses they generate for the economy, but also because this is a type of crime that is mostly viewed favorably by the general public in Spain [3].

More than 70 % of the Spanish population use the internet every day. But these individuals, as well as businesses and groups of all sizes, are all putting themselves at risk of some form of cyberattack each time they go online. After the many high-profile cases of cyber-attacks all around the world in the last years, Spain and its people are more aware of the importance of cybersecurity than ever before. A big focus of Spain's National Cyber Security Strategy is to educate the general public on cybersecurity and raise awareness regarding cyber-attacks and what can be done to protect against them. The authorities understand that to see the stats on cybercrime in Spain dropping, the Spanish people need to know what they're dealing with and the best ways to protect themselves. Some studies even indicate that three in four of Spain's internet users have zero protection [4].

Of course, the implementation of security measures will only minimize the possibility of accidental unauthorized access to your devices and systems, but it is impossible to provide a complete guarantee of avoiding hacking. Thus, the most common type of crime is fraud on the Internet.

***Список використаних джерел***

1. What is cybercrime? How to protect yourself from cybercrime. URL: https://www.kaspersky.com/resource-center/threats/what-is-cybercrime.
2. Spanish policy on cybercrime. URL: https://eucpn.org/document/spanish-policy-on-cybercrime-1.
3. Cybercrime in Spain – Statistics & Facts. URL: https://www.statista.com/topics/7011/cyber-crime-in-spain/#dossier Contents__outerWrapper.
4. Cybersecurity in Spain. URL: https://cybernews.com/security/cybersecurity-in-spain/.

***Савка Н.,***
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
*Консультант з мови:* **Козубенко І.**

## COMBATING OF INTERNATIONAL TERRORISM IN THE EUROPEAN UNION

Nowadays, the phenomenon of terrorism is quite common. Until recently, turning to terror as a means of solving political or religious problems was an exceptional, extraordinary phenomenon, nowadays, almost daily reports of terrorist acts are seen as inevitable. Terror has become an organic component of modern life and has acquired a global character.

Terrorism (from Latin *terror* – fear, intimidation) is a form of political extremism, the use of the most violent methods of violence, including the physical destruction of people to achieve certain goals. Terrorism is committed by individuals, groups that express the interests of particular political movements or represent the country. Where terrorism is elevated to the rank of public policy. Terrorism is an anti-human way of solving political problems in the face of confrontation, clashing interests of different forces, manifestations of inequality in interstate, interreligious relations. It can also be used as a means of satisfying ambitions by individual politicians, as well as as an instrument of their goals by the mafia structures, the criminal world. Terrorism can be defined as a policy of intimidation, suppression of the enemy by force. There are three main types of terrorism: political, religious and criminal. There is little legal comment on the classification of acts of terrorism [1].

These include:

– Attack on government or industrial sites that cause material damage and is an effective means of intimidation and demonstration of force;

– seizure of state institutions or embassies (accompanied by hostage-taking, which causes serious public outcry);

– seizure of aircraft or other vehicles (political motivation);

– the release of fellow party members from prison; criminal motivation – demand for redemption);