- take action when you find a violation.

As we see, the theft of works of art is a very widespread crime today, so it needs attention and constant monitoring by the law enforcement of the world, and particularly in Ukraine.

Список використаних джерел:

1. How art treasures are stolen to order. URL: https://www.theguardian. com/uk/2000/jan/08/nickhopkins

2. Stealing the Mona Lisa, 1911. URL: https://web.archive.org/web/ 20070303065050/http://www.time.com/crimes/2.html

3. Art theft. URL: https://en.wikipedia.org/wiki/Art_theft

4. Art Crime Team. URL: https://www.fbi.gov/investigate/violent-crime/art-theft

Колесник А.Є.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: Ченківська Н.

CYBERCRIME – ONE OF THE BIGGEST THREAT OF 21ST CENTURY

The 21st century has seen the rise of entirely new challenges, in which criminal and national security threats strike from afar through computer networks with potentially devastating consequences. The National Police of Ukraine continues to adapt to meet these challenges. Department of Cyberpolice was formed on 3 October 2015 to combat cyber-based terrorism, hostile foreign intelligence operations conducted over the Internet and cybercrime by applying the highest level of technical capability and investigative expertise. The Cyber Division continues to evolve for defend Ukraine against the rapidly growing cyber threat [1].

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers [2].

There are more connected devices, connected people and connected things than at any time in history and, as the 21st century progresses, this trend is set to continue. For many people, all this innovation is going to make the world a smarter, sharper and more captivating place to be, with

new technologies offering us plenty by way of opportunities. Others, naturally, remain skeptical.

At the same time, in the dark, beneath the surface, there lies another world where cybercriminals are equally enabled and empowered by these technologies (as they become exploited and manipulated). It's a world without borders, the digital wild west, where the rules of law are disregarded [3].

21st century cybercriminals are more sophisticated, daring and organized than ever. The threat landscape has evolved and conditionally divided into:

VIRUS (Virtual information resource under size networking) - although often used as the collective term for Malware, is actually just a type of Malware.

WORM - is similar in many ways to a Virus but with one key difference: A Worm does not require a host to replicate itself.

PAYLOAD - "Payload Code often simply called the "Payload, is the additional functionality present in Viruses, Worms or Trojan Horses.

PUPs - are programmes, which not cause harm to your system but might be unwanted (Potentially Unwanted Program).

ROOTKIT - is a collection of one or more tools designed to covertly gain and maintain control of a computer.

BOT - Short for "ROBOT", a bot is a program that is designed to automate tasks.

SCAMS - are very similar to phishing, but are not usually interested in obtaining your details, they often appeals to human greed.

MALWARE - stands for MALicious SoftWARE term such as Virus, Trojan, Worm, and Bot all have specific meanings.

TROJAN HORSE - in computing term is similar to its Homeric namesake: An attractive or desire file, which hides a sinister payload within.

SPYWARE - does almost exactly, what it says on the tin: it is the software, which spies on the infected user.

PHISHING - is a social engineering attack, which attempts to fraudulently acquire sensative personal information.

DWARE - a type of Advertising Display Software, whose primary purpose is to deliver advertising content that may be un- expected and unwanted by users.

BOTNET - is a group of BOT infected PC's that are all controlled by the same "command and control center.

HOAXES - are usually silly pranks, chain mail or Urban Legends.

Given the constant evolution of the cybercrime landscape, police agencies need to share information and knowledge with their counterparts around the world to develop a timely, intelligence-based response.

INTERPOL has created two secure and flexible services to facilitate cybercrime-related communication among police and other stakeholders:

Cybercrime Knowledge Exchange workspace, which handles general, non-police information and is open to all relevant users;

Cybercrime Collaborative Platform – Operation, to support law enforcement operations, with access restricted to operational stakeholders only [4].

In recent years, as our personal and professional lives have increasingly been defined and shaped by gadgets and gizmos, we've become accustomed to a more streamlined way of living. That's the brilliant thing about connected technologies – it helps to make life easier and more fun.

Yet, thanks to 21st century cybercriminals, everything we take for granted – paying for a book online, inputting your name and address on a webpage – is at risk. More so if we don't invest in security software, develop skills and work together. The threat landscape may have evolved, but together, the security environment can also advance. It just takes effort.

Список використаних джерел:

1. Cyber URL: https://archives.fbi.gov/archives/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/cyber-1

2. The Biggest Threat of 21st Century – CyberCrime URL: https://www.zenesys.com/infographics/the-biggest-threat-of-21st-century-cybercrime

3. 21st century cybercriminals: The threat landscape has evolved URL: https://www.welivesecurity.com/2016/08/26/21st-century-cybercriminals-threat-landscape-evolved/

4. Cybercrime Collaboration Services URL: https://www.interpol.int/Crimes/ Cybercrime/Cybercrime-Collaboration-Services