It is impossible not to mention on what luxury cars Dubai policemen drive. Instead of a simple sedan, they drive around on super-fast Lamborghini and Ferrari. For the police service, which is just a little over 50 years old the Dubai police is remarkably well equipped. The Dubai government explains this by the fact that the work of the police must be safe, fast and effective, so these cars are used in police equipment.

When police are dealing with suspects, they have an electronic fingerprint recognition system. In the near future, the robotic police officers will be used in police equipment.

Список використаних джерел

1. [Електронний ресурс]. - Код доступу : http://dubai.in.ua/policiya-dubaya.html
2. [Електронний ресурс]. - Код доступу : https://en.wikipedia.org/wiki/Dubai_Police_Force
3. [Електронний ресурс]. - Код доступу : https://en.wikipedia.org/wiki/Crime_in_the_United_Arab_Emirates
4. [Електронний ресурс]. - Код доступу : https://www.rt.com/shows/sophieco/440000-united-arab-emirates-trade/
5. [Електронний ресурс]. - Код доступу : https://eeas.europa.eu/generic-warning-system-
6. [Електронний ресурс]. - Код доступу : https://dubai-freezone.ae/novosti-oae/uroven-prestupnosti-v-dubae-i-oae.html

Чабан К.,
курсант ННІ № 2 Національної академії внутрішніх справ
Консультант з мови: **Василенко О.В.**

PROBLEM OF CYBER SECURITY PROTECTION IN UKRAINE

Cybercrime exploits cross-national differences in the capacity to prevent, detect, investigate, and prosecute such crime, and is fast becoming a growing global concern. Cybercrime has quickly evolved from a relatively low volume crime committed by an individual specialist offender to a mainstream or common high volume crime «organized and industrial like».

The Internet has also been used as a vehicle for fraud. Spurious investment solicitations, marriage proposals, and a variety of other fraudulent overtures are made daily by the hundreds of millions. In recent years, insurgent and extremist groups have used Internet technology as an instrument of theft in order to enhance their resource base.

Cybercrimes begin with unauthorized access to a computer system. Information systems may be targeted for the data they contain, including banking and credit card details, commercial trade secrets, or classified information held by governments. Theft of personal financial details has provided the basis for thriving markets in such data, which enable fraud on a significant scale.

As digital technology pervades modern society, we have become increasingly dependent upon it to manage our lives. Much of our ordinary communications and record keeping rely on the Internet and related technologies. Criminals and terrorists use the Internet as a medium of communication in furtherance of criminal conspiracies.

And like for law-abiding citizens, it is a means of storing records and other information, and performing financial transactions, albeit in the case of criminals, such transactions may be part of money laundering activities. Manufacturers of illicit drugs advertise and trade recipes over the Internet.

Since the end of the Cold War, there has been a proliferation in online criminal activity in Eastern Europe, and Ukraine is no exception. Famous for its hacker community, Ukraine ranks among the Top 10 countries in the world in cyber crime and number 15 as a source of Distributed Denial of Service (DDoS) attacks. In 2012, five Ukrainian nationals stole more than $72 million from U.S. bank accounts; in 2013, Ukrainian hackers stole 40 million sets of debit and credit card details from the US retail chain Target; in 2014, the RAND Corporation wrote that Russian and Ukrainian were the lingua franca of online hacker forums. In this light, it is natural to wonder if Ukraine is today a safe haven for cyber criminals.

Current cyber security protection in Ukraine is rather low, cases of illegal collection, storage, use, distribution of personal data, illegal financial transactions, theft and fraud become more and more common on the Internet.

Several factors contributed to making Ukraine a cyber safe haven. First, its Soviet school STEM (science, technology, engineering, and mathematics) education is among the best in the world. Second, its underwhelming economic performance since independence in 1991 has led these STEM specialists to explore alternative career paths, often online. In addition, the conflict in eastern Ukraine has given rise to numerous high-level cyber attacks.

Moreover various sectors of the Ukrainian economy and life are very vulnerable in cyberspace now, state and private companies suffer from cyber attacks to which they were completely unprepared. Unfortunately Ukraine has no any instruments for prevention and repulse of attacks in information sphere, all measures of cyber protection are unsystematic and ineffective.

Less than two months after the spread of the WannaCry ransomware in May, Ukraine faced yet another cyberattack, perhaps the most serious one in its history. Referred to as «Petya», «Petya.A», «PetrWrap», «GoldenEye», «Diskcoder.C», etc., the virus had quickly spread among Ukrainian systems, temporarily putting out of commission those of state bodies, airports, banks, media companies, delivery services and even the radiation monitoring systems at the former Chernobyl nuclear power plant. Damage was also done to many organizations abroad, including US Merck, Russian Rosneft, British WPP, French Saint-Gobain, Australian Cadbury, etc. The speed of the malware's spread, the multitude of organizations harmed, including various objects of key infrastructure, as well as the serious obstacles to restoring the corrupted data once again underline today's priority of cybersecurity within the areas of national security of a state.

That malware spread itself around systems, encrypted files and provided the user with «ransom» demands for their decryption. One might attempt to imagine an analogy in a world without information technologies. A group of offenders makes their way into an office of an organization, breaks into a safe, steals several folders of documents and leaves a letter with ransom demands on the director's table. This crime would definitely harm the organization; some of its consumers, maybe business partners, perhaps go as far as harming the industry sector. In our world, however, the act, carried out in a digital environment, causes global chaos and a widespread panic.

Another problem is underfinancing of the relevant public institutions that leads to a reduced attractiveness of workplaces over low salaries – only a limited number of highly skilled cybersecurity and cyber defence professionals are employed with the public sector institutions.

To sum up, we need to notice that Ukraine has already carried out many steps in establishing its system of cybersecurity. It has adopted a substantial number of acts designed to create a general normative framework, as well as to regulate different specific aspects of cybersecurity. Ukraine has identified the threats to the national interests in this area of national security, set out directions of future policy measures and established a circle of actors responsible for the provision of cybersecurity. Our country has more than enough STEM expertise, but it must be refocused and repurposed toward a more transparent and accountable legal and cultural online environment.

Список використаних джерел

1. Crime in Cyberspace: Offenders and the Role of Organized Crime Groups, working paper, Roderic Broadhurst, Peter Grabosky, Mamoun

Alazab, Brigitte Bouhours, Steve Chon & Chen Da Australian National University Cybercrime Observatory, 15.05.2013.

2. Cybersecurity in Ukraine: National Strategy and international cooperation Nadiya Kostyuk - 'Ukraine: A Cyber Safe Haven?,chapter 13, University of Michigan, NATO CCDCOE, 2015.

3. Cybersecurity in Ukraine: National Strategy and international cooperation, Oleksii Tkachenko, International Relations Officer, Cyber Department, Security Service of Ukraine,2017.

Шахрай Д.,
курсант ВСФП Національної академії внутрішніх справ
Консультант з мови: **Литвиненко Я.В.**

FACE RECOGNITION IS THE NEW WAY TO PREVENT CRIME

Facial recognition is an important and rapidly evolving biometric science which opens up many new opportunities for identifying individuals and solving crimes.

INTERPOL launched a database of facial images in November 2016, with the support of our Strategic Partner, Safran Identity & Security (formerly Morpho).

This tool enables the global law enforcement community to share and compare data in order to:

- Identify fugitives and missing persons;
- Identify unknown persons of interest;
- Identify subjects in public media images;
- Verify mugshots received against a database.

In a future project, they plan to make selected images available through mobile devices in order to assist operations and investigations in the field. This will enable the Organization to carry out facial recognition checks in real time against specific watchlists [1].

Face recognition starts with building a database of relevant individuals. Retail organizations would include known organized retail criminals and shoplifters. For airports, it might be a watchlist of terrorists and fugitives wanted by Interpol. Stadiums using face recognition for event security, on the other hand, might want to keep out fans who have previously disrupted sports games or caused disturbances. While face recognition for banking might involve keeping out individuals with a history of fraud.

The next phase is matching. Cameras can be set up and optimized for angle and lighting conditions. As individuals enter a secure area, images of