tested in Dnipropetrovsk and Kirovohrad regions, there is every chance to take these reservations into account and avoid mistakes. So that the next law enforcement reform does not become a "bubble". Especially since Ukraine has a positive experience of implementing changes in this area.

### Список використаних джерел

1. https://nationalcorps.org/reformi-pravoohoronno-sistemi-v-ukran-chi-stalo-ukrancjam-bezpechnshe/
2. http://reformsguide.org.ua/ua/analytics/law-enforcement-reform/
3. https://ukrainesecuritysector.com/wp-content/uploads/2017/04/law_enforcementreform_ukraine.pdf

**Євсеєнкова К.,**
урсантка ННІ № 1
Національної академії внутрішніх справ
Консультант з мови: **Грабовська Н.А.**

## THE IBM X-FORCE COMMAND CYBER TACTICAL OPERATIONS CENTER (C-TOC)

The process of evolution, the introduction of new technologies bring benefits to the modern world, on the one hand, and new threats on the other. One of these threats is cybercrime. Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network. Criminals steal information from other people's computers, send e-mail viruses, which are able to completely shut down your computer, break into bank networks, and commit other kinds of fraud on the Internet. As a result, cybercrime may suffer the interests of the ordinary citizen and the whole country, including the entire National Security.

Based on the data of the Global Cybersecurity Index (GCI), Ukraine is included in the medium level of commitment in 2018. The Global Cybersecurity Index (GCI) is a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. [1] In the fight against cybercrime, Ukraine is collaborating with international organizations, introducing new prevention mechanisms. However, according to the results of the 2018 Worldwide Economic Crime and Fraud Survey conducted by PwC, it turned out that the level of cybercrime is increasing compared to 2016.

Due to the increase in the level of cybercrime in Ukraine, there is a need to expand the country's technical capabilities. In this case, it would be right to turn to foreign experience on this issue.

In 2018 IBM Security announced the industry's first mobile Security Operations Center, capable of traveling onsite for cybersecurity training, preparedness, and response. The IBM X-Force Command Cyber Tactical Operations Center (C-TOC) will travel around the U.S. and Europe, running incident response drills with clients, providing on-demand cybersecurity support, and building cybersecurity awareness and skills with professionals, students and consumers.

The IBM X-Force C-TOC is a fully operational Security Operations Center on wheels, modeled after Tactical Operations Centers used by the military and incident command posts used by first responders. Housed in a tractor trailer, the mobile facility provides a gesture-controlled cybersecurity "watch floor," data center and conference facilities that can accommodate two dozen operators, analysts and incident command center staff. The facility can be deployed in a variety of environments, with self-sustaining power, satellite and cellular communications, providing a sterile and resilient network for investigation and response as well as a state-of-the-art platform for cybersecurity training.

Historically, cybersecurity teams have been focused on detection and protection against cybersecurity incidents. However, as the threat landscape has evolved, organizations are now recognizing the need to plan and rehearse their response to security incidents as well. The 2018 Cost of a Data Breach Study1 found that companies that are able to respond to incidents effectively and remediate the event within 30 days can save over $1 million on the total cost of a data breach – yet less than 25% of professionals surveyed say their company has a coordinated incident response plan applied across the organization.

IBM also designed the C-TOC to have the potential to supplement onsite support for clients at times when their cybersecurity needs may surge. Cybercriminals are constantly on the lookout for major events and moments in time to help launch their attacks, taking advantage of increased interest, cashflow and internet activities to get higher returns on their malicious activities.

Cybersecurity at large-scale events is increasingly being considered alongside emergency services response and public safety. For these events, IBM can bring the C-TOC onsite to help not only with preparation, but to provide an isolated network, cybersecurity watch floor and incident command infrastructure. [3]

In his speech at the IBM Security Summit, Charles Henderson, the founder of IBM, said: “We are not only testing network security, we are testing it in general. And I do not mean that we have a criminal organization here. I mean that we are looking for vulnerabilities. " Charles Henderson also gave some tips for ordinary citizens:

First - think like a hacker in everything you do. Of course, it’s still useful to hire someone for an offline test, but, in my experience, people who think like an attacker before my team starts working with them are usually much better at their job. All in all, this is a great mental exercise that prepares for the moment when everything goes wrong. And such moments happen.

Second - test everything. It is clear that budgets are limited, but often you can find some way. Because if you rely on luck, the first person to test your system will be a criminal.

Third - the vulnerability found is good. Maybe this sounds trivial, but you do not need to be afraid to find vulnerabilities and you do not need to convince yourself that closing them is too expensive. [4]

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging treats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 60 billion security events per day in more than 130 countries, and has been granted more than 8,000 security patents worldwide. [3]

As we can see, this Cyber Tactical Operations Center on wheels is a high-tech, mobile and effective anti-cybercrime tool. It is worth noting that this method can act as preventive, the main task of which is to identify vulnerabilities. C-TOC can be closely interlinked with the state authorities to combat cybercrime, and can also act as a separate and independent unit, which will have some of its tasks.

Such a device is not unique in its kind. There are various ways and mechanisms in the campaigns against cybercrime, which are represented in different countries of the world. This experience can be a useful acquisition for our country in the fight against this rapidly developing crime.

### Список використаних джерел

1. International Telecommunication Union Global Cybersecurity Index (GCI) 2018 // Studies & research. - 2019. - ISBN: 978-92-61-28201-1. - C. 14.

2. Електронний ресурс: Cybercrime // https://en.wikipedia.org/wiki/Cybercrime

3. Електронний ресурс: IBM Rolls Out Industry's First Cybersecurity Operations Center on Wheels // https://newsroom.ibm.com URL: https://newsroom.ibm.com/2018-10-15-IBM-Rolls-Out-Industrys-First-Cybersecurity-Operations-Center-on-Wheels

4. Електронний ресурс: IIBM X-Force Red. Как красная команда IBM проверяет организации на прочность // https://xakep.ru URL: https://xakep.ru/2019/07/11/ibm-x-force-red/

**Качковський В.,**
курсант ННІ №1
Національної академії внутрішніх справ
Консультант з мови: **Драмарецька Л.Б.**

## CORPS OF RAPID ACTION

The Euromaidan has spurred efforts to shed the communist and post-communist policing legacy marked by authoritarianism and corruption, and opened a space for democratic policing in Ukraine. This work conceptualizes police reform during the first three years after the revolution