Cybercrime Directorate at the INTERPOL Global Complex for Innovation in Singapore [2].

Urgent measures that are needed to preserve data at the national level are also necessary within the framework of international co-operation.

Список використаних джерел:

1. **Council of Europe.** [Електронний ресурс]. – Режим доступу: https://www.coe.int/en/web/cybercrime/international-cooperation

2. INTERPOL desk targets cybercriminals and Internet fraud in Africa. [Електронний ресурс]. – Режим доступу: https://www.interpol.int/News-and-Events/News/2021/INTERPOL-launches-initiative-to-fight-cybercrime-in-Africa

3. United Nations. [Електронний ресурс]. – Режим доступу: https://www.unodc.org/unodc/en/cybercrime/index.html

Кубишин І.,
здобувач ступеня вищої освіти бакалавра Національної академії внутрішніх справ
Консультант з мови: Ващук А.

FOREIGN EXPERIENCE IN COMBATING CYBERCRIMES COMMITTED WITH THE RANSOMWARE

Today, the global problem of the international community is cybercrime, the number of which is growing every year. Utilities and other critical infrastructure are a popular target for cyber attacks.

Since the beginning of 2020, there have been several high-profile attacks by various groups on large corporations, including critical infrastructure operators. Colonial Pipeline has been hit by cybercriminals, resulting in gasoline shortages in several US states. [1] The Washington Police Department, District of Columbia, hackers blocked secret files from the department and demanded $ 4 million to prevent data leaks. The Russian group said they had collected 250 GB of files, including information about informants and the history of the department's staff. The Comparitech report shows that in 2020, 92 attacks by individual ransomware affected more than 600 individual clinics, hospitals and organizations and more than 18 million patient records. Comparitech estimates that the attacks cost nearly $ 21 billion. [2]

Thus, it can be concluded that the need to sharply strengthen cybersecurity around strategically important infrastructure needs to be addressed.

Numerous attacks have led to a significant investment in the development of cybersecurity software products, the creation of teams of

specialists in the protection of computer systems, which have joined the staff of organizations.

In the United Kingdom, a non-profit organization CREST has been established, which deals with information security, accreditation of organizations and certification of individuals who provide services in the IT field. Thanks to this organization, systems for technical assessment and certification of cybersecurity standards for the British government - Cyber Essentials and Cyber Essentials Plus, have been developed to protect against malware. CREST is actively involved in the government's efforts to combat illegal online activities. [3, p.7]

The Australian Cyber Security Center has been established in Australia, the purpose of which is to develop companies by:

- Technical expertise in Information and Operational Technologies;
- Principles-based advice tailored toward high-risk environments;
- Remediation activities;
- Proactive partnerships and threat assessments. [4]

Cyber attacks are on the increase and becoming more dangerous. More and more damage is being caused, too. In order to counteract this, the Federal Cabinet has now adopted the Cyber Security Strategy for Germany 2021. In addition to carrying forward the existing strategy, this sets down fundamental, long-term goals.

The strategy comprises four overarching guidelines:

- Establish cyber security as a joint task of the state, business, society and science,
- Strengthen the digital sovereignty of the state, business, science and society,
- Ensure the secure development of digitalization,
- Make targets measurable and transparent. [5, p. 122]

The lack of ability to monitor the cryptocurrency market, due to its anonymity, has led to an increase in the number of cryptographers. Therefore, cryptocurrencies need to be included in the broad international financial structure. This will reduce the number of safe places for cybercriminals.

In addition, in my opinion, the formation of common terminology and definitions remains important for international cooperation in combating cybercrime. What is cybercrime and what is a ransomware virus is understood differently in different countries because there are so many different viruses. Cooperation between government agencies should be in one language.

The magnitude of the threats faced by Ukrainian infrastructure and citizens has increased. They will become more acute as our society and economy become increasingly connected. As the threat evolves, so too must our response.

Lack of trained personnel in the field of combating cybercrime; lenient position of judges in sentencing; low level of public awareness of cybercrime and its harm, as well as measures to protect digital information from criminal encroachment (the most vulnerable targets of ransomware hackers were computer systems of schools and medical institutions) essentially create conditions for the development of cybercrime. In my opinion, the work of the Government of Ukraine in the field of information security should be focused on their elimination. At the same time, the results of monitoring irregular cash flows should be taken into account when developing effective measures to combat cybercrime.

At the same time, as a direction to improve the protection of computer information, it is proposed to raise public awareness of cybersecurity issues and create a hotline for victims of cybercrime.

Список використаних джерел:

1. FBI Statement on Network Disruption at Colonial Pipeline May 9, 2021 URL: https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-networkdisruption-at-colonial-pipeline

2. P. Bischoff. Ransomware attacks on US healthcare organizations cost $20.8bn in 2020. URL: https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

3. Identify, Intervene, Inspire. CREST/NCA, 2015 URL:https://www.crest-approved.org/wp-content/uploads/CREST_NCA_CyberCrimeReport.pdf

4. "National security reform announcement press conference". Prime Minister of Australia. 18 July 2017. URL: https://web.archive.org/web/20170828183852/ https:// www.pm.gov.au/media/2017-07-18/press-conference-attorney-general-senator-hon-george-brandis-qc-minister

5. Cyber Security Strategy for Germany 2021.Federal Ministry of the Interior, Building and Community,05 October 2021 URL : https://docreader.readspeaker. com/docreader/?jsmode=1&cid=btste&lang=en_uk&url=https%3A%2F%2Fwww.bmi.bund.de%2FSharedDocs%2Fdownloads%2FEN%2Fthemen%2Fit-digital-policy%2 Fcyber-security-strategy-for-germany2021.pdf%3Bjsessionid%3DE51F8EB90DD08

50509BB8487FC22422F.1_cid364%3F__blob%3DpublicationFile%26amp%3Bv%3D3

Кузнєцов І.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: Скриник Л.

MODERN METHODS OF MONEY LAUNDERING

One of the leading international organizations for the prevention and fight against money laundering is a working group for the establishment of financial and regulatory measures against money laundering (Financial Action Task Force on Money Laundering, FATF). This organization cooperates closely with the World Bank and International Monetary Fund, and from June 2000 develops a list of countries and territories that do not cooperate in the fight against money laundering (Non-Cooperative Countries and Territories, NCCT). Twenty-five criteria that a country should satisfy to not appear on the list were developed. For instance, in June2000, the list included 15 states, with a number varying each year [1]. If a country is not on the NCCT list, it does not automatically mean that it has no money laundering, but that it is difficult to officially obtain relevant data from its economic, banking and judicial systems.

Money laundering is not an isolated case characteristic for a country or a number of countries, but happens worldwide and it is unlikely to disappear, so it isrealistic to speak about its reduction to a level tentatively tolerated by a society. In fact, criminal groups will always try to 'clean' illegally acquired "black" resources and bring them into the legal economy. Thus, the phenomenon of money laundering does not appear separately from other harmful social phenomena and corresponds to the general level of crime in a society, but it has certain characteristics that distinguish it from other types of crime.

Money is commonly laundered through the banking system operations, due to suitability of this domain for various forms of abuse related to money laundering. In particular, banking involves a wide range of operations regulated by the system of legal acts at national and supranational level. These operations include: deposit, credit, foreign-currency and exchange operations, issuing, storing, buying and selling of securities, payment operations in the country (taking into account natural and legal persons, making invoice payments, receiving payments, issuing and paying with credit cards and other payment instruments), foreign payment transactions and others. Taking into account a wide range of