coincide with the norms of fighting and countering domestic violence in Ukraine. In my opinion, the Ukrainian police should familiarize themselves with the Polish "Blue Card" practice for further application in their activities. The relationship between Ukraine and Poland in this matter is the best solution to the global problem of domestic violence.

Список використаних джерел:

1. « Ustawa – Kodeks karny ». URL: www.gov.pl/web/mswia/ustawa---kodeks-karny.

2. « Zapobieganie i zwalczanie przemocy wobec kobiet i przemocy domowej. Raport GREVIO na temat Polski». URL: https://bip.brpo.gov.pl/pl/content/RPO-raport-grevio-przemoc-domowa.

3. « PORADNIK – Jak przeciwdziałać przemocy w rodzinie? Przeciwdziałanie przemocy w rodzinie». URL: https://cloud-7.edupage.org/cloud/PORADNIK_przemoc_w_rodzinie.pdf?z%3ApyZYPBlORS%2B%2FSpojvpu5QwxgdWFvBsA0rHKHj5Yydn2RE7aBUzRoKGCDTftzaR%2Bj

4. «USTAWA z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie». URL:https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20051801493/U/D20051493Lj.pdf.

Слободян О.,
здобувач ступеня вищої освіти бакалавр
Національної академії внутрішніх справ
Консультант з мови**: Скриник Л.М.**

CYBER SECURITY IN FRANCE

With the help of the Internet and computer technology, people make various bank payments, create online stores and earn money from it. But with the appearance of this, new problems appeared, and more precisely, new crimes - cybercrimes. Many states have already begun to take care of the information security system of their citizens. Various organizations are being created to combat hackers and other cybercriminals.

Cybersecurity requires a lot of efforts that cover not only the security of application, but also the behavior of employees in the field of information security, other risks and many other potential vulnerabilities. Let's talk about the general system of fighting France with cybercrime.

The regulatory act that regulates the activity of state policy in the field of security is the White Book (2008) is coming out with the need to deal with new types of dangers that appeared in 1994. Among the most likely threats to the territory of France and the

European community (terrorism, use of ballistic missiles, organized crime, natural risks and worsening of the epidemiological situation in large cities, hidden imigration) are large-scale attacks on information systems, espionage and strategic influence [1].

Other major cyber dangers include: malware, which gets to and harms a gadget without permission; clandestine mining, which invades a computer or a phone to create cryptocurrency without the assent of the owner; the robbery and divulgence of data and individual data [4].

Law No. 2013-1168 of December 18, 2013 was also introduced in France, which stipulates that "the prime minister defines the policy and coordinates the government's actions in the field of cyber security and cyber protection. For this purpose, he/she has at his/her disposal “the French National Agency for Cyber Security”, ANSSI, reporting to the Secretary General for Defense and National Security [2].

Let us note that France adopted a national cyber security strategy in 2015. This Strategy aims to accompany French society’s digital transition and address the new challenges of changing uses of digital technology and the associated threats: It focuses on five goals:

- Guaranteeing national sovereignty,
- Providing a strong response to acts of cyber crime,
- Informing the public,
- Making digital security a competitive advantage for French businesses,
- Enhancing France’s voice on the international stage [3].

In recent years, the number of cybercrimes has been increasing significantly, especially in European countries, and France is no exception. Statistics on the number of cybercrimes in recent years help to understand how important cyber security is.

According to statistics in 2021, more than 54% of French companies suffered a computer attack. This percentage, taken from the CESIN 2022 Corporate Security Barometer, is cause for concern. For its part, the ANSSI (National Information Systems Security Agency) specifies that 43% of cyberattacks have targeted small and medium-sized enterprises, which are less equipped to deal with hackers. Local authorities (20% of cyberattacks) and hospitals (11%) are also hard hit, as are large companies (26%) [4].

Also, according to the data of the public organization Orange Cyberdefense, in 2021, businesses in France suffered more cyberattacks than, for example, in 2020. After that, French President Emmanuel Macron announced the creation of a special school to train cyber patrolmen who will counter information crimes. The decision is correct because it will help reduce the number of cyber attacks and prevent the emergence of new Internet crimes.

In addition to all of the above, we note the mobilization of the international community through the Paris appeal. The Paris Call for Trust and Security in Cyberspace demonstrates France's active role in promoting a safe, stable and open cyberspace.

This high-level political declaration marks a renewed commitment to the fundamental issue of stability in cyberspace. The Paris Appeal was launched at the Paris Peace Forum on 12 November 2018 and was presented by the President of France to UNESCO before the Internet Governance Forum. This demonstrates France's ability to broadly support its vision for regulating cyberspace.

The text was supported by many different organizations (the number of which reaches approximately 500). It notes key principles such as the application of international law and human rights to cyberspace, as well as principles such as: responsible state behavior, state monopoly on lawful violence, and recognition of the specific responsibilities of private page interests, which are part of the French vision of a safe cyberspace.

The inclusive approach of the Paris Call highlights the need for a multi-stakeholder approach to developing standards and best practices to securely and safely harness the opportunities offered by the digital revolution. France intends to review, together with its foreign public partners, as well as the private sector and civil society, the role and specific responsibility of private interest pages in strengthening the stability and international security of cyberspace.

So, the article provides information about the methods of combating cybercrimes in France and about the regulatory and legal framework that ensures the regulation of the information space.

Список використаних джерел :

1. «Біла книга - найменування французької доктрини з питань оборони і національної безпеки». [Електронний ресурс] . — URL: http://ni.biz.ua/13/13_3/13_37239_belaya-kniga--naimenovanie-frantsuzskoy-doktrini-po-voprosam-oboroni-i-natsionalnoy-bezopasnosti.html
2. «CYBERSECURITY IN FRANCE». [Електронний ресурс] . — URL: https://www.ssi.gouv.fr/en/cybersecurity-in-france/
3. «French Diplomasy». [Електронний ресурс] . — URL: https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/
4. «Cybercrime in France and Europe». [Електронний ресурс] . — URL: https://www.cybersecurity-business.school/en/cybercrime-in-france-and-europe/