2. Cybercrime Laws In The United States. URL : <http://www.aaronkellylaw.com/cybercrime-laws-united-states/>

3. Cybercrimes in America. Cyber security insights report. URL : <https://us.norton.com/internetsecurity-online-scams-top-5-cybercrimes-in-america-norton-cyber-security-insights-report.html>

4. The riskiest states for cybercrime in America. URL : <https://www.webroot.com/blog/2018/06/05/2018-riskiest-states-for-cybercrime-in-america/>

Торбич О.,
курсант ННІ 1 Національної академії внутрішніх справ
Консультант з мови: **Драмарецька Л.Б.**

FRENCH POLICY ON CYBERSECURITY

In recent years, France has completely reformulated its defense and national security priorities, taking into account the increase in volume, level, intensity and complexity of cyber-threats, including cybercrime, political and economic espionage. The White Paper on National Defense and Security 2008 was the first fundamental document devoted only to the problem of national cyber threats as a risk for national security and sovereignty. It defines new priorities, such as prevention and response to cyber-attacks, and institutional changes needed to ensure national security.

In accordance with the recommendations of the "White Paper" in 2008, one of the three bodies, directly subordinate to the Prime Minister - the Secretariat General of National Defense (General Secretariat of Defense Nationale, SGDN) was renamed General of Defense and the Secretariat National Security Council (General Secretariat for Defense and Security National, SGDSN). These changes led to the enlargement of powers of the Secretariat - to provide conventional defense with armed forces - to the wider responsibilities of the security of the whole society in cases beyond the need to use only military forces by traditional or security agencies.

These larger powers reflected the need to protect society in newer times, more complex and more turbulent, especially given the probability increasing cyber-crimes committed by adversaries of the enemy state or non-systemic. In 2009, the General Directorate of Computer Security (DCSSI) has been transformed into the National Security Systems Agency information system (National Agency for Information Systems Security, ANSSI), and is now the body responsible for the safety of national information systems.

Focus on solving of the problem of increasing the likelihood of new cyber-attacks against the country is placed under the direct supervision of the Prime Minister, responsible for coordinating activities aimed at ensuring cybersecurity at the national level for key companies and government agencies, including military forces. Since 2011, ANSSI has also been the national body responsible for the defense of information systems and networks in the public and private sectors.

Following the creation of this organization, the first cyber strategy was published in France in 2011: "Defense and security of the systems information: the strategy of France". This strategy has four main objectives: to provide global leadership in cyber defense, protect the decision-making apparatus in France by protecting sovereign information, increase the level of cyber security of elements of critical infrastructure and ensure security in cyberspace.

The 2013 White Paper on National Defense and Security was a revised version of this 2008 document and put special emphasis on the threat of cyber sabotage with respect to infrastructure critics.

In 2015, the French government published a second strategy National Security Council - "National Security Strategy of France", as its response to the increase in the number and the severity of cyber-attacks in various areas. On the basis of previous documents in the field of security, as well as the experience in the implementation of the previous digital strategy, the new strategy in 2015 announced its intention to transform France into a "digital republic", recognizing that ICT - is both a source of economic growth and innovation, and a cyber-risk elevation. The new strategy calls on the government to create means to protect the fundamental interests of France in cyber space, to protect national information systems, as well as critical infrastructure elements. In general, the strategy of cyber security of France has five key objectives for creation a "digital republic", while ensuring the security and flexibility of ICT systems. These five strategic priorities include:

1) protection fundamental interests of France in cyberspace - such as the government information systems and infrastructure elements critics;

2) to ensure mutual trust, privacy and the protection of personal data in the network through product development for cybersecurity, as well as providing legal and technical assistance in this domain;

3) to raise awareness of cybersecurity issues and strengthen national capacities in this area;

4) development of favorable atmosphere for the development of entrepreneurial activities, ICT investments and innovative business;

5) development of a "roadmap" to achieve strategic digital European autonomy.

Список використаних джерел

1. Ssi.gouv.fr[Електронний ресурс]. – Код доступу: https://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-decyberdefense-et-cybersecurite.

2.Ssi.gouv.fr[Електронний ресурс]. - Код доступу: https://www.ssi.gouv.fr/agence/cybersecurite/mois-de-la-cybersecurite-2017.

3. Potomacinstitute[Електронний ресурс]. - Код доступу: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

4. Diplomatie.gouv.fr[Електронний ресурс Electronic resource]. - Код доступу: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/defense-etsecurite/cybersecurite.

5. How to work.[Електронний ресурс Electronic resource]. - Код доступу: http://www.commentcamarche.net/contents/1235-virus-informatique.

Удовицька Я.,
курсант ННІ № 1 Національної академії внутрішніх справ
Консультант з мови: **Хоменко О.Ю.**

FIGHTING MONEY LAUNDERING: UNITED KINGDOM EXPERIENCE

What is Money Laundering?

Criminal activities, such as drug trafficking, smuggling, human trafficking, corruption and others, tend to generate large amounts of profits for the individuals or groups carrying out the criminal act. However, by using funds from such illicit sources, criminals risk drawing the authorities' attention to the underlying criminal activity and exposing themselves to criminal prosecution. In order to benefit freely from the proceeds of their crime, they must therefore conceal the illicit origin of these funds. [1]

The UK community has made the fight against money laundering and the financing of terrorism a priority. Among the goals of this effort are: protecting the integrity and stability of the financial system, cutting off the resources available to terrorists, and making it more difficult for those engaged in crime to profit from their criminal activities. The UK's unique blend of universal membership, surveillance functions, and financial sector expertise make it an integral and essential component of international efforts to combat money-laundering and the financing of terrorism. The