The second is the issues with Irish borders. The EU tabled a paper which suggested that Northern Ireland may need to stay in the EU customs union if there are no checks at the border. That is something which Britain cannot accept as it would effectively create a border between Northern Ireland and the rest of the UK.

The third and probably the most important issue is the money the UK owes to the EU because of long and short-term financial UK commitments made while an EU member. The UK could, in theory, walk away from the EU without paying any money at all. Leading Brexiteers are fond of saying that there is no legal obligation on the UK to pay anything at all to the EU as it departs. There is no deal under the Article 50 that is almost certainly correct as a strictly legal interpretation. And "no deal" on money would also mean "no deal" on any other issues either.

To sum up, it is worth noting that the EU is also going to lose due to the UK withdrawal. Thus, we have an opportunity to discuss some of the main losses of the EU as well.

T. Milach
Т. А. Милач
БГУ (Минск)
Научный руководитель И. А. Таранда

CYBERSECURITY IN INTERNATIONAL LAW

КИБЕРБЕЗОПАСНОСТЬ В МЕЖДУНАРОДНОМ ПРАВЕ

The topic of this research is very relevant in connection with the fact that the current stage of development of society is characterized by an extremely high role of computer technologies. All these things require the development of special acts that take into account the informatization factor. But, unfortunately, the law doesn’t always manage to develop quickly in response to the challenges thrown to it by changes in the world.

In order to understand the phenomenon of cybersecurity itself better, it is necessary to correlate such concepts as cyber attack, cyber crime and cyber war.

The common element of all these concepts is that they are all carried out via computer networks.

The differences are the subjective composition: the cyber attack (and hence the cyber war) is carried out by the state in the name of its bodies or appropriated to it in accordance with the rules of appropriation of behavior. Cyber crime, by contrast, is carried out by private actors.

Analysis of the international experience of legal provision of cybersecurity shows that the development of this problem in the world community is mainly in the following areas: the protection of individual rights in the information sphere, the protection of public interests, the protection of business and financial activities and the protection of information against computer crimes.

To ensure their information security by the end of the XIX century, almost all leading European countries have adopted their laws against espionage.

In international law, there are two principles that are subsequently reflected in municipal law on computer science:

- The establishment of limits to interference with privacy using computer systems;
- The introduction of administrative mechanisms to protect citizens from such interference.

Also at the 55th session of the UN General Assembly in October 2000, the next report of the UN Secretary General on "Advances in the field of information and telecommunications in the context of international security" was presented.

The main idea of the document is formulated in the provisions of Principle 1, according to which the activities of each state in the information space should contribute to the overall progress and not contradict the task of maintaining world stability and security, the interests of the security of other states, the principles of non-use of force, non-interference in internal affairs, respect for human rights and freedoms.

Thus, summing up all of the above, in parallel with the development of an international legal regime for information security, it is necessary to coordinate national laws regulating information activities of states. Moreover, over the past decade in many countries of the world, great legislative work has been done to develop legal documents aimed at combating computer crime and other aspects of using the global information space.

As a result of my the research I'd like to suggest: establishing the UN Cybersecurity Agency (UNCSA), calling the UNCSA to create a draft Convention on Cyberspace with the help of the group of international experts, inviting the UNCSA to conduct regular meetings and consultations of states to discuss the questions of cybersecurity and cyber warfare, making the key conclusions of the meetings publicly available with the consent of participating states, creating a special committee within the UNCSA that will investigate alleged violations of international law in cyberspace with the consent of the States cyber networks or infrastructure of which are required for the investigation and provide states with relevant recommendations.