DOI: 10.46340/eppd.2021.8.1.7

Viktoriia Muzyka
ORCID ID: https://orcid.org/0000-0002-6907-0280
National University «Odesa Law Academy», Ukraine

EU POLICY TOWARDS PROVIDING CYBER RESILIENCE OF CRITICAL INFRASTRUCTURE IN THE CONTEXT OF INTERNATIONAL SECURITY

Вікторія Музика
Національний університет «Одеська юридична академія», Україна

ПОЛІТИКА ЄС ЩОДО ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В КОНТЕКСТІ МІЖНАРОДНОЇ БЕЗПЕКИ

The article analyzes the European Union's Cybersecurity Strategy for the Digital Decade presented by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy at the end of December 2020. It discusses the efficiency of external policy areas enshrined therein, as well as the outcomes of the the European Union's cyber diplomacy toolbox option first ever applied – sanctions. Within the scope of the research, a few principal conclusions are reached. First, the European Union's Cybersecurity Strategy foresees the creation of a European Cyber Shield, which will be a network of security operations centers across the Union, to increase the cyber resilience of critical infrastructure. Moreover, it is important that "critical infrastructure" encompasses a quite broad understanding of sectors that provide essential services, such as transport, energy and health, telecommunications, finance, security, democratic processes, space and defense, both public and private. Second, all the strategic directions are aimed at the creation of global capacities to detect, recognize and respond to various cyber threats, and at making critical infrastructure more cyber resilient to malicious activity in cyberspace. For this end, efficient partnership between public and private sectors that foresees information-sharing and cooperation should be established. Finally, this article concludes that the Union plays a key role in promoting responsible state behavior in cyberspaces. It not only endorses the existing binding and non-binding rules, but also advances technological sovereignty and cooperation with various stakeholders – international organizations, both universal and regional, public and private sectors, academia and civil society in the context of international security.
Keywords: EU's Cybersecurity Strategy, cyberattacks on critical infrastructure, cyber resilience, cyber shield, partnership between public and private sectors.

Постановка проблеми. Проблема захисту об'єктів критичної інфраструктури з'явилась в повістці європейських інституцій ще на початку двадцять першого століття. Після атаки 11 вересня 2001 року в Сполучених Штатах Америки і терактів на території Європейського Союзу – 2004 року в Мадриді та 2005 року в Лондоні, Європейська Комісія розпочала дискусію, присвячену питанням захисту критичної інфраструктури, оскільки від нормального функціонування таких об'єктів залежить як життя людей, так і національна та міжнародна безпека[1].

Наразі можливості, які надає кіберпростір та інформаційно-комунікаційні технології, змінили спосіб функціонування урядів, бізнесу, вплинули на життя людей та міждержавні відносини в цілому.

[1] Setola, R., Luiijf, E., Theocharidou M. (2016) Critical Infrastructures, Protection and Resilience. In: Setola R., Rosato V., Kyriakides E., Rome E. (eds) *Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control*, *90*, Springer, 1-18; COM (2001) 298, *Network and Information Security: Proposal for A European Policy Approach* (European Commission), 6 June 2001 <https://ec.europa.eu/transparency/regdoc/rep/1/2001/EN/1-2001-298-EN-F1-1.Pdf> (2021, січень, 25).

Порівняно недавнє «народження» кіберпростору змінило динаміку та характер глобальних загроз. Так, наприклад, зловмисна діяльність у вигляді кібератак, попри свій віртуальний характер, може призвести до серйозних кінетичних наслідків. Нові можливості кіберпростору та загрози, пов'язані з його використанням, також фактично встановили знак рівності між державними та недержавними кіберакторами, що змусило членів міжнародної спільноти змінити підхід до питання кібербезпеки, зокрема задля підвищення кіберстійкості критичної інфраструктури.

Зобов'язання та відповідальність держави і приватного сектору, а також конвергенція їх знань та навичок в питаннях кібербезпеки переконали політиків перейти від державо центризму до ідеї партнерства між державами та приватним сектором з ціллю мінімізації наслідків, попередження кібероперацій і зміцнення міжнародної безпеки. З огляду на прогресивну позицію Європейського Союзу в питаннях, пов'язаних з кібербезпекою, актуальним є дослідження напрямів діяльності ЄС та його спрямованість на забезпечення кіберстійкості критичної інфраструктури, що досить часто досягається за рахунок партнерства з приватним сектором. Крім того, факт лідерства ЄС в питаннях кібербезпеки викликає потребу проаналізувати основі положення прийнятої наприкінці 2020 року Стратегії кібербезпеки ЄС.

Формулювання цілей статті. Метою дослідження є проведення аналізу напрямів діяльності ЄС щодо забезпечення кіберстійкості критичної інфраструктури в контексті міжнародної безпеки, оцінка нової Стратегії кібербезпеки ЄС, а також ефективності застосування інструментарію кібердипломатії ЄС.

Виклад основного матеріалу. В грудні 2020 року Європейський Союз представив нову Стратегію кібербезпеки, яка передбачає підвищення стійкості секторів критичної інфраструктури та протидії кібератакам ззовні[1]. Під час презентації стратегії високий представник ЄС із закордонних справ і політики безпеки Жозеп Боррель зазначив, що «у минулому році зафіксовано близько 450 інцидентів, направлених на об'єкти європейської критичної інфраструктури, включаючи фінансовий та енергетичний сектори. З пандемією загроза стає все більш помітною. Лише минулого тижня на Європейське агентство з лікарських засобів був здійснений напад»[2].

Нова Стратегія кібербезпеки охоплює п'ять напрямків зовнішньої політики Європейського Союзу, серед яких основне місце займає лідерство в сфері формування норм щодо відповідальної поведінки держав в кіберпросторі та зміцнення довіри. Наразі ЄС має найкращі можливості для просування, координації та закріплення позицій держав-членів ЄС на міжнародній арені, тому цілком обґрунтованим є намагання ЄС виробити позицію щодо застосування міжнародного права в кіберпросторі. Зокрема, в Стратегії робиться акцент на подальшому сприянні дотримання Статуту ООН, міжнародного права прав людини та юридично не обов'язкових норм, правил та принципів відповідальної поведінки держав в кіберпросторі, розроблених Групою урядових експертів у 2015 році[3].

Для цього ЄС спільно з рядом інших держав запропонували Організації Об'єднаних Націй «Програму дій щодо підвищення відповідальної поведінки держави у кіберпросторі» («Programme of Action to Advance Responsible State Behavior in Cyberspace»)[4]. Пропозиція має на меті ліквідувати паралельні обговорення в Групі урядових експертів ООН з питань підвищення відповідальної поведінки держав в кіберпросторі в контексті міжнародної безпеки, в якій беруть участь представники 25 держав, і Відкритій робочій групі з питань розвитку ІКТ в контексті міжнародної безпеки, в якій беруть участь всі зацікавлені держави.

---

[1] European Commission (2021). *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient – Questions and Answers* <https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2392#cybersecurity> (2021, січень, 25).

[2] European Commission (2021). *Cybersecurity Strategy: Remarks by the High Representative/Vice-President Josep Borrell at the joint press conference with Vice-President Margaritis Schinas and Commissioner Thierry Breton* <https://eeas.europa.eu/headquarters/headquarters-homepage/90700/cybersecurity-strategy-remarks-high-representativevice-president-josep-borrell-joint-press_en> (2021, січень, 25).

[3] European Commission (2021). *The EU's Cybersecurity Strategy for the Digital Decade*, *Joint Communication to the European Parliament and the Council* <https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade> (2021, січень, 25).

[4] United Nations (2020). *The future of discussions on ICTs and cyberspace at the UN* <https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf> (2021, січень, 27).

Згідно з пропозицією Програма має стати єдиною, довгостроковою, всеохоплюючою та орієнтованою на прогрес платформою, тоді як реалізація та подальші заходи схвалюватимуться Генеральною Асамблеєю ООН. Відтак, взаємодія в рамках запропонованої Програми допоможе створити певні межі та політичні зобов'язання на підставі існуючих міжнародних рекомендацій, норм та принципів, які вже узгоджені та зокрема містяться у звіті Групи урядових експертів ООН за 2015 рік, прийнятому Резолюцією Генеральної Асамблеї ООН 70/237.

В контексті кібератак проти об'єктів критичної інфраструктури це означає підтримку закріплених в Резолюції Генеральної Асамблеї ООН 70/150 спеціальних норм та принципів, що наразі не мають обов'язкового характеру. Так, наприклад, згідно з пунктами 13 (h) та (g) держави повинні вживати відповідних заходів для захисту своєї критичної інфраструктури від загроз, створених в ході використання інформаційно-комунікаційних технологій (13(g)), а також реагувати на запити про допомогу інших держав, критична інфраструктура яких стала об'єктом зловмисних дій при використанні ІКТ. Тобто, мова йде про забезпечення кіберстійкості національної критичної інфраструктури та кіберстійкості критичної інфраструктури держав, що звертаються із запитом. Держави також повинні реагувати на відповідні прохання щодо пом'якшення зловмисної діяльності, спрямованої проти критичної інфраструктури іншої держави у випадку, коли джерело походження знаходиться в межах території держави, якій направлено запит (13 (h))[1].

Будучи прихильником зазначених в Резолюціях ООН норм, Європейський Союз в своїй Стратегії кібербезпеки від 2020 року не випадково робить акцент на кіберстійкості «усіх відповідних секторів, державних та приватних, що виконують важливу функцію в економіці та суспільстві»[2]. Для реалізації цієї цілі передбачається формування «європейського кіберщита», здатного виявляти та реагувати на потенційні загрози до того, як вони можуть завдати масштабної шкоди. В системі такого «щита» ключова роль належить центрам обміну інформацією та аналізу, командам реагування на випадки комп'ютерної небезпеки та операційним центрам безпеки. Останні функціонують не тільки на базі державних інституцій, а й створенні у ряді приватних компаній, некомерційних організаціях тощо. Тобто, побудова «європейського кіберщита» сприятиме обміну інформацією між державними та приватними структурами, а також більш швидкому та ефективному виявленні кіберзагроз для їх подолання. Такий підхід є послідовним продовженням реалізації ідеї партнерства між приватним та публічним секторами заради підвищення кіберстійкості критичної інфраструктури, адже переважна більшість мережевих та інформаційних систем належить приватному сектору. Відтак, посилення взаємодії з ним є надзвичайно важливим напрямом діяльності. Якщо приватний та публічний сектори будуть розвивати технічні можливості щодо кіберстійкості, а потім обмінюватимуться передовим досвідом та інформацією, – кіберщит стане не тільки ефективним механізмом захисту від кіберзагроз в контексті міжнародної безпеки, а також інструментом взаємодії для встановлення відповідальних за кібератаки акторів.

В Програмі дій ЄС щодо підвищення відповідальної поведінки держави у кіберпросторі також передбачається необхідність активізувати співпрацю та розбудову потенціалу, а також організувати консультації з іншими зацікавленими сторонами, регіональними організаціями та установами ООН, приватними компаніями, неурядовими організаціями, громадянським суспільством, представниками інших інституцій ООН та відповідними багатосторонніми ініціативами, що займаються проблемами, пов'язаними з питаннями кібербезпеки у контексті міжнародної безпеки[3]. Європейський Союз планує налагодити структурований обмін з такими регіональними організаціями як Африканський союз, регіональний форум АСЕАН, Організація американських держав та Організація безпеки та співробітництва в Європі[4]. Беручи участь у таких організаціях як ООН і НАТО та шляхом взаємодії

[1] United Nations (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* <http://undocs.org/A/70/150> (2021, січень, 24).
[2] European Commission (2020). *The EU`s Cybersecurity Strategy for the Digital Decade*, *Joint Communication to the European Parliament and the Council* <https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade> (2021, січень, 25).
[3] United Nations (2020). *The future of discussions on ICTs and cyberspace at the UN* <https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf> (2021, січень, 27).
[4] European Commission (2020). *The EU's Cybersecurity Strategy for the Digital Decade*, *Joint Communication to the European Parliament and the Council* <https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade> (2021, січень, 25).

з вище перерахованими регіональними організаціями, ЄС фактично прагне встановити універсальні «правила гри в кібепросторі» та принципи відповідальної поведінки держави при його використанні, співпрацювати, обмінюватися досвідом та найкращими практиками, а також розробити відповідні засоби для вирішення загроз та викликів, пов'язаних з кібербезпекою.

Серед напрямів зовнішньої політики в Стратегії ЄС зазначається і такий напрям як «Співпраця ЄС у галузі кіберзахисту та ініціативи з розвитку можливостей», що передбачає використання потенціалу кіберпроектів в межах Постійного структурованого співробітництва (PESCO), зокрема «Кіберкоманд швидкого реагування та взаємодопомоги». Основне завдання таких кіберкоманд полягає у забезпеченні більш високого рівня кіберстійкості та колективного реагування на кіберінциденти. При цьому, кіберкоманди будуть оснащені розробленим інструментарієм для виявлення, розпізнавання та мітігації кіберзагроз.

В свою чергу, спільний кіберпідрозділ («Joint Cyber Unit») стане центром оперативного співробітництва ЄС з питань кібербезпеки. Цей підрозділ буде співпрацювати з державами-членами та відповідними установами, органами та агентствами ЄС, включаючи ENISA, CERT-EU та Європол, з метою просування поступового та всеохоплюючого підходу. Отже, підрозділ може сприяти подальшій співпраці між учасниками певної кіберспільноти, де учасники цього потребують.

Значного прогресу Європейський Союз також досяг в сфері реагування на кібератаки, яка є частиною зовнішньополітичного напряму «Інструментарій з кібердипломатії» («Cyber Diplomacy Toolbox»). Інструментарій включає реагування у формі політичних декларації, демаршів та діалогу, а також застосування таргетованих санкцій. Важливо, що Європейський Союз уже почав застосовувати санкції, і в новій Стратегії мова йде про можливість розширення інструментарію.

30 липня 2020 року Рада Європейського Союзу вперше ввела санкції проти фізичних та юридичних осіб, причетних до кібератак, що загрожують Європейському Союзу та походять з Союзу або інших держав, що не входять в його склад. Обмежувальні заходи зачепили шість індивідів та три юридичні особи, пов'язані з такими кібератаками як «WannaCry», «NotPetya», «Operation Cloud Hopper» та кібератаки проти Організації із заборони хімічної зброї. Введені санкції передбачають заборону на виїзд, замороження активів та заборону для осіб і структур ЄС надавати кошти тим, хто перерахований в рішенні[1]. Ще дві фізичні та одна юридична особи були додані рішенням Ради ЄС в жовтні 2020 року[2].

Найважливішим для України є наявність в списку Головного центру спеціальних технологій Головного Управління Збройних сил Російської Федерації (військова частина 74455, що знаходиться за адресою вул. Кірова, 22, м. Москва). Була встановлена відповідальність центру за кібератаки, що завдали значної шкоди та становили зовнішню загрозу для Європейського Союзу або його держав-членів, а також за кібератаки зі значним ефектом проти третіх держав, включаючи такі кібератаки як «NotPetya» або «EternalPetya» у червні 2017 року та кібератаки, спрямовані проти українських енергосистем взимку 2015 та 2016 років.

Враховуючи те, що їх ціллю були вразливості комп'ютера, кібератака «*NotPetya*» або «*EternalPetya*» зробила дані недоступними для ряду компаній в ЄС, Європі та в усьому світі. Блокування доступу до таких даних спричинило, серед іншого, значні економічні втрати. А кібератака на українську електромережу призвела до відключення її частин взимку.

Такий висновок та його офіційне опублікування є важливим кроком на шляху встановлення відповідальності держав за кібератаки. Разом з тим, цільові обмежувальні заходи мають стримуючий

[1] EUR-Lex (2020). *Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (ST/9564/2020/INIT)* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020D1127> (2020, грудень, 20); EUR-Lex (2020). *Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (ST/9568/2020/INIT)* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2020.246.01.0004.01.ENG&toc=OJ:L:2020:246:TOC> (2020, грудень, 20).

[2] EUR-Lex (2020). *Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020D1537> (2020, грудень, 20); EUR-Lex (2020). *Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.LI.2020.351.01.0001.01.ENG> (2020, грудень, 20).

і попереджувальний характер, тому, як зазначається в прес-релізі Ради ЄС, «їх слід відрізняти від присвоєння відповідальності державі»[1]. Залишається не зрозумілим, який ефект має таке «застереження», оскільки Головний центр спеціальних технологій Головного Управління Збройних сил Російської Федерації є офіційним державним органом, уповноваженим на виконання урядових функцій в області оборони та розвідки. Навіть, якщо допустити, що кібератака є актом *ultra vires*, вона в будь-якому випадку атрибутується державі. Але таке припущення є безпідставним, оскільки Головний центр спеціальних технологій ГУЗС РФ є виконавчим органом і органом управління Міністра оборони та Генерального штабу Збройних сил РФ. Наряд чи можна прийти до висновку стосовно необізнаності Міністра оборони та Генерального штабу Збройних сил РФ щодо запланованих Головним центром спеціальних технологій кібератак проти України, і їх здійснення без відома суб'єктів, яким центр підпорядковується.

Попри те, що Рада ЄС намагається відокремити відповідальність цілого державного органу від відповідальності держави, таке рішення може зіграти позитивну роль при вирішення спорів між Україною та Російською Федерацією, адже за загальним правом відповідальності – поведінка *de facto* та *de jure* державних органів, уповноважених на виконання урядових функцій, атрибутується останній. Що ж стосується санкцій, то Верховний представник прагне розглянути пропозиції щодо розширення заходів реагування в межах набору інструментів кібердипломатії, включаючи можливість застосування додаткових обмежувальних заходів, шляхом прийняття рішення про їх застосування кваліфікованою більшістю держав-членів Європейського Союзу[2]. В будь-якому випадку, конкретний приклад демонструє можливості ЄС щодо встановлення відповідальних осіб за здійсненні кібератаки проти об'єктів критичної інфраструктури, а також перспективність інструментарію кібердипломатії.

Висновки. З огляду на здійснений аналіз, видається, що Європейський Союз має намір всіляко заохочувати відповідальну поведінку в кіберпросторі, шляхом підвищення поваги до міжнародного права та не обов'язкових для виконання норм відповідальної поведінки в кіберпросторі.

Загалом діяльність Європейського Союзу в сфері виявлення та реагування на кіберзагрози демонструє принципово важливу позицію цього об'єднання до взаємодії з приватним сектор задля обміну інформацією та формування «європейського щита» кіберстійкості критичної інфраструктури. Залучення різноманітних кібераторів, співпраця з ООН, НАТО та регіональними організаціями, які зазначені в Стратегії, сприятиме мітігації існуючих кіберзагроз, а також створенню універсальної системи виявлення та реагування на зловмисну діяльність в кіберпросторі.

Що ж до ефективності інструментарію кібердипломатії, то факт встановлення відповідальних осіб в межах Європейського Союзу є однозначно позитивним кроком, який підкреслює неможливість безкарності за кібератаки на об'єкти критичної інфраструктури держав, які є джерелом основних послуг, а значить – забезпечення прав та свобод людини і нормального функціонування держав.

References:

1. Council of the EU (2020). *EU imposes the first ever sanctions against cyber-attacks* <https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/pdf> (2021, January, 25). [in English].
2. EUR-Lex (2020). *Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (ST/9564/2020/INIT)* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020D1127> (2020, December, 20). [in English].
3. EUR-Lex (2020). *Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020D1537> (2020, December, 20). [in English].
4. EUR-Lex (2020). *Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*

[1] Council of the EU (2020). *EU imposes the first ever sanctions against cyber-attacks* <https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/pdf> (2021, січень, 25).

[2] European Commission (2020). *The EU`s Cybersecurity Strategy for the Digital Decade*, *Joint Communication to the European Parliament and the Council* <https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade> [in English]. (2021, січень, 25).

(ST/9568/2020/INIT) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2020.246.01.0004.01.ENG&toc=OJ:L:2020:246:TOC> (2020, December, 20). [in English].
5. European Commission (2020). *The EU`s Cybersecurity Strategy for the Digital Decade*, *Joint Communication to the European Parliament and the Council* <https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade> (2021, January, 25). [in English].
6. European Commission (2021). *Cybersecurity Strategy: Remarks by the High Representative/Vice-President Josep Borrell at the joint press conference with Vice-President Margaritis Schinas and Commissioner Thierry Breton* <https://eeas.europa.eu/headquarters/headquarters-homepage/90700/cybersecurity-strategy-remarks-high-representativevice-president-josep-borrell-joint-press_en> (2021, January, 25). [in English].
7. European Commission (2021). *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient – Questions and Answers* <https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2392#cybersecurity> (2021, January, 25). [in English].
8. European Commission (2021). *The EU's Cybersecurity Strategy for the Digital Decade*, *Joint Communication to the European Parliament and the Council* <https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade> (2021, January, 25). [in English].
9. Setola, R., Luiijf, E., Theocharidou M. (2016) Critical Infrastructures, Protection and Resilience. In: Setola R., Rosato V., Kyriakides E., Rome E. (eds) *Managing the Complexity of Critical Infrastructures*. *Studies in Systems, Decision and Control*, *90*, Springer, 1-18; COM (2001) 298, *Network and Information Security: Proposal for A European Policy Approach* (European Commission), 6 June 2001 <https://ec.europa.eu/transparency/regdoc/rep/1/2001/EN/1-2001-298-EN-F1-1.Pdf> (2021, January, 25). [in English].
10. United Nations (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* <http://undocs.org/A/70/150> (2021, January, 24). [in English].
11. United Nations (2020). *The future of discussions on ICTs and cyberspace at the UN* <https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf> (2021, January, 27). [in English].
12. UR-Lex (2020). *Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.LI.2020.351.01.0001.01.ENG> (2020, December, 20). [in English].