DOI: 10.35774/app2020.01.128
УДК 347.83:34:002.1

Тетяна Сліпченко,
кандидат економічних наук, доцент кафедри безпеки, правоохоронної діяльності та фінансових розслідувань Тернопільського національного економічного університету
ORCID: https://orcid.org/0000-0001-9679-6231

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА СИСТЕМИ ЗАХИСТУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ЄВРОПЕЙСЬКИЙ ДОСВІД

Досліджено передумови й особливості формування законодавства України у сфері кібербезпеки, визначено проблеми та перспективи його подальшого розвитку з точки зору оцінбвання наявних небезпек та загроз. Окреслено напрями адаптації чинного законодавства про кібербезпеку до стандартів ЄС у межах реалізації положень Угоди про асоціацію між Україною та ЄС. Проаналізовано досвід європейських країн щодо законодавчого забезпечення у сфері кібербезпеки, доведено доцільність розвитку договірного державно-приватного партнерства в сфері захисту кіберпростору. Визначено напрями розвитку національної системи кіберзахисту: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки.

Ключові слова: *інформаційна безпека, кіберпростір, кібербезпека, договірне державно-приватне партнерство, імплементація міжнародних норм.*

Бібл.: 10.

Слипченко Т.

Кибербезопасность как составляющая в системе защиты национальной безопасности: европейский опыт

Исследовано предпосылки и особенности формирования законодательства Украины в сфере кибербезопасности, определены проблемы и перспективы его дальнейшего развития с точки зрения оценки имеющихся опасностей и угроз. Очерчено направления адаптации действующего законодательства о кибербезопасности со стандартами ЕС в рамках реализации положений Соглашения об ассоциации между Украиной и ЕС. Проанализирован опыт европейских стран по законодательному обеспечению в сфере кибербезопасности, доказана целесообразность развития договорного государственно - частного партнерства в сфере защиты киберпространства. Определены направления развития национальной системы киберзащиты: совершенствование правовой основы киберзащиты объектов критической инфраструктуры; внедрение системы независимого аудита информационной безопасности; развитие международного сотрудничества в сфере обеспечения кибербезопасности.

Ключевые слова: *информационная безопасность, киберпространство, кибербезопасность, договорное государственно - частное партнерство, имплементация международных норм.*

Slipchenko T.

Cyber Security as a Component of National Security Protection System: European Experience

The fundamental consequence of the global informatization of state structures was the emergence of a fundamentally new environment of confrontation between competing states-cyberspace. The use of the Internet and information technology opens up endless opportunities for humanity, but also poses new serious threats. Increasing the number of cyber threats to the economic component of our country makes the issue of optimization of legal regulation of this sphere more relevant.

According to ISO / IEC 27032: 2012, cybersecurity is the preservation of the integrity, confidentiality and accessibility of information circulating in the cybersystem (that is, information fed into the cybersystem, accumulated and stored in it for further processing) ensuring the stability and continuity of the system's implementation of management functions by cybersystem with respect to the respective objects.

The purpose of the research is to comprehensively assess the state and trends of the development of the European Union's cybersecurity system in the context of globalization, to justify the ways and mechanisms of using the European experience in national security.

The most promising directions of development of the national cyber defense system, today, are as follows: improvement of the legal basis of cyber defense of critical infrastructure; implementation of the system of independent information security audit on critical infrastructure facilities; establishment of sectoral cyber incident response centers; development of international cooperation in the field of cybersecurity; development of cyber security training system; increasing digital literacy of citizens.

Keywords: *information security, cyberspace, cybersecurity, public and private partnerships, implementation of international standards.*

Постановка проблеми. Глобальна інформатизація активно впливає на функціонування держав світової спільноти, інформаційні технології застосовуються в процесі вирішення завдань забезпечення національної, військової, економічної безпеки. Водночас одним з фундаментальних наслідків глобальної інформатизації державних та приватних структур стало виникнення принципово нового середовища протиборства конкурентних держав – кіберпростору. Використання Інтернету та інформаційних технологій не тільки відкриває перед людством безмежні можливості, а й створює нові серйозні загрози. Все більше інформації переміщується в онлайн і за останніми підрахунками у світі вже понад 20 млрд пристроїв підключених до інтернету, що у кілька разів більше, ніж населення Землі. Також на серверах збирається мільярди гігабайт різної інформації. Світ стає відкритим, та таке стрімке зростання потребує формування «правил гри».

Збільшення кількості кіберзагроз на економічну соціальну складову нашої держави все актуальнішим робить питання оптимізації правового регулювання цієї сфери. В Києві контексті євроінтеграційних процесів важливою для України є демонстрація того, що ми готові протистояти загрозам того виду злочинності, що найбільш стрімко зростає. Окрім того, в сучасних умовах важливою є готовність приймати необхідні зміни, що відповідатимуть стандартам, встановленим на європейському та світовому рівнях.

Аналіз останніх досліджень і публікацій. Проблеми кібербезпеки та результати запровадження європейського досвіду в систему захисту національної безпеки України відображені в наукових працях таких вчених, як: О. О. Баєв, Г. Р. Бєляков, Дж. Блумбекер, Г. П. Власова, В. Д. Гавловський, Р. Є. Джансараєва, В. Б. Дзюндзюк, Н. В. Кардава, О. В. Манжай, В. В. Марков, М.А. Ожеван, Ю. М. Онищенко, О. В. Орлов, П. І. Пушкаренко, Є. Д. Скулиш, В. Г. Хахановський, В. В. Черней та ін.

Нормативною базою дослідження є Конституція України, Кримінальний кодекс України, Кримінально процесуальний кодекс України, Цивільний кодекс України, Господарський кодекс України, Конвенція про кіберзлочинність, Закони Верховної Ради України, рішення Конституційного Суду України, рішення Європейського суду з прав людини, які стосуються боротьби з організованою кіберзлочинністю, законодавство зарубіжних держав частині захисту свого кіберпростору.

Незважаючи на наявність великої кількості наукових праць із зазначеної проблематики, чимало питань все ще є нерозкритими або вирішеними фрагментарно.

Мета дослідження полягає в комплексному оцінюванні стану і тенденцій розвитку системи кібербезпеки Європейського Союзу в умовах глобалізації, обґрунтуванні шляхів і механізмів використання європейського досвіду в забезпеченні національної безпеки.

Виклад основного матеріалу дослідження. Явище «безпека» нерозривно пов'язане з поняттям «національні інтереси» і, можливо, в якомусь сенсі є похідним від нього, тому що, перш за все, функція національної безпеки – це забезпечення гарантій невразливості найголовніших інтересів національного суверенітету, територіальної цілісності держави, захисту населення – тих інтересів, через які держава бореться і не погоджується на поступки. Національна безпека – це стратегія, необхідна для забезпечення інтересів держави [5, с. 37]. На сьогодні поняття кібербезпеки багатогранне, тому доволі важко формалізується. Наявність правильного формулювання поняття кібербезпеки є вкрай важливим для окреслення головних цілей роботи різних структур і подальшого захисту кіберпростору від загроз.

В сучасних умовах питання кібербезпеки виходять з рівня захисту інформації на окремому об'єкті обчислювальної техніки на рівень створення єдиної системи кібербезпеки держави як складової частини системи інформаційної та національної безпеки, що відповідає за захист не тільки інформації у вузькому сенсі цього слова, а й усього кіберпростору. Кіберпростір можна визначити, як «метафоричну абстракцію, яка використовується в філософії і в комп'ютерній технології, яка є віртуальною реальністю, представляє неосферу, другий світ як «всередині» комп'ютерів, так і «всередині» комп'ютерних мереж» [5, с. 43].

Згідно із стандартом ISO/IEC 27032:2012, кібербезпека, безпека кіберпростору (cybersecurity, cyberspace security) – збереження цілісності, конфіденційності та доступності інформації, що циркулює

в кіберсистемі (тобто інформації, що надходить у кіберсистему, накопичується та зберігається в ній для подальшої обробки), з метою забезпечення стійкості і безперервності реалізації кіберсистемою управлінських функцій щодо відповідних об'єктів управління. Відповідно, кіберпростір – частина інформаційного простору, утворена інформаційними потоками й інформаційними полями, що породжуються в процесі функціонування кібернетичних систем [5, с. 45].

Говорячи про вирішення проблем кібербезпеки, необхідно враховувати доволі важливий її аспект – взаємозв'язок між учасниками, тобто користувачами, який може привести до синергетичного ефекту. Необхідні ретельні дослідження властивостей кіберпростору, динаміки його розвитку, методів управління цією динамікою. Вкрай складно, практично неможливо побудувати дійсно ефективну систему кібербезпеки без її системного аналізу, тому доцільно включити в комплекс досліджень у галузі кібербезпеки такі напрямки, як:

– вироблення єдиної термінології кібербезпеки і кіберпростору;

– розробка системи показників функціонування кіберпростору, а також його захисту від потенційних загроз;

– розробка моделей кіберпростору і факторів, що впливають на його функціонування;

– створення спеціальних методів забезпечення стійкості кіберпростору при впливі загроз;

– створення інтелектуальних методів забезпечення кібербезпеки (метод ситуаційного аналізу стану інформаційної безпеки, нові методи криптографічного захисту, інтелектуальні методи виявлення вторгнень у системи, методи інтелектуальної ідентифікації користувачів при кібератаці) [4, с. 144].

Європейський союз загалрм і окремі європейські держави серйозно стурбовані своєю кібербезпекою. Кіберстратегії ЄС і країн, які входять до нього, акцентують увагу на необхідності спільних зусиль держави, суспільства, бізнесу і всіх громадян у сфері боротьби з кіберзагрозами.

Останнім часом змінюється ієрархія пріоритетів у сфері кібербезпеки. Якщо на початку XXI ст. на перший план виходили проблеми боротьби з міжнародними терористичними організаціями, а також питання безпеки промислової інфраструктури, то останнім часом практично всі європейські країни стурбовані можливим втручанням хакерів в їхні виборчі кампанії. Кіберстратегія багатьох європейських держав допускає не тільки оборонні, а й наступальні дії в кіберпросторі.

У 2013 р. Європейський Союз ухвалив Стратегію кібербезпеки, метою якої є відкритий, надійний і безпечний кіберпростір. Для цього передбачені заходи з таких напрямків: досягнення кіберстійкості, суттєве скорочення кіберзлочинності, розробка політики кібероборони, пов'язаної зі Спільною політикою безпеки і оборони, розвиток виробничих і технологічних ресурсів для кібербезпеки, створення узгодженої міжнародної політики кіберпростору для ЄС і просування основних цінностей ЄС. Одразу після оприлюднення Стратегії було розпочато роботу над відповідною директивою. Важливо наголосити, що цей документ розроблявся не окремо від інших напрямків, а як частина Стратегії Єдиного Цифрового Ринку (Digital Single Market Strategy), з одного боку, і частини Європейського порядку денного з питань безпеки (European Agenda on Security). Стратегія та Порядок денний були оприлюднені навесні 2015 р. в липні 2016 р. Європейська Комісія презентувала «Додаткові заходи по сприянню розвитку індустрії кіберзахисту», а 06.07.2016 р. була ухвалена Директива ЄС щодо заходів щодо забезпеченн високого загального рівня безпеки мережевих та інформаційних систем у всьому Європейському Союзі [8]. Кібербезпека – стратегічна проблема державної ваги, серед країн-членів Євросоюзу стратегії кібербезпеки прийняли: Швеція (2008 р.), Естонія (2008 р.), Фінляндія (2008 р.), Словаччина (2008 р.): Чехія (2011 р.), Франція (2011 р.), Німеччина (2011 р), Литва (2011 р.), Люксембург (2011 р.), Голландія (2011 р). Список країн наочно показує, що проблема кібербезпеки визнається важливою в усьому світі. Зокрема, Естонія є одним з європейських лідерів у сфері кібербезпеки. Саме в Талліні знаходиться Центр кіберзахисту НАТО. 25 листопада 2016 р., під час відвідування цього Центру, президент країни Керсти Кальюлайд заявила: «Не залишилося ні найменшого сумніву в тому, що кіберпростір як поле бою можна порівняти з морем, повітрям і водою» [4].

Естонія активно розвиває власні ресурси в сфері кібербезпеки. Так, в червні 2011 р. Центр розвитку державних інфосистем був перетворений в Департамент державної інформаційної системи, який займається розвитком державної інформаційної системи як єдиного цілого. Тільки в 2018 р. даний Департамент розглянув 9135 випадків в комп›ютерних мережах Естонії, з яких 348 впливали на роботу важливою адміністративної послуги або сторінки [4].

Європейський союз має унікальну можливість інвестувати в розширення співпраці і координації між державами-членами ЄС, а також ключовими зацікавленими сторонами ЄС в сфері кібербезпеки. Саме виходячи з цього, в 2016 році, Європейська комісія підписала з Європейською Організацією Кібербезпеки (ECSO) договірне державно - приватне партнерство. Перш за все, це сприяє структуруванню і координації

промислових ресурсів цифрової безпеки в Європі. Воно включає в себе широке коло учасників: виробників компонентів і обладнання, операторів основних послуг і дослідницьких інститутів, об›єднаних під егідою ECSO. ЄС зобов'язався інвестувати до 450 млн. євро в це партнерство [10].

В 2018 році Європейська Комісія заявила про створення мережі національних координаційних центрів з кібербезпеки і нового Європейського центру компетенції в галузі промислової, технологічної та дослідницької компетенції в області кібербезпеки [4].

На сьогодні ЄС стикнувся з проблемою нестачі кваліфікованих фахівців у сфері інформаційно-комунікаційних технологій і особливо експертів в області кібербезпеки. В пропозиції бюджету ЄС на 2021-2027 роки, робиться наголос на розвиток цифрових навичок, особливо в області кібербезпеки .

Європейська Комісія інвестувала понад 63,5 млн. євро в чотири пілотні проекти, щоб закласти основу для створення європейської мережі центрів експертизи з кібербезпеки, яка допоможе посилити дослідження та координацію кібербезпеки в ЄС. Чотири пілоти: CONCORDIA, ECHO, SPARTA та CyberSec4Europe, мають завдання внести напрацювання у спільну Європейську дорожню карту з питань кібербезпеки та інновацій після 2020 року та європейську Стратегію кібербезпеки для промисловості. Окрім того, вони допоможуть ЄС у визначенні та тестуванні моделей управління європейською мережею спеціалістів у сфері центрів передової технології в галузі кібербезпеки [4].

Правова база кібербезпеки України складається з міжнародних зобов'язань та національного законодавства. На міжнародному рівні слід виділити Будапештську конвенцію та Директиву щодо мережевої та інформаційної безпеки (NIS) [8].

У національному законодавстві мають знайти відображення зобов'язання, взяті на себе Україною як підписантом міжнародних угод і конвенцій, а також ті, які їй доведеться взяти, якщо вона й надалі демонструватиме прагнення вступити до Європейського Союзу. На національному рівні, Закон № 2163-VIII від 5 жовтня 2017 року «Про основні засади забезпечення кібербезпеки України» та Національна стратегія кібербезпеки України є основними документами, що регулюють дану сферу. Відсутність в українському законодавстві необхідної термінології, невизначеність питань щодо розподілу повноважень між різними державними та приватними установами в сфері кіберзахисту, відсутність законодавчо врегульованої та фінансово забезпеченої стратегії державно-приватного партнерства, невирішеність багатьох процедурних питань щодо дій правоохоронних та контролюючих органів, а також недостатня увага, що приділяється проблемам загальної освіти з кібербезпеки, підвищення обізнаності, нарощуванню потенціалу значно підвищують вразливість України перед кіберінцидентами та кібератаками. Необхідність законодавчого врегулювання перелічених питань вимагає прозорості законодавчого процесу, плідної співпраці українських та міжнародних стейкголдерів, сприяння підвищення довіри між ними.

Закон України «Про основні засади забезпечення кібербезпеки України» заклав загальну архітектуру національної системи кібербезпеки та розподіляє завдання та повноваження між основними суб'єктами забезпечення кібербезпеки (Національним координаційним центром кібербезпеки, Міністерством оборони, Генеральним штабом Збройних Сил, Державною службою спеціального зв'язку та захисту інформації, Службою безпеки України, Національною поліцією, Національним банком, розвідувальними органами України) [1].

Реалізація положень Стратегії кібербезпеки України та Закону України «Про основні засади забезпечення кібербезпеки України» передбачає розроблення та застосування якісно нового законодавства у сфері кібербезпеки, що засноване на напрацьованому за п'ять років гібридної війни досвіді, усвідомленні та імплементації досвіду та нормативних документів ЄС та НАТО.

Висновки. Аналізуючи стратегічні документи в галузі кібербезпеки європейських країн, можна зробити наступні висновки.

У середовищі, де постійно з'являються і еволюціонують кіберзагрози, країни – члени Євросоюзу при зустрічі з новими, глобальними загрозами мають намір проваджувати гнучкі, оперативні стратегії кібербезпеки. Транскордонний характер загроз змушує країни вступати в тісну міжнародну взаємодію. Співпраця на європейському рівні необхідна не тільки для ефективної підготовки до кібератак, але і для своєчасної реакції на них. Комплексна державна стратегія кібербезпеки – перший крок на цьому шляху. В межах стратегії в галузі кібербезпеки європейських країн найчастіше зустрічаються наступні рекомендації щодо вирішення основних питань в галузі кібербезпеки на короткострокову і середньострокову перспективу.

У короткостроковій перспективі:

– спроектувати, переоцінити і підтримувати державну стратегію кібербезпеки, а також заходи, що проводяться в рамках стратегії;

– чітко визначити рамки дії, цілі стратегії і саме тлумачення терміну «кібербезпека»;

– врахувати в стратегії інтереси промисловості, наукового суспільства і цивільних представників;

– переконатися, що в стратегії береться до уваги вже виконана робота з підвищення рівня безпеки національних і європейських інформаційних систем. Необхідно уникати дублювання заходів і сфокусуватися на нових проблемах;

– співпрацювати з іншими країнами, що входять в Євросоюз, а також з комісією Євросоюзу, щоб гарантувати узгоджений характер кібербезпеки;

– підтримати комісію Євросоюзу в справі створення Стратегії безпеки Інтернету.

У середньостроковій перспективі:

● домовитися про загальноприйняте тлумаченні терміну «кібербезпека» для того, щоб в подальшому сформулювати загальну мету для всього Євросоюзу;

● переконатися, що стратегії кібербезпеки Євросоюзу і його членів не суперечать цілям міжнародного співтовариства, а підтримують боротьбу з проблемами кібербезпеки на глобальному рівні;

● для реалізації стратегій кібербезпеки приватний і державний сектори повинні тісно співпрацювати. Співпраця повинна здійснюватися за допомогою обміну інформацією, передовими практиками (наприклад, в сфері управління інцидентами), а також навчаннями на національному та європейському рівнях [7, с. 8].

Найбільш перспективними напрямами розвитку національної системи кіберзахисту, на сьогодні, вважаємо: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури; створення галузевих центрів реагування на кіберінциденти; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки; розвиток системи підготовки кадрів у сфері кібербезпеки; підвищення цифрової грамотності громадян.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України: Закон України №2163-VIII від 05.10.2017 р. *Відомості Верховної Ради* (ВВР). 2017. № 45. 403 с.
2. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». 27.12.2016. №448. URL: http://online.budstandart.com/ ua/catalog/doc-page.html?id_doc=69128 (дата звернення: 02.02.2020).
3. Інформаційне насильство та безпека: світоглядно-правові аспекти: Монографія / Дзьобань О.П., Пилипчук В.Г. / За заг. ред. проф. В.Г. Пилипчука. Харків: Майдан, 2017. 244 с.
4. Кибербезопасность: рекомендации для ЕС. URL://http://www.lawtrend.org/in formation-access/blog-information-access/kiberbezopasnost-rekomendatsii-dlya-es (дата обращения: 02.02.2020).
5. Ліпкан В. А., Ліпкан О. С. Національна і міжнародна безпека у визначеннях та поняттях. навч.посіб. Вид 2-ге, перероб. і допов. Київ. 2018. 400 с.
6. Лук'янчук. Р. В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник Національної академії державного управління при Президентові України.* 2015. № 4. С. 50–56.
7. Пантин В. И., Кардава Н. В. Кибербезопасность: проблемы формирования единой политики в Европейском Союзе. *Вестник Пермского университета. Политология.* 2018. № 3 . С. 5–18.
8. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2017). URL://http:// eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (Last Accessed: 02.02.2020)
9. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cyber- security. URL: www.iso.org/standard/44375.html. (Last Accessed: 02.02.2020).
10. Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union.* L 151/15, 7.6.2019

References

1. Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: pryiniati 5 zhov. 2017 roku № 2163-VIII [Law of Ukraine on the basic principles of cyber security in Ukraine from October 10 2017, № 2163-VIII] (2017). *Vidomosti Verkhovnoi Rady (VVR*) - *Bulletin of Verkhovna Rada of Ukraine, 45,* 403 [in Ukrainian].

2. *Informatsiini tekhnolohii. Metody zakhystu. Nastanovy shchodo kiberbezpeky [Information Technology. Methots of protection. Cybersecurity Guidelines]*. Retrieved from http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128 [in Ukrainian].
3. Dzoban, O. P., & Pylypchuk, V. H. (2017). *Informatsiine nasylstvo ta bezpeka: svitohliadno-pravovi aspekty: Monohrafiia [Information violence and security: legal aspects: Monograph]*. Kharkiv [in Ukrainian].
4. *Kyberbezopasnost: rekomendatsyy dlia ES.[Cyber security: recommendations for the EU]*. Retrieved from http://www.lawtrend.org/in formation-access/blog-information-access/kiberbezopasnost-rekomendatsii-dlya-es [in Ukrainian].
5. Lipkan, V. A., & Lipkan, O. S. (2018). *Natsionalna i mizhnarodna bezpeka u vyznachenniakh ta poniattiakh [National and international security in definitions and concepts]*. Kyiv [in Ukrainian].
6. Lukianchuk, R. V. (2015). Mizhnarodne spivrobitnytstvo u sferi zabezpechennia kibernetychnoi bezpeky: derzhavni priorytety [International cooperation in the field of cyber security: national priorities]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy - Bulletin of the National Academy of Public Administration under the President of Ukraine, 4,* 50-56 [in Ukrainian].
7. Pantyn, V. Y., & Kardava, N. V. (2018). Kyberbezopasnost: problemы formyrovanyia edynoi polytyky v Evropeiskom Soiuze [Cyber security: the problems of forming a unified policy in the european union]. *Vestnyk Permskoho unyversyteta. Polytolohyia - Bulletin of Perm University. Political science, 3,* 5-18 [in Russian].
8. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2017)*. Retrieved from http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf [in English].
9. *ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity*. Retrieved from www.iso.org/standard/44375.html. [in English].
10. Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union*, L 151/15, 7.6.2019 [in English].

Стаття надійшла до редакції 25.02.2020.