інформацію про вразливі місця інфраструктури. Повна перевірка IT-обладнання, програмного забезпечення, мережі та компонентів даних становить основу для оцінювання вразливостей в IT-інфраструктурах, які можуть вплинути на внутрішню структуру. Системи та мережі, підключені до інтернету, наражаються на загрози, які не існують для автономних систем і мереж. Після того, як буде досягнуте належне розуміння IT-середовища, головний аудитор і група внутрішнього аудиту можуть виконати оцінювання ризиків і розробити план проведення аудиту.

Ключові слова: аудит, аудит інформаційних технологій, IT-аудит, IT-інфраструктура, ризики, план проведення аудиту.

work and data components. Systems and networks connected to the Internet are exposed to threats that do not exist for self-contained systems and networks. When thorough understanding of the IT environment has been achieved, the executive auditor and the internal audit group can perform the risk assessment and develop the audit plan.

Key words: audit, IT audit, IT infrastructure, risk, audit plan evolving.

УДК 35.746.1

СОЛОДКА Олена Маркіянівна

ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ ВЗАЄМОДІЇ ДЕРЖАВ У ГЛОБАЛЬНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Постановка проблеми. Двома ключовими характеристиками сучасного історичного періоду є глобалізація та інформаційно-комунікаційні технології. Останні виступають у ролі головної рушійної сили глобалізованих суспільств, в основі яких лежать знання та інформація, що привело до формування нового типу суспільного устрою – інформаційного суспільства, яке існує і розвивається на двох рівнях – національному та міжнародному. У міру його розвитку створюються умови для економічного зростання окремих країн, інтенсивного включення держав і цілих регіонів у світові інтеграційні процеси, формування єдиного інформаційного простору. Відтак зростає значущість інформації і знань, унаслідок чого економічний розвиток більшою мірою, ніж раніше, залежить від ідей і знань, а держави, які стимулюють технологічні інновації, посилюють свій вплив на міжнародній арені; розмиваються кордони між міжнародною та внутрішньою

політикою, між військовою і цивільною сферами; бізнес-структури, неурядові організації активно виходять на міжнародну арену; відбувається стиснення часу і простору тощо. Разом із тим в умовах відсутності загальноприйнятих правил взаємодії та забезпечення безпеки формуються національні, але не міжнародні правові ініціативи, що створює нові і загострює вже існуючі ризики та загрози для інформаційної безпеки, що й зумовлює потребу дослідження цих важливих питань.

Аналіз останніх досліджень і публікацій. У сучасній науковій літературі питання правового регулювання взаємодії держав в інформаційному просторі відображені у наукових працях І. Арістової, О. Баранова, О. Довганя, Б. Кормича, В. Пилипчука, О. Олійника, В. Цимбалюка, М. Швеця, Є. Макаренко та багатьох інших, проте розвиток інформаційної сфери потребує перманентного дослідження зазначених питань із метою вироблення адекватних сучасності правових заходів безпеки.

Метою статті є визначення характерних особливостей взаємодії держав у глобальному інформаційному просторі.

Виклад основного матеріалу. У глобальному вимірі правова основа функціонування інформаційного суспільства повинна гарантувати стабільність кіберпростору й водночас бути достатньо гнучкою, відображати зміни, викликані технічним прогресом, на нормативному рівні, не вдаючись, однак, до надмірної деталізації нормативних положень. Крім того, нормативно-правове забезпечення суспільних відносин у глобальному інформаційному суспільстві має бути стандартизованим, упроваджуючи глобальний регуляторний механізм, оскільки фрагментація нормативно-правового регулювання інформаційного суспільства на рівні національних правових систем може сприяти утворенню декількох центрів впливу та дискримінаційному становищу менш впливових політичних акторів. Проте, за оцінками фахівців, можлива певна сегментація глобального інформаційного суспільства (європейський, американський, азійський сегменти тощо), що проявлятиметься в адаптації універсальних стандартів до конкретних умов, пов'язаних із рівнем розвитку відповідного суб'єкта в межах певного регіону або наддержавного утворення. Загалом експерти розрізняють чотири можливі шляхи розвитку правового регулювання інформаційного простору [1]:

– «доктрина абсолютної свободи», яка відкидає ідею регулювання інтернет-ЗМІ та ЗМК, популярна передусім серед інтернет-користувачів. Водночас відкритий доступ до ресурсів глобального інформаційного суспільства має регулюватися з метою запобігання зловживанням, адже відсутність регуляторного механізму провокує ризики обмеження доступу до інформації та комунікації. Розглядаючи систему інформаційної безпеки західних країн, можна помітити, що більша частина інформаційної інфраструктури знаходиться в руках приватного сектору й керується ним, що призводить до формування такої мо-

делі взаємодії, коли держава встановлює свої правила, а громадяни, дотримуючись цих правил, роблять спроби убезпечити себе. Отже, сьогодні найгострішою проблемою щодо забезпечення безпеки в інформаційній сфері є зберігання великої кількості інформації про особисті дані громадян держав, які вони надають у глобальній мережі Інтернет. Персональні дані користувачів виступають певними параметрами, за якими можна оцінювати стан і динаміку розвитку суспільних систем, знаходити уразливі місця та здійснювати на них тиск. Звідси випливає, що інформація має глобальний характер. А персональні дані можна використовувати в різних цілях, зокрема й із метою накопичення та подальшого використання інформації для проведення пропаганди;

– «саморегулювання» – на користь цього підходу висловлюються переважно ІТ-компанії та виробники контенту, які вбачають у ньому передусім вирішення проблем, пов'язаних з образливим контентом та захистом прав користувачів. Однак, зважаючи на гостру проблематику захисту авторських прав та електронної торгівлі, навіть за умов саморегулювання існує необхідність у створенні впорядкованої правовими нормами структурованої мережі, у межах якої відбувалася б комунікативна активність;

– «закритий клуб» – цей підхід спрямований на заповнення прогалин у національному законодавстві, пов'язаних із вирішенням регуляторних питань. Зокрема відповідні рішення розробляються в межах Великої вісімки, СОТ, а також новими інституціями, що формуються в корпоративному секторі. Ризики такого підходу полягають у тому, що найсильніші економічно та розвинуті в технологічному плані суб'єкти можуть диктувати правила гри всім іншим, а ЗМІ та ЗМК сприйматимуться як бізнес, засоби розваги й тотального контролю над інформаційними ресурсами;

– «інституційний підхід», підґрунтям якого є демократизація глобального управління, що має відображення в деяких ініціативах ООН та концепції «космополітичної демократії», реалізується в процесах на зразок Всесвітнього саміту з інформаційного суспільства (ВСІС) і передбачає багатосторонню участь усіх зацікавлених суб'єктів у вирішенні питань, що їх безпосередньо стосуються, можуть стосуватися в майбутньому або, на їхнє переконання, є такими, що можуть прямо чи опосередковано зачіпати їхні інтереси.

Відповідні паралелі можливо провести, досліджуючи взаємодію держав в інформаційній сфері, зокрема в межах Європейського Союзу (ЄС). Так, формування єдиного цифрового простору в межах ЄС почалося з прийняттям Єврокомісією у 2015 році Стратегії Єдиного цифрового ринку ЄС [2], згідно з якою цифрова інтеграція ЄС передбачає три «стовпи» (напрямки) політики і, відповідно, правового регулювання: забезпечення якісного онлайн-доступу до цифрових послуг і товарів; формування цифрового середовища для розвитку цифрових послуг і цифрових мереж; розвиток цифровізації як драйвера зростання єдиної європейської економіки.

У Європейському Союзі актуальним є питання захисту персональних даних: аналітики звертають увагу, що транснаціональні компанії (Google, Apple, Facebook, Amazon і Microsoft) збирають величезні обсяги персональних даних для просування реклами, які до того ж можна використати з метою формування політичних уподобань, просування потрібних ідей. У 2016 році ЄС був уведений у дію Загальний регламент захисту персональних даних (General Data Protection Regulation – GDPR) [3], на підставі якого, зокрема, користувачі інтернету мають право знати, які дані збираються під час відвідування певного вебсайту. Регламент також вимагає, щоб дані цих користувачів не виходили за межі ЄС у будь-якому вигляді.

Крім того, ухвалено Стратегію кібербезпеки ЄС на цифрове десятиліття [4], яка є ключовим компонентом формування цифрового майбутнього Європи, Плану Єврокомісії щодо відновлення Європи, Стратегії Союзу безпеки на 2020–2025 роки, Глобальної стратегії зовнішньої політики та політики безпеки ЄС і Стратегічного порядку денного Європейської Ради на 2019–2024 роки та визначає, яким чином ЄС захищатиме своїх громадян, підприємства й установи від кіберзагроз і як сприятиме міжнародній співпраці та стане лідером у забезпеченні глобальної та відкритої мережі Інтернет. Стратегія спрямована на забезпечення глобальної та відкритої мережі Інтернет із потужним захистом для запобігання виникненню ризиків для безпеки й основних прав і свобод людей у Європі. Враховуючи прогрес, досягнутий під час виконання попередніх стратегій, вона містить конкретні пропозиції щодо розгортання трьох основних інструментів – регуляторного, інвестиційного та політичного – для застосування у трьох сферах діяльності ЄС:

1) стійкість, технологічний суверенітет та лідерство;

2) нарощування оперативного потенціалу для запобігання, стримування та реагування;

3) забезпечення глобального та відкритого кіберпростору.

Стратегія також має на меті встановити пріоритети в галузі розвитку штучного інтелекту, оскільки ця сфера в наш час розвивається найбільш стрімко і являє собою непередбачену й потенційно небезпечну технологію, пропонуючи певний баланс між державними гарантіями збереження персональних даних, з одного боку, та розвитком систем штучного інтелекту – з іншого.

Важливим також є прийняття Закону ЄС про цифрові послуги (Digital Services Act). Його основні завдання: удосконалити механізм захисту прав користувачів в інтернеті; захистити від небажаної реклами; скоротити кількість нелегального контенту в інтернеті, покращити умови для запуску та розширення цифрових послуг для учасників онлайн-ринку в ЄС; збільшити прозорість онлайн-платформ, зокрема щодо алгоритмів, які використовуються для реклами; запобігти зловживанням «інтернет-владою» з боку надвеликих платформ, які охоплюють аудиторію в понад 10 % населення ЄС; сприяти зростанню та розширенню невеликого бізнесу й залученню нових учасників онлайн-ринку;

впровадити систему зобов'язань та відповідальності, а також звільнення від відповідальності для забезпечення прав споживачів цифрових послуг. Закон має на меті забезпечити захист основних прав користувачів інтернету, упроваджує безпрецедентний стандарт відповідальності онлайн-платформ щодо незаконного та шкідливого вмісту, а також визначає єдиний набір правил на внутрішньому ринку, сприяючи конкуренції.

ЄС активно протидіє дезінформації: у 2016 році було прийнято документ «Спільні рамки протидії гібридним загрозам – відповідь Європейського Союзу» («Joint Framework on countering hybrid threats – a European Union response») [5], у якому зазначалося, що «масові дезінформаційні кампанії, використання соціальних медіа для контролю політичного наративу, радикалізації, вербування осіб можуть бути засобами поширення гібридних загроз» та мало на меті сприяти цілісному підходу, який дасть змогу ЄС у координації з державами-членами конкретно протидіяти загрозам гібридного характеру. У контексті цього у 2018 році було опубліковано саморегулюючий «Кодекс поведінки з протидії дезінформації» (Code of Practice on Disinformation) [6], у якому визначено питання, пов'язані з формуванням основи для структурованого діалогу та протидії дезінформації в інтернеті. Його підписали представники найбільших інтернет-платформ та соціальних медіа (Google, Facebook, Twitter та Mozilla).

Ще одним важливим кроком щодо протидії дезінформації в європейському інформаційному просторі стало прийняття у 2018 році «Плану дій щодо протидії дезінформації» (Action Plan against Disinformation) [7] у Європі та поза межами з акцентуванням на чотирьох ключових сферах: вдосконалення можливостей установ ЄС виявляти, аналізувати та викривати дезінформацію; посилення скоординованих та спільних реакцій на дезінформацію; мобілізації приватного сектору в боротьбі з дезінформацією; підвищення обізнаності та підвищення стійкості суспільства.

Отже, викладене вище засвідчує те, що питання правового внормування інформаційних відносин набувають особливого значення в межах ЄС, існують тісні зв'язки інформаційної безпеки із загальною політикою безпеки ЄС, що відображено в кіберелементах Стратегії безпеки ЄС на 2020 рік та Програмі боротьби з тероризмом ЄС [8], а ключовими питаннями для ЄС у контексті забезпечення інформаційної взаємодії держав є правове регулювання захисту персональних даних, побудова цифрового суверенітету ЄС, протидія дезінформації та меседжам ненависті в інтернеті, технологічний розвиток (штучний інтелект).

Це відображає загальну тенденцію стурбованості Євросоюзу не стільки з приводу «м'якої сили» й ідеологічної боротьби з боку інших країн, скільки з приводу необхідності вдосконалити своє законодавство та виробити норми для технологічних компаній і транснаціональних корпорацій, що оперують у цифровій сфері, а відтак – значно впливають на повсякденне життя громадян країн Євросоюзу. То ж головним акцентом у євро-

пейській інформаційній політиці є вироблення правил і контроль за доброчесністю з боку засобів масової комунікації як можливих засобів або ж суб'єктів недоброчесних дій стосовно не тільки держави, а й простих громадян. При забезпеченні цифрового суверенітету також важливим є забезпечення прав громадян при використанні засобів масової комунікації, включно не тільки із захистом персональних даних, а й правом розпоряджатися своїми даними й обмежувати їх поширення без згоди автора [9].

Нормативно-правові акти, прийняті на рівні НАТО у сфері забезпечення інформаційної безпеки, можна умовно поділити на дві групи:

– міжнародні стандарти, які на державному рівні визнаються всіма країнами – членами НАТО і використання яких спрямоване на забезпечення інтероперабельності;

– власне документація НАТО – стандарти, положення та правила, які встановлюють мінімальні вимоги щодо забезпечення захисту інформації на встановленому рівні.

Положення стандартів НАТО спрямовані, передусім, на об'єднання великої кількості правових норм країн – членів Альянсу, деякі принципи можливо застосувати для об'єднання, налагодження обміну інформацією між інформаційними системами різних структур, зокрема, об'єднавши розвідувальну, тактичну, стратегічну інформацію, оперативну інформацію військових підрозділів різних родів військ і правоохоронних органів, МНС, метеорологічних служб тощо за допомогою механізму захищеного зв'язку.

Одним із найновіших чинних стандартів НАТО у сфері забезпечення інформаційної безпеки є AJP-3.20 «Спільна доктрина щодо операцій у кіберпросторі» – Allied Joint Doctrine for Cyberspace Operations, опублікована у 2020 році [10]. У Доктрині, зокрема, зазначається, що вільний потік даних і безперебійне функціонування мереж стало критичним для функцій і послуг громадянського суспільства й військових сил, а державні та недержавні суб'єкти прагнуть використати вразливі місця військових та невійськових інформаційних систем для проникнення, пошкодження чи знищення даних або для отримання престижу, політичних чи військових переваг або прибутку. Тож цифрові мережі та системи потрібно захистити від пошкодження інформації. У взаємопов'язаному світі, де військовий успіх може залежати не стільки від створення фізичних наслідків, скільки від контролю наративів, свобода дій у віртуальному просторі може бути такою ж важливою, як і контроль над землею, повітрям, космосом або морем.

Також наголошується на тому, що кіберпростір – це набагато більше, ніж просто інтернет, адже всі пристрої доступні через кіберпростір, тож можуть бути потенційними цілями та потенційними загрозами. До цього постійно зростаючого переліку додається використання Інтернету речей. Інформаційний простір включає власне інформацію, осіб, організації та системи, які отримують, обробляють та передають інформацію, а також когнітивний, віртуальний та фізичний про-

стір, у якому це відбувається. Останніми роками в цьому середовищі відбулися значні зміни, тож важливість поширення в усьому світі інформації, швидкість, з якою інформація поширюється, роль соціальних медіа та надійність інформаційних систем створили ситуацію, коли жодне рішення або дії Альянсу не можуть бути вжиті, не враховуючи їхній потенційний вплив на інформаційне середовище або ж вплив інформаційного середовища на ці рішення. Зазначається, що вразливість у кіберпросторі пов'язана з її залежністю від кіберпростору. Отже, Альянс повинен мати можливість протистояти супротивникам і підтримувати свої операції, оскільки можливості продовжують розвиватися та вдосконалюватися.

Висновки. При розробленні концепцій переходу до інформаційного суспільства використовується комплексний підхід, заснований на підтримці балансу інтересів людини та держави, а формування глобального інформаційного суспільства відбувається під впливом прогресу нових інформаційних і телекомунікаційних технологій у поєднанні з глобалізацією ринків, тому для гармонійного входження в інформаційне суспільство та дотримання необхідного балансу необхідні координуючі зусилля міжнародних організацій. У перспективі доцільним видається добровільне вироблення норм безпечного співіснування держав в інформаційному просторі в багатосторонньому або двосторонньому форматах. Також мова може йти про підписання рамкових міжнародних угод щодо встановлення загальних принципів забезпечення міжнародної безпеки в інформаційній сфері. У довгостроковій перспективі доцільно виробити комплекс зобов'язань щодо відповідальної поведінки держав та інших суб'єктів в інформаційному просторі. Також слід приділити увагу зовнішнім функціям держави із захисту національних інтересів в інформаційній сфері з урахуванням фактичної нерівності між державами за рівнем розвитку інформаційно-комунікаційної інфраструктури та технологій.

Список використаних джерел

1. Інтеграція України в Європейське інформаційне суспільство. Виклики і завдання. Київ, 2014. 212 с.

2. Digital Single Market Strategy for Europe. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A52015DC0192 (дата звернення: 20.12.2022).

3. General Data Protection Regulation - GDPR. URL: https://gdpr-info.eu/ (дата звернення: 20.12.2022).

4. The EU's Cybersecurity Strategy for the Digital Decade. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Brussels, 16.12.2020 JOIN (2020) 18 final. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164 (дата звернення: 20.12.2022).

5. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Joint Framework on coun-

tering hybrid threats a European Union response. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (дата звернення: 21.12.2022).

6. The 2022 Code of Practice on Disinformation. URL: https://digital-strategy.ee.europa.eu/en/policies/code-practice-disinformation (дата звернення: 21.12.2022).

7. Action Plan against Disinformation. URL: https://www.eeas.europa.eu/node/54866_en (дата звернення: 21.12.2022).

8. Комунікація Програми боротьби з тероризмом ЄС: Передбачити, запобігти, захистити, відповісти, 09.12.2020, COM (2020) 795 остаточна.

9. Шульга О. Цифровий суверенітет і українське суспільство. Час для дискусії настав. URL: https://dt.ua/gazeta/issue/1232 (дата звернення: 21.12.2022).

10. Allied Joint Doctrine for Cyberspace Operations. Jan. 2020. URL: https://assets.publishing.service.gov.uk/govemment/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_l_.pdf (дата звернення: 22.12.2022).

Рецензенти:
доктор педагогічних наук, професор
Г. Артюшин,
кандидат юридичних наук, доцент
О. Шепета

Анотація. У статті досліджуються особливості взаємодії держав у глобальному інформаційному просторі та правова основа цієї взаємодії з урахуванням наявності інформації у всіх сферах державного та міждержавного рівнів, що потребує вжиття необхідних заходів і розроблення відповідних правових основ.

Ключові слова: глобальний інформаційний простір, інформаційний простір, інформація, інформаційне суспільство.

Abstract. Peculiarities of the interaction of states in the global information space and the legal basis of this interaction are investigated, availability of information in all spheres of state and interstate level is given, which requires implementing appropriate measures and development of legal frameworks.

Key words: global information space, information space, information, information society.