КОНСТИТУЦІЙНЕ ТА АДМІНІСТРАТИВНЕ ПРАВО

DOI: 10.18372/2307-9061.72.19064
УДК 343.326:004.056.53(045)

Є. В. Криволап,
здобувач вищої освіти третього (освітньо-наукового) рівня
ORCID ID: https://orcid.org/0000-0003-2599-2520

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХОДІВ ПРОТИДІЇ КІБЕРЗАГРОЗАМ АКТАМИ ЄВРОПЕЙСЬКОГО РІВНЯ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03058, Київ, Україна
E-mail: krivolap.evgeniy@gmail.com

Метою *статті є дослідження системи та змісту актів європейського рівня у сфері протидії кіберзагрозам.* ***Методи дослідження****: документальний аналіз, узагальнення правової інформації, інформації із сфери кіберзахисту інформаційно-комунікаційних систем.* ***Результати****: визначені особливості правового регулювання заходів забезпечення кібербезпеки правовими актами європейського рівня. Наголошено, що три засадничих нормативних акти ЄС у сфері кіберзахисту, а саме: Директива Європейського парламенту і Ради ЄС 2016/1148 від 06.07.2016 про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу; Директива Ради 2008/114/ЄС від 08.12.2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту; Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27.04.2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, – підлягають імплементації у законодавство України відповідно до Угоди про асоціацію між Україною та Європейським Союзом 2014 року. Вперше встановлено, що керівними документами європейського рівня щодо практичного впровадження вимог вказаних Конвенцій про кіберзахист слід вважати і брати до виконання Конвенцію від 23.11.2001 року Ради Європи «Про кіберзлочинність» з Додатковим протоколом від 28.01.2003 року до Конвенції про кіберзлочинність; Рекомендацію від 30.10.1997 р. № R (97) 19 Комітету міністрів Ради Європи «Про показ насильства електронними ЗМІ»; Рекомендацію від 30.10.1997 р. № R (97) 20 Комітету міністрів Ради Європи «Про розпалювання ненависті»; Рекомендацію від 27.04.1989 р. № R (89) 7 Комітету міністрів РЄ «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту». Здійснюються заходи унормування вимог до програмного та апаратного забезпечення, спрямованих на протидію кібервтручанням.* ***Обговорення****: реалізація зазначених положень дозволяє виробити національні стандарти належного захисту від кібервтручань та глядачів від «необґрунтованого показу насильства».*

Ключові слова*: кібербезпека; Директива Європейського парламенту і Ради ЄС; Регламент Європейського парламенту і Ради ЄС; Рекомендація Комітету міністрів Ради Європи; вразливість; комп'ютерні мережі.*

Постановка проблеми та її актуальність. Сьогодні практично жодна сфера людської діяльності, у тому числі і цивільна авіація, не обходиться без використання інформаційних технологій. Але повсюдна інформатизація стала приводом для зловмисників атакувати

комп'ютерні інформаційні системи. Таким чином кібератаки стали звичайною справою [1, с. 41-42]. У січні 2024 року Держспецзв'язку України повідомив, що у попередньому році в Україні кількість кібератак зросла, порівняно з 2022 роком, на 15,9% – до 2543 інцидентів. За даними урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, 347 кібератак було зафіксовано на уряд та урядові організації, 276 – на місцеві органи влади, 175 – на організації у секторі безпеки та оборони, 127 – комерційні організації. Ще 92 рази було атаковано енергетичний сектор, 81 – телеком, 38 – освітні установи, 32 – транспортну галузь, 30 – фінансовий сектор, 25 – IT-сектор, 15 – ЗМІ, 12 – медичні установи [2]. Кібератаки стали чинником агресії російської федерації проти України і цивілізованого світу. У січні 2023 року речник федерального уряду Німеччини Крістіне Гоффманн повідомила, що російські хакери атакували Німеччину після її рішення передати Україні танки. Насамперед кібератаки торкнулися сайтів аеропортів, установ фінансового сектора, органів влади федерального та земельного рівнів, зокрема, МВС землі Баден-Вюртемберг. Відповідальність за атаки взяло на себе російське хакерське угруповання Killnet, лояльне до Путіна. Вони заявили, що їхні дії є відповіддю на анонсоване постачання до України німецьких танків Leopard 2. У той же час повідомлено, що Федеральне відомство інформаційної безпеки попередило уразливі інституції та дало поради, як протистояти таким атакам [3]. Отже, проблема протидії кіберзагрозам є актуальною.

Аналіз досліджень і публікацій з проблеми. Проблеми врегулювання і унормування діяльності у кіберпросторі вже давно стали ключовими у політиці багатьох держав світу. Всі вони однозначні у твердженні, що кіберпростір – це міжнародний простір, і діяльність держав у кібепросторі повинна в першу чергу відповідати нормам міжнародного права. Україна інтегрована у світовий цифровий простір, тому запобігання кіберзагрозам можливе завдяки поєднанню національної та міжнародної стратегій кібербезпеки [4-8 та ін.]. Як зазначається у дисертації [7], для України є надзвичайно актуальним впровадження міжнародного досвіду у сфері адміністративно-правового та організаційного забезпечення кібербезпеки, який є необхідним у якості успішного прикладу щодо формування відповідної політики і побудови власної системи правового та організаційного забезпечення кібербезпеки, у першу чергу, в умовах гібридної війни. Успіх та ефективність адміністративно-правового забезпечення кібербезпеки забезпечується одночасними заходами, спрямованими як у напрямі співпраці з фаховими міжнародними інституціями щодо забезпечення кібербезпеки, так і у напрямі формування адекватного викликам гібридної війни національного законодавства у цій сфері [7, с. 404]. Важливим елементом подальшої розбудови системи забезпечення кібербезпеки України, особливо в умовах гібридної війни, є необхідність імплементації положень Директиви Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу [7, с. 374]. Окремі питання правового регулювання заходів забезпечення кібербезпеки актами європейського рівня розглянуті автором (у співавторстві) у статті [9].

Виклад основного матеріалу дослідження. На європейському рівні слід виокремити такі акти загальноєвропейського правового регулювання:

- Директива Європейського парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу;

- Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту;

- Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних);

- Конвенція від 23.11.2001 року Ради Європи «Про кіберзлочинність»; ратифікована Законом

України від 07.09.2005 № 2824-IV «Про ратифікацію Конвенції про кіберзлочинність». Конвенція набрала чинності для України 01.07.2006 року;

- Додатковий протокол від 28.01.2003 року до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи; протокол ратифіковано Законом України від 21.07.2006 № 23-V. Дата набрання чинності для України 01.04.2007 року;

- Рекомендація від 30.10.1997 р. № R (97) 19 Комітету міністрів Ради Європи «Про показ насильства електронними ЗМІ», ухвалена Комітетом міністрів на 607-му засіданні заступників міністрів від 30.10.1997 р.;

- Рекомендація від 30.10.1997 р. № R (97) 20 Комітету міністрів Ради Європи «Про розпалювання ненависті», ухвалена Комітетом міністрів на 607-му засіданні заступників міністрів від 30.10.1997 р.;

- Рекомендація від 27.04.1989 р. № R (89) 7 Комітету міністрів РЄ «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту», ухвалена Комітетом міністрів на 425-му засіданні заступників міністрів від 27.04.1989 р.

Даний перелік не є вичерпним. Окремі питання правового регулювання заходів забезпечення кібербезпеки висвітлюються у певних суміжних актах. Наприклад, у Конвенції від 25.10.2007 року Ради Європи «Про захист дітей від сексуальної експлуатації та сексуального насильства» мітиться посилання на Рекомендацію № R (91) 11 Комітету міністрів про сексуальну експлуатацію, порнографію, проституцію, а також торгівлю дітьми та підлітками, Рекомендацію Rec (2001) 16 про захист дітей від сексуальної експлуатації та Конвенцію про кіберзлочинність, зокрема статтю 9 цієї Конвенції, а також Конвенцію Ради Європи про заходи щодо протидії торгівлі людьми.

Перші три перелічені документи (Директива 2016/1148 від 06.07.2016; Директива 2008/114/ЄС від 08.12.2008; Регламент 2016/679 від 27.04.2016) підлягають імплементації у законодавство України відповідно до Угоди про асоціацію між Україною та Європейським Союзом 2014 року.

Зокрема, у Директиві 2016/1148 від 06.07.2016 відзначається, що вона прийнята, між іншим, виходячи з наступних міркувань:

(1) Мережеві та інформаційні системи та послуги відіграють важливу роль у суспільстві. Їхня надійність та безпека суттєва для економічної та соціальної діяльності і, зокрема, для функціонування внутрішнього ринку.

(2) Масштаб, частота та вплив інцидентів, пов'язаних з безпекою, зростають та становлять велику загрозу для функціонування мережевих та інформаційних систем. Такі системи можуть також ставати об'єктом умисних шкідливих дій, мета яких – пошкодити такі системи або завадити їх експлуатації. Такі інциденти можуть перешкоджати здійсненню економічної діяльності, завдавати значних фінансових збитків, підривати довіру користувачів та спричиняти значну шкоду економіці Союзу.

(3) Мережеві та інформаційні системи і, в першу чергу, Інтернет, відіграють важливу роль у сприянні транскордонному руху товарів, послуг та людей.

(62) Інциденти можуть бути результатом злочинної діяльності, попередженню, розслідуванню та кримінальному переслідуванню яких сприяє координація та співпраця між операторами основних послуг, надавачами цифрових послуг, компетентними органами та правоохоронними органами. У разі підозри, що інцидент пов'язаний із серйозною злочинною діяльністю відповідно до національного законодавства або законодавства Союзу, держави-члени повинні заохочувати операторів основних послуг та надавачів цифрових послуг повідомляти відповідні правоохоронні органи про інциденти, щодо серйозного злочинного характеру яких виникає підозра. Якщо доречно, бажано, щоб координації компетентних органів та правоохоронних органів різних держав-членів сприяли Європейський центр боротьби з кіберзлочинністю (ЕСЗ) та ENISA.

(63) У багатьох випадках персональні дані викрадають у результаті інцидентів. З огляду на це, компетентні органи та органи з питань захисту даних повинні співпрацювати та обмінюва-

тися інформацією щодо всіх відповідних питань, з метою боротьби з витоками персональних даних внаслідок інцидентів.

(75) Ця Директива поважає фундаментальні права та дотримується принципів, визнаних Хартією фундаментальних прав Європейського Союзу, зокрема права на повагу особистого життя та комунікацій, захисту персональних даних, свободи підприємництва, права власності, права дієвого правового захисту в суді та права бути вислуханим.

Згідно пункту 2 статті 1 Директива:

(a) встановлює обов'язки для всіх держав-членів для ухвалення національної стратегії безпеки мережевих та інформаційних систем;

(b) створює Групу співпраці для підтримки та сприяння стратегічній співпраці та обміну інформацією серед держав-членів та розвитку повної довіри між ними;

(c) створює мережу груп реагування на інциденти, пов'язані з комп'ютерною безпекою («мережа CSIRT») з метою зміцнення повної довіри між державами-членами та сприяння швидкій та дієвій оперативній взаємодії;

(d) встановлює вимоги до безпеки та повідомлення для операторів основних послуг та надавачів цифрових послуг;

(e) встановлює обов'язки для держав-членів для призначення національних компетентних органів, єдиних контактних пунктів та CSIRT із завданнями, пов'язаними з безпекою мережевих та інформаційних систем.

Згідно пункту 1 статті 2 Директиви, опрацювання персональних даних відповідно до цієї Директиви необхідно здійснювати згідно з Директивою 95/46/ЄС, на зміну якій прийнято Регламент 2016/679 від 27.04.2016.

Конвенція Ради Європи «Про кіберзлочинність» з Додатковим протоколом до неї вважається універсальним міжнародним документом, що встановлює і класифікує злочини у сфері кіберзлочинності [10, с. 70]. Усього можна виділити 2 групи кіберзлочинів: які вчиняються у кіберпросторі та які вчиняються з використанням останнього.

До першої групи злочинів можна віднести три категорії кіберзлочинів:

- злочини проти конфіденційності, цілісності і працездатності комп'ютерних даних і систем – незаконний доступ, незаконне перехоплення, створення перешкод для обміну даними, створення перешкод для функціонування систем, неправомірне використання апаратних пристроїв;
- комп'ютерні злочини – фальсифікація і підробка, що здійснюються з використанням комп'ютерної техніки;
- злочини, пов'язані з контентом – виготовлення, поширення і зберігання дитячої порнографії.

Об'єктом таких кіберзлочинів може стати будь-який користувач Інтернету.

Разом із тим, до другої групи злочинів можна віднести дві категорії кіберзлочинів:

- злочини, пов'язані з порушенням авторського права і суміжних прав, при цьому встановлення таких правопорушень віднесено документом до компетенції національних законодавств держав;
- кіберзлочини як акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж.

Об'єктом таких кіберзлочинів може стати не тільки і навіть не стільки будь-який користувач Інтернету, але й особа, яка не є користувачем Інтернету. Наприклад об'єктом злочину у вигляді поширення контрафактної продукції через мережу Інтернет може стати суб'єкт авторського права, який не є користувачем Інтернету.

Як зазначається у дисертації [7, с. 71], деякі кіберзлочини нормами Конвенції про кіберзлочинність не виділено в окремі групи. В наукових колах ведуться дискусії щодо даних кіберзлочинів, які до цього часу викликають суперечки щодо необхідності гармонізації законодавства на міжнародному рівні з точки зору техніки їх криміналізації. Це «кібертероризм» та використання кіберпростору в терористичних цілях. Державами та міжнародними організаціями вживаються зусилля щодо боротьби з терористичними організаціями, які використовують кіберпростір. Як приклад, можна навести проект Clean IT, який існує на рівні ЄС та метою якого є боротьба з кібертероризмом.

Не можна поза увагою залишити ще одну категорію кіберзлочинів, а саме – крадіжка, передача і використання персональних даних з метою вчинення злочинів (identity theft), яка, хоча і не включена окремо в Конвенцію про кіберзлочинність, але отримала поширення після прийняття міжнародного документа. Деякі країни виділяють ці злочини в окрему категорію, інші вважають, що дані діяння підпадають під кілька статей кримінального законодавства [11, с. 33], що, у свою чергу, спонукає до виділення даного злочину в окрему групу та гармонізації міжнародного законодавства у цій сфері.

Вище зазначено, що серед стратегічних цілей та напрямів реалізації Стратегії інформаційної безпеки України визначені, зокрема, протидія пропаганді війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті. Комплекс підходів, що дає уявлення про європейські стандарти обмеження поширення матеріалів, що містять показ насильства та жорстокості, надають Рекомендації Комітету міністрів Ради Європи № R (89) 7 від 27.04.1989 р. «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту», № R (97) 19 від 30.10.1997 р. «Про показ насильства електронними ЗМІ», № R (97) 20 від 30.10.1997 р. «Про розпалювання ненависті». Базовим принципом підходу до обмежень в даній сфері є правила, встановлені ст. 10 Конвенції про захист прав людини і основоположних свобод 1950 року (ЄКПЛ).

У Рекомендації № R (89) 7, враховуючи, зокрема, норми ст.ст. 8 і 10 ЄКПЛ щодо свободи вираження поглядів і безперешкодного поширення інформації та ідей, визнається, тим не менш, важливість консолідації дій, спрямованих проти поширення відеозаписів насильницького, жорстокого й порнографічного змісту, а також проти вживання наркотиків, зокрема задля захисту неповнолітніх. З цією метою визнано, що Держави-члени повинні: заохочувати створення систем саморегулювання, або створювати системи класифікації й контролю за відеозаписами за допомогою відповідних професійних секторів чи органів державної влади, або запроваджувати системи, які поєднують саморегулювання з системами класифікації й контролю чи іншими, які не суперечать національному законодавству. В усіх випадках можливе застосовування кримінального законодавства та відповідних заходів впливу фінансового й фіскального характеру. Зокрема, обмеження поширення можуть здійснюватися шляхом: заборони поставок з комерційною метою або пропозицій щодо поставок неповнолітнім; заборони на рекламу; заборони на продаж по пошті. Класифікація кожного відеозапису має бути вказана на упаковці матеріального носія і у відеокаталозі, рекламі та ін.

Рекомендація № R (97) 20 від 30.10.1997 р. виходила з засудження розпалювання расової ненависті, ксенофобії, антисемітизму та всіх форм нетерпимості, оскільки це підриває безпеку демократії, культурну єдність, плюралізм. Зазначається, що окремі випадки розпалювання ненависті можуть бути настільки образливі для окремих осіб і груп населення, що вони вийдуть за рамки правового захисту, що надається ст. 10 ЄКПЛ відносно свободи форм самовираження. Деякі форми необґрунтованого показу насильства, розпалювання ненависті можуть законним чином бути обмежені, враховуючи обов'язки й відповідальність, що їх несе із собою здійснення права на свободу вираження поглядів, за умови, що такі втручання в свободу вираження поглядів передбачені законодавством і є необхідними в демократичному суспільстві, згідно ч. 2 ст. 10 ЄКПЛ.

Найбільш докладно аналізована проблема викладається у Рекомендації № R (97) 19. Ця Рекомендація виходили з того, що здійснення свободи вираження поглядів пов'язані з обов'язками і відповідальністю, і що воно може бути законним чином обмежене з метою підтримки рівноваги між здійсненням цього права і дотриманням інших основних прав, свобод і інтересів, які захищає Конвенція. Керівним принципом у визначенні меж показу насильства є ст. 10 ЄКПЛ.

Зокрема, у Рекомендації № R (97) 19 наголошено, що свобода вираження поглядів, в принципі, включає також право поширювати й одержувати інформацію та ідеї, які становлять показ насильства. Проте деякі форми необґрун-

тованого показу насильства можуть законним чином бути обмежені з метою гарантування поваги людської гідності й захисту вразливих груп, наприклад, дітей і підлітків, фізичному, розумовому й моральному розвитку яких може зашкодити показ такого насильства. У Рекомендації № R (97) 19 дано визначення поняттю «необґрунтований показ насильства», яке розуміється як поширення повідомлень, слів і зображень, насильницькому змісту яких або способу подання надається особлива виразність, не виправдана контекстом.

Виходячи з принципу єдності права на самовираження та обов'язків, пов'язаних з використанням цього права, Рекомендація № R (97) 19 сформулювала способи, якими на фахівців ЗМІ може бути покладена відповідальність за належну редакційну політику, в тому числі і щодо уникнення «необґрунтованого показу насильства»: i) попередня поінформованість громадськості про повідомлення, слова́ й зображення насильницького характеру, які збираються зробити доступними; ii) запровадження кодексів поведінки, які визначатимуть конкретні обов'язки відповідного професійного сектора; iii) впровадження внутрішніх керівних принципів, у т.ч. стандартів для оцінювання змісту в організаціях електронних ЗМІ; iv) заснування на секторальному рівні та окремими телерадіомовниками відповідних консультативних і контрольних механізмів для моніторингу процесу впровадження стандартів саморегулювання; v) врахування стандартів саморегулювання в контрактах з іншими секторами, наприклад, виробниками аудіовізуальної продукції й відеоігор, рекламними агенціями та ін.; vi) регулярні контакти та обмін інформацією з національними регуляторними органами, а також з органами саморегулювання в інших країнах.

Серед дієвих національних заходів обмеження «необґрунтованого показу насильства» Рекомендація № R (97) 19 визначає: надання користувачам ЗМІ – і громадянам, й іноземцям, – незадоволеним насильницьким спрямуванням певних служб або продукції, – можливості звертатись із скаргою до регуляторного або іншого уповноваженого національного органу; включення до умов ліцензій для телерадіомовників певних зобов'язань, що стосуються показу насильства, разом із попереджувальними заходами адміністративного характеру (наприклад, непродовження ліцензії за недодержання цих зобов'язань) тощо.

Слід також врахувати, що останнім часом в законодавство ЄС імплементуються нормативні вимоги до програмного та апаратного забезпечення, спрямовані на протидію кібервтручанням. Так, повідомляється [12], що ЄС пропонує стандарти безпеки для складових мережі Інтернет (IoT). Законодавці ЄС запровадили нові стандарти безпеки для підключених до Інтернету продуктів – від смартфонів до холодильників – оскільки Союз намагається протистояти зростаючій загрозі, яку становлять кібератаки. Запропонований Закон про кіберстійкість (Cyber Resilience Act, CRA) запроваджує кілька ключових заходів, включаючи основні вимоги безпеки для продуктів, які вважаються безпечними для ринку, і зобов'язання їхніх виробників щодо усунення вразливостей після їх виявлення. CRA вимагає від компаній мати механізми для усунення будь-яких недоліків, виявлених у їхніх пристроях після того, як вони були продані споживачам протягом періоду до п'яти років або принаймні протягом очікуваного терміну експлуатації продукту. Пристрої, які не відповідають цим стандартам, можуть бути зняті з ринку, а виробники можуть зіткнутися зі штрафом у розмірі 15 мільйонів євро або 2,5% від їх загального річного доходу за недотримання правил.

Висновки. Визначені особливості правового регулювання заходів забезпечення кібербезпеки правовими актами європейського рівня. Наголошено, що три засадничих нормативних акти ЄС у сфері кіберзахисту, а саме: Директива Європейського парламенту і Ради (ЄС) 2016/1148 від 06.07.2016 про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу; Директива Ради 2008/114/ЄС від 08.12.2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту; Регламент Європейського парламенту і Ради (ЄС) 2016/679

від 27.04.2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, – підлягають імплементації у законодавство України відповідно до Угоди про асоціацію між Україною та Європейським Союзом 2014 року. Вперше встановлено, що керівними документами європейського рівня щодо практичного впровадження вимог вказаних Конвенцій про кіберзахист слід вважати і брати до виконання Конвенцію від 23.11.2001 року Ради Європи «Про кіберзлочинність» з Додатковим протоколом від 28.01.2003 року до Конвенції про кіберзлочинність; Рекомендацію від 30.10.1997 р. № R (97) 19 Комітету міністрів Ради Європи «Про показ насильства електронними ЗМІ», ухвалену Комітетом міністрів на 607-му засіданні заступників міністрів від 30.10.1997 р.; Рекомендацію від 30.10.1997 р. № R (97) 20 Комітету міністрів Ради Європи «Про розпалювання ненависті», ухвалену Комітетом міністрів на 607-му засіданні заступників міністрів від 30.10.1997 р.; Рекомендацію від 27.04.1989 р. № R (89) 7 Комітету міністрів РЄ «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту», ухвалену Комітетом міністрів на 425-му засіданні заступників міністрів від 27.04.1989 р. Реалізація зазначених положень дозволяє виробити національні стандарти належного захисту прав глядачів на захист від «необґрунтованого показу насильства». Здійснюються заходи унормування вимог до програмного та апаратного забезпечення, спрямованих на протидію кібервтручанням.

Публікація підготовлена на підставі Звіту [7].

Література

1. Філінович В.В. Кібербезпека та загрози авіаційній сфері: правовий аспект. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право».* 2021. № 3 (60). С. 38-43. URL: 10.18372/2307-9061.60.15950.

2. Жарикова А. Кількість кібератак у 2023 році зросла на 16% – Держспецзв'язку. *Економічна правда.* 31.01.2024. URL: https://www.epravda.com.ua/news/2024/01/31/709355/.

3. Глущенко О. Російські хакери атакували Німеччину після її рішення передати Україні танки. *Українська правда.* 28.01.2023. URL: https://www.pravda.com.ua/news/2023/01/28/7386899/.

4. Размєтаєва Ю.С. Система міжнародної безпеки у світлі кіберзагроз: правові проблеми та перспективи. Актуальні проблеми сучасного міжнародного права: зб. наук. ст. за матеріалами І Харк. міжнар.-прав. читань, присвячених пам'яті проф. М.В. Яновського і В.С. Семенова, Харків, 27 листоп. 2015 р.: у 2 ч. Харків. 2015. ч. 1. С. 17-177.

5. Maskun S.H. Cyber Security: Rule of Use Internet Safely. Journal of Law, Policy and Globalization. 2013. Vol. 15. P. 22.

6. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва. Монографія. Київ НІСД, 2014. 328 с.

7. Веселова Л.Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни. Дис … д-ра юр. наук. Спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Одеса. Одеський державний університет внутрішніх справ. 2021. 500 с.

8. Валюшко І.О. Інформаційна безпека України в контексті російсько-українського конфлікту. Дис … канд. політичних наук. Спец. 23.00.04 – політичні проблеми міжнародних систем та глобального розвитку. Київ, 2018. 210 с.

9. Криволап Є.В., Юринець Ю.Л., Бєлкін Л.М. Правове регулювання заходів забезпечення кібербезпеки актами європейського рівня. Moderní aspekty vědy: XL. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. str. 103-114.

10. Лихова С.Я., Леонов Б.Д. Інформаційний тероризм як загроза національній безпеці України. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. Київ НАУ. 2021. № 2 (59). С. 170-176.

11. Бабакін В.М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів. *Форум права*. 2011. № 4. С. 27-35. URL: http:/Avww.nbuv.gov.ua/e-journals/FP/ 2011-

4/11bvmprk.pdf.

12. Martin A. EU proposes security standards for IoT products. The Record. September 15th, 2022. URL: https://therecord.media/eu-proposes-security-standards-for-iot-products.

13. Проблеми формування та реалізації державної політики у сфері інформаційної безпеки України: теорія і практика. Звіт про науково-дослідну роботу № 312-ДБ20. № державної реєстрації 0120U102136. Київ. 2022. 624 с. Рукопис. Закінчено 7 груд. 2022 р.

References

1. Filinovych V.V. Kiberbezpeka ta zahrozy aviatsiinii sferi: pravovyi aspekt. *Naukovi pratsi Natsionalnoho aviatsiinoho universytetu: Seriia «Yurydychnyi visnyk. Povitriane i kosmichne pravo».* 2021. № 3 (60). S. 38-43. URL: 10.18372/2307-9061.60.15950.

2. Zharykova A. Kilkist kiberatak u 2023 rotsi zrosla na 16% – Derzhspetszviazku. *Ekonomichna pravda.* 31.01.2024. URL: https://www.epravda.com.ua/news/2024/01/31/709355/.

3. Hlushchenko O. Rosiiski khakery atakuvaly Nimechchynu pislia yii rishennia peredaty Ukraini tanky. *Ukrainska pravda*. 28.01.2023. URL: https://www.pravda.com.ua/news/2023/01/28/7386899/.

4. Razmietaieva Yu.S. Systema mizhnarodnoi bezpeky u svitli kiberzahroz: pravovi problemy ta perspektyvy. Aktualni problemy suchasnoho mizhnarodnoho prava: zb. nauk. st. za materialamy I Khark. mizhnar.-prav. chytan, prysviachenykh pamiati prof. M.V. Yanovskoho i V.S. Semenova, Kharkiv, 27 lystop. 2015 r.: u 2 ch. Kharkiv. 2015. ch. 1. S. 17-177.

5. Maskun S.H. Cyber Security: Rule of Use Internet Safely. Journal of Law, Policy and Globalization. 2013. Vol. 15. P. 22.

6. Dubov D.V. Kiberprostir yak novyi vymir heopolitychnoho supernytstva. Monohrafiia. Kyiv NISD, 2014. 328 s.

7. Veselova L.Iu. Administratyvno-pravovi osnovy kiberbezpeky v umovakh hibrydnoi viiny. Dys … d-ra yur. nauk. Spets. 12.00.07 «Administratyvne pravo i protses; finansove pravo; informatsiine pravo». Odesa. Odeskyi derzhavnyi universytet vnutrishnikh sprav. 2021. 500 s.

8. Valiushko I.O. Informatsiina bezpeka Ukrainy v konteksti rosiisko-ukrainskoho konfliktu. Dys … kand. politychnykh nauk. Spets. 23.00.04 – politychni problemy mizhnarodnykh system ta hlobalnoho rozvytku. Kyiv, 2018. 210 s.

9. Kryvolap Ye.V., Yurynets Yu.L., Belkin L.M. Pravove rehuliuvannia zakhodiv zabezpechennia kiberbezpeky aktamy yevropeiskoho rivnia. Moderní aspekty vědy: XL. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. str. 103-114.

10. Lykhova S.Ia., Leonov B.D. Informatsiinyi teroryzm yak zahroza natsionalnii bezpetsi Ukrainy. *Naukovi pratsi Natsionalnoho aviatsiinoho universytetu. Seriia: Yurydychnyi visnyk «Povitriane i kosmichne pravo».* Kyiv NAU. 2021. № 2 (59). S. 170-176.

11. Babakin V.M. Osoblyvosti mizhnarodnoho spivrobitnytstva pry rozsliduvanni kiberzlochyniv. *Forum prava*. 2011. № 4. S. 27-35. URL: http:/Avww.nbuv.gov.ua/e-journals/FP/2011-4/11bvmprk.pdf.

12. Martin A.EU proposes security standards for IoT products. The Record. September 15th, 2022. URL: https://therecord.media/eu-proposes-security-standards-for-iot-products.

13. Problemy formuvannia ta realizatsii derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy: teoriia i praktyka. Zvit pro naukovo-doslidnu robotu № 312-DB20. № derzhavnoi reiestratsii 0120U102136. Kyiv. 2022. 624 s. Rukopys. Zakincheno 7 hrud. 2022 r.

Ievgenii Kryvolap

ADMINISTRATIVE AND LEGAL REGULATION OF MEASURES AGAINST CYBER THREATS BY ACTS OF THE EUROPEAN LEVEL

National Aviation University
Liubomyra Huzara Avenue, 1, 03058, Kyiv, Ukraine
E-mail: krivolap.evgeniy@gmail.com

The purpose *of the article is to study the system and content of acts of the European level in the field of combating cyber threats.* ***Research methods:*** *documentary analysis, summarization of legal information, information from the field of cyber protection of information and communication systems.* ***Results:*** *specific features of the legal regulation of measures to ensure cyber security by legal acts of the European level have been determined. It was emphasized that the three basic EU regulations in the field of cyber protection, namely: Directive of the European Parliament and the Council of the EU 2016/1148 of 07.06.2016 on measures for a high common level of security of network and information systems on the territory of the Union; Council Directive 2008/114/EU of 08.12.2008 on the identification and definition of European critical infrastructures and assessment of the need to improve their protection and protection; Regulation of the European Parliament and Council (EU) 2016/679 of 27.04.2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data – subject to implementation into the legislation of Ukraine in accordance with the Association Agreement between Ukraine and the European Union of 2014. It was established for the first time that the Council of Europe Convention on Cybercrime dated November 23, 2001 with the Additional Protocol dated January 28, 2003 to the Convention on Cybercrime should be considered and implemented as European-level guidelines for the practical implementation of the requirements of the specified Conventions on cyber protection; Recommendation dated October 30, 1997 No. R (97) 19 of the Committee of Ministers of the Council of Europe «On the display of violence by electronic media»; Recommendation dated October 30, 1997 No. R (97) 20 of the Committee of Ministers of the Council of Europe «On incitement to hatred»; Recommendation dated 04/27/1989 No. R (89) 7 of the Committee of Ministers of the Council of Europe «On the principles of distribution of video recordings of violent, cruel or pornographic content». Measures are being taken to standardize software and hardware requirements aimed at countering cyber interference.* ***Discussion:*** *the implementation of the specified provisions allows for the development of national standards for adequate protection against cyber interference and viewers from "unwarranted display of violence".*

Key words: *cyber security; Directive of the European Parliament and the Council of the EU; Regulation of the European Parliament and the Council of the EU; Recommendation of the Committee of Ministers of the Council of Europe; vulnerability; computer networks.*

Стаття надійшла до редакції 22.08.2024