9. Surface Mining Control and Reclamation Act (1977). Retrieved from: https://en.wikipedia.org/wiki/Surface_Mining_Control_and_Reclamation_Act_of_1977. [in English].

10. Mandryk, V. O. (2005). Vidtvorennia porushenykh zemel: zarubizhnyi dosvid, mekhanizm finansuvannia. [Reproduction of disturbed lands: foreign experience, financing mechanism]. *Naukovyi visnyk Natsionalnoho lisotekhnichnoho universytetu Ukrainy*, (5.3). 208-212. [in Ukrainian].

11. Shvets, O. H., & Drebot, O. I. (2015). Napriamy pidvyshchennia efektyvnosti vykorystannia ahroresursnoho potentsialu v rehionakh tekhnohenno porushenykh zemel z urakhuvanniam svitovoho dosvidu. [Directions for increasing the efficiency of the use of agricultural resource potential in the regions of man-made disturbed lands, taking into account world experience] *Investytsii: praktyka ta dosvid.* (18). 54-58. [in Ukrainian].

Стаття надійшла до редакції: 20.05.2023

УДК 342.951
DOI: 10.36550/2522-9230-2023-14-143-147

Мігалатюк Владислав Вікторович,
аспірант кафедри права та правоохоронної діяльності
Центральноукраїнського державного університету
імені Володимира Винниченка
e-mail: vmihalatiuk@cuspu.edu.ua
https://orcid.org/0009-0007-7638-1873

УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ: ДОСВІД ЄВРОПЕЙСЬКИХ КРАЇН

Стаття присвячена діяльності Європейського Союзу та НАТО, які вважають боротьбу з гібридними загрозами пріоритетом міжнародного співробітництва. Проаналізовано низку документів ЄС, які формують чітке уявлення про гібридність кіберзагроз та основні напрямки адміністративного, правового та організаційного забезпечення кібербезпеки, зокрема щодо протидії гібридним кіберзагрозам у Європейському Союзі. Виходячи з проведеного аналізу, на сучасному етапі розвитку суспільства сформувалися основи щодо утвердження стійкого сприйняття проблеми ризику як одного з факторів формування сучасного і особливо майбутнього суспільства, яке до того ж набуває дедалі більшої суспільної значущості.

Наголошується, що вітчизняна нормативна база має суттєві недоліки та потребує запровадження відповідних правил запровадження ризик-орієнтованого підходу в діяльності з кібербезпеки в Україні, а також визначення основних термінів («ризик-орієнтований підхід до кібербезпеки», «ризик-орієнтований підхід до захисту критичної інфраструктури», «ризики», «ризик-менеджмент»).

Розглянуто сутність та значення терміну «стійкість», який набув практичного застосування у стратегічних документах у сфері безпеки та за своєю суттю є новітньою концепцією сучасної теорії національної безпеки, що має практичне значення для державної політики у безпековому середовищі та є важливим для практики безпеки в кіберпросторі, оскільки саме наявність гібридних загроз у кіберпросторі, яким неможливо запобігти, зумовлює необхідність формування нового підходу, зокрема, формування «стійкості», яка, у свою чергу, має бути реалізована в публічній політиці кіберпростору.

Ключові слова: кібератаки, кібербезпека, гібридна війна, стійкість суспільства, відповідь, ризики.

Mihalatiuk V. IMPROVING THE ADMINISTRATIVE AND LEGAL ENSURE OF CYBER SECURITY IN UKRAINE: EXPERIENCE OF EUROPEAN COUNTRIES

The article is devoted to the activities of the European Union and NATO, which consider the fight against hybrid threats a priority of international cooperation. A number of EU documents have been analyzed, which form a clear idea of the hybridity of cyber threats and the main directions of administrative, legal and organizational support for cyber security, in particular, regarding countering hybrid cyber threats in the European Union. Based on the conducted analysis, at the current stage of the development of society, the foundations have been formed for the establishment of a stable perception of the problem of risk as one of the factors in the formation of modern and especially future society, which, moreover, is gaining more and more social significance.

It is emphasized that the domestic regulatory framework has significant shortcomings and requires the introduction of appropriate rules for the introduction of a risk-oriented approach in cyber security activities in Ukraine, as well as the definition of the main terms ("risk-oriented approach to cyber security", "risk-oriented approach to the protection of critical infrastructure", "risks").

The essence and meaning of the term "sustainability", which has gained practical application in strategic documents in the field of security and is essentially the newest concept of the modern theory of national security, which has practical significance for state policy in the security environment and is important for the practice of security in cyberspace, is considered. because it is the presence of hybrid threats in cyberspace, which cannot be prevented, that necessitates the formation of a new approach, in particular, the formation of "resilience", which, in turn, must be implemented in the public policy of cyberspace.

Key words: cyber attacks, cyber security, hybrid warfare, societal resilience, response, risks.

Постановка проблеми: На сьогоднішній день питання захисту інформації та кібербезпеки набуло чималого значення у зв'язку із активною повномасштабною війною, з якою зіштовхнулася Україна. Значний та швидкий розвиток науково-технічного прогресу став передумовою гібридним кіберзагрозам, яким стали наражати суспільство та державу на небезпеку, підриваючи фундаментальні демократичні цінності та свободи. Кібербезпека відіграє життєво важливу роль у забезпеченні національної безпеки, захищаючи від кіберзагроз з боку національних держав, терористичних груп та інших зловмисників, які використовують кібератаки як засіб впливу або зриву операцій уряду. Державні системи, інфраструктура та конфіденційні дані, такі як військова таємниця, розвідувальна інформація та критична національна інфраструктура, потребують надійних заходів кібербезпеки, щоб запобігти несанкціонованому доступу, шпигунству та саботажу. Саме тому для забезпечення національної безпеки, захисту даних громадян, захисту демократичних процесів, сприяння співпраці та підтримки економічної стабільності слід приділити значну увагу адміністративно-правовому забезпеченню кібербезпеки в Україні.

Аналіз останніх досліджень та публікацій. Питання кібербезпеки та державної політики, спрямованої на її забезпечення, є предметом дослідження багатьох провідних науковців у галузі адміністративного, конституційного та інших суміжних галузей права, зокрема: В.Б. Авер'янов, І.В. Арістова, І.Л. Бачило, І.П. Голосніченко, О.Д. Довгань, Р.О. Додонов, І.М. Доронін, Л.В. Кузенко, О.І. Кутафін, В.Л. Манілов, О.В. Нестеренко, Х.В. Падалко, В.П. Пєтков, С.В. Пєтков, В.Л. Сидоренко, О.Ю. Синявська, С.Г. Стеценко, В. Тертичко, М.М. Тищенко, Ю.П. Тихомиров, О.М. Шевчук, В.К. Шкарупа та ін. Але питання щодо вдосконалення адміністративно-правового забезпечення кібербезпеки в Україні через досвід ЄС і НАТО у боротьбі з гібридними кіберзагрозами все ще залишаються недостатньо вивченими.

Метою статті є визначення напрямків удосконалення адміністративно-правового забезпечення кібербезпеки в Україні шляхом запозичення досвіду ЄС та НАТО щодо протидії гібридним кіберзагрозам.

Виклад основного матеріалу дослідження. Сьогодні, в умовах повномасштабної війни, в яку Україна була втягнута фактично ще в 2014 році, кібербезпека є надзвичайно важливою, оскільки кібератаки за своєю суттю являються ескалацією бойових дій у кіберпросторі, поширюючи новітні форми агресії та загрожуючи громадянам та суспільству, а в окремих випадках, і завдаючи реальної шкоди державі.

Гібридні загрози спрямовані на використання вразливості країн і спрямовані на підрив фундаментальних демократичних цінностей і свобод. Підходи Заходу до усвідомлення гібридних загроз базуються на контрзаходах: ЄС фокусується на кібербезпеці, протидії злочинності, нейтралізації ризиків, зміцненні стійкості суспільства та інформаційній безпеці.

НАТО та ЄС мають чітке розуміння того, що гібридним загрозам необхідно запобігати як «пасивним» елементам, таким як підвищення стійкості до потрясінь або несподіванок, і більш проактивним, включаючи жорсткі заходи для підготовки та захисту функцій і структур, які, швидше за все, стануть ціллю при гібридних атаках. У цьому контексті неможливо перебільшити важливість активних дій для зміцнення громадянської готовності, освіченого населення та ефективної правової структури [1].

Виділення певних заходів у напрямку протидії гібридним загрозам яскраво демонструє сформований пріоритет в ЄС. Подальший розвиток системи кібербезпеки в ЄС досить детально охарактеризовано в підсумкових документах, які були видані у вигляді: спільні комюніке Європейського Парламенту та Європейської Ради щодо реалізації заходів щодо протидії гібридним загрозам у Європейському Союзі, зокрема: 06.04.2016 [2]; 19.07.2017 [3]; 13 червня 2018 р. [4]; звіт про виконання плану дій 2016 року з протидії гібридним загрозам та Спільного повідомлення 2018 року щодо підвищення стійкості та посилення можливостей для подолання гібридних загроз від 28.05.2019 [5].

Загальний аналіз цих документів ЄС формує чітке уявлення про гібридність кіберзагроз та основні напрямки адміністративно-правового та організаційного забезпечення кібербезпеки, зокрема, боротьби з гібридними кіберзагрозами в Європейському Союзі. Основною метою цих щорічних звітних документів є представлення звіту Європейському Співтовариству про прогрес і наступні кроки у впровадженні дій у чотирьох сферах, запропонованих у Спільній діяльності: підвищення обізнаності про ситуацію: стійкість суспільства; зміцнення спроможності запобігати кризам і реагувати на них, а також координувати відновлення та розширення співпраці з НАТО для забезпечення взаємодоповнюваності в діяльності.

У розробці заходів з підвищення обізнаності щодо гібридних кіберзагроз наголос робиться на виявленні суспільної вразливості до них і скоординованих діях для оцінки цих загроз. Для виявлення ключових вразливостей з урахуванням конкретних гібридних показників проводиться аналіз ризиків, що впливають на установи та мережі.

Стосовно ризик-орієнтованого підходу доцільно відзначити прийняття Резолюції 57/239 «Елементи глобальної культури кібербезпеки» [6] Генеральною Асамблеєю ООН 20 грудня 2002 р., згідно з якою термін «кібербезпека» активно використовується в юридичній термінології. Показово, що ще у 2002 році в документах ООН вказувалося на необхідність оцінки ризиків з метою виявлення загроз і вразливостей. Глобальна культура кібербезпеки включає дев'ять взаємопов'язаних елементів, зокрема:

– обізнаність (тобто учасники повинні знати про необхідність безпеки інформаційних систем і мереж, а також про те, що вони можуть зробити для підвищення безпеки);

– відповідальність (учасники несуть відповідальність за безпеку мережі відповідно до своєї ролі);

– реагування (учасники мають вживати своєчасних та спільних заходів для запобігання, виявлення та реагування на інциденти безпеки, включаючи обмін інформацією та процедурами, які забезпечують оперативну та ефективну співпрацю у запобіганні, виявленні та реагуванні на такі інциденти); етичність (врахування законних інтересів інших);

– демократія (безпека повинна забезпечуватися у спосіб, який узгоджується з демократичними цінностями, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації, належний захист приватної інформації; відкритість і прозорість); оцінка ризиків (учасники повинні проводити періодичні оцінки ризиків для виявлення загроз і вразливостей, мати для цього відповідні технології та засоби контролю, враховуючи важливість інформації, що захищається);

– проектування та впровадження заходів безпеки;

– переоцінка (своєчасні заходи щодо внесення змін у політику, практику безпеки з урахуванням нових та змін у існуючих загрозах) [7, с. 72-73].

Резолюція ООН – не єдиний міжнародно-правовий документ, який наголошує на необхідності оцінки ризиків у системі кібербезпеки. Директива ЄС про заходи щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (NIS Directive) [8] встановлює єдині правила та вимоги у сфері кібербезпеки, але залишає кожну Держава-член має право вживати власних заходів щодо впровадження положень цієї Директиви в національне законодавство. Крім того, Директива вимагала від держав-членів впровадження цих правил до 9 травня 2018 року.

Це означає, що для підвищення спроможності забезпечувати кібербезпеку на національному рівні країни-члени ЄС повинні розробити національну стратегію мережевої та інформаційної безпеки, яка повинна включати: стратегічні цілі, пріоритети та державну основу; заходи щодо підготовки, реагування та відновлення після кіберінцидентів, принципи державно-приватного партнерства; програма освітніх, навчальних та просвітницьких заходів; план дослідження; план оцінки та управління ризиками; перелік зацікавлених сторін, відповідальних за реалізацію стратегії; визначити один або більше державних органів, які відповідатимуть за імплементацію Директиви; створити одну або кілька команд реагування на комп'ютерні надзвичайні ситуації.

Загалом для досягнення мети Директиви, забезпечення вищого рівня мережевої та інформаційної безпеки в межах Європейського Союзу, як необхідні заходи визначено три основні напрямки: підвищення спроможності системи кібербезпеки на національному рівні; підвищення рівня загальноєвропейського співробітництва; запровадження управління ризиками та зобов'язання повідомляти про кіберінциденти операторам базових послуг і постачальникам цифрових послуг. Таким чином, міжнародне право визначає управління ризиками не лише як рекомендацію, а й як обов'язковий елемент, що підвищує обізнаність про вразливість системи у сфері кібербезпеки.

Для розуміння проблем, які виникають у сфері кібербезпеки, а також пошуку шляхів їх вирішення важливим є дослідження історії та логіки виникнення поняття «ризик», його сутності, змісту та місця в сучасному суспільному розвитку. Загалом слід зазначити, що розвиток суспільства протягом досить тривалого історичного періоду певною мірою був позначений ризиком. Водночас відносно новим продуктом розвитку наукової думки стало усвідомлення ризикованості людської діяльності та її атрибутивності в процесах сучасного суспільного розвитку. Важливим завданням є з'ясування можливостей державного управління соціальними ризиками розвитку інформаційного суспільства в Україні.

Важливим елементом подальшого розвитку системи кібербезпеки України, особливо в умовах гібридної війни, є необхідність імплементації положень Директиви Європейського Парламенту та Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи щодо високого спільного рівня безпеки мережевих та інформаційних систем в Союзі (далі – NIS Directive) [9].

Положення цієї Директиви NIS містять низку вимог щодо підвищення рівня кібербезпеки. Зокрема, національні стратегії кібербезпеки стосуються таких питань: цілі та пріоритети національної стратегії безпеки мереж та інформаційних систем; рамки управління для досягнення цілей і пріоритетів національної стратегії безпеки мережевих та інформаційних систем, включаючи ролі та відповідальність державних органів та інших відповідних учасників; визначення інструментів готовності, реагування та відновлення, включаючи співпрацю між державним і приватним секторами; із зазначенням освітніх, навчальних та просвітницьких програм, пов'язаних із національною стратегією безпеки мережевих та інформаційних систем; зазначення планів досліджень та розвитку, пов'язаних із національною стратегією безпеки мережі та інформаційних систем; план оцінки ризиків для визначення ризиків; перелік різних учасників, залучених до реалізації національної стратегії безпеки мережевих та інформаційних систем.

Крім того, у статтях 14 і 16 першої вимоги щодо звітування про безпеку та інциденти зазначено, що держави-члени гарантують, що оператори базових послуг, а також постачальники цифрових послуг вживають технічних і організаційних заходів для управління системами ризиків мережевої та інформаційної безпеки, які вони використовують у своїй діяльності. Такі заходи мають забезпечити рівень безпеки мережевих та інформаційних систем, який відповідає ризику, що виник. Загалом у тексті Директиви NIS термін «ризик» вживається 17 разів, який у ст. 4 «Терміни та визначення» визначено наступним чином: «ризик» означає будь-яку обставину чи подію, яку можна обґрунтовано ідентифікувати та яка потенційно може негативно вплинути на безпеку мережі та інформаційних систем [9].

У зв'язку з імплементацією європейського законодавства в Україні, ми будемо змушені імплементувати ці положення Директиви NIS у вітчизняне законодавство. Чинний Закон України «Про основні засади забезпечення кібербезпеки України» не передбачає жодних заходів з оцінки ризиків у сфері кібербезпеки. На нашу думку, це є суттєвим недоліком чинного вітчизняного законодавства, який мотивується нами з кількох точок зору:

– об'єктивно сучасні процеси суспільного розвитку вимагають запровадження в управлінських рішеннях інституту наукового прогнозування, забезпечення якого методологічно знаходиться в площині безпеки та ґрунтується на ризик-орієнтованому підході до прогнозування;

– оцінка ризиків у сфері кібербезпеки України є не лише необхідністю сучасного етапу розвитку суспільства, а й вимогою формально-правового міжнародного законодавства, зокрема європейського, імплементація якого в Україні потребує впровадження та примусове виконання;

– з методологічної точки зору, оцінка ризику передбачає не тільки інформування про масштаби загрози в кіберсфері, але й уточнення стійкості суспільства в боротьбі з цими загрозами, що формує основу для визначення пріоритетів для підвищення стійкості системи кібербезпеки України;

– сучасний стан кібербезпеки в Україні безпосередньо залежить від активності агресора в кіберпросторі, а тому кіберзагрози нашому суспільству, перш за все, лежать не в площині внутрішніх факторів, а лише – зовнішньої цілеспрямованої діяльності спецслужб агресора, яка об'єктивно мотивує ефективну національну систему кібербезпеки в Україні.

Висновки. Чинне вітчизняне законодавство вимагає запровадження відповідних правил запровадження ризик-орієнтованого підходу в діяльності з кібербезпеки в Україні. Зокрема це стосується як Закону України «Про основні засади забезпечення кібербезпеки України» та Закону України «Про критичну інфраструктуру». Зокрема, нововведення цього змісту має містити визначення основних термінів: ризик-орієнтований підхід до кібербезпеки – принцип кібербезпеки, заснований на оцінці ризиків порушення прав і свобод, а також інтересів суспільства і держави в кіберпросторі та вжиття відповідних заходів з управління ризиками в кіберпросторі. спосіб і ступінь мінімізації таких ризиків залежно від їх рівня; ризик-орієнтований підхід до захисту критичної інфраструктури - принцип захисту критичної інфраструктури, що ґрунтується на оцінці ризиків порушення безпеки критичної інфраструктури, а також вжиття відповідних заходів з управління ризиками у спосіб та в обсязі, що мінімізує такі ризики залежно від їх рівня; ризики – рівень реальної загрози порушення прав і свобод, а також інтересів суспільства і держави в кіберпросторі (порушення безпеки критичної інфраструктури). Управління ризиками – комплекс заходів, які вживають суб'єкти кібербезпеки: ідентифікація та оцінка загроз і вразливостей національної системи кібербезпеки, оцінка ризиків загроз – і на цій основі прийняття відповідних управлінських рішень з мінімізації ризики.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Співпраця протидії гібридним загрозам. URL: https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnimzagrozam/index.html.

2. Спільне повідомлення Європейському парламенту та Раді про спільну рамкову програму протидії гібридам загрожує відповіддю Європейського Союзу. 2016. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52016JC0018.

3. Спільна доповідь Європейському Парламенту та Раді про імплементацію Спільної рамкової програми щодо протидії гібридним загрозам – відповідь Європейського Союзу. 2017. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52017JC0030.

4. Спільний звіт для Європейського Парламенту, Європейської Ради та Ради щодо імплементації Спільної рамкової програми щодо протидії гібридним загрозам з липня 2017 року по червень 2018 року. URL: https://eurlex.europa.eu/legal-content/EN /TXT/?uri=JOIN:2018:014:FIN.

5. Звіт про спільний робочий документ штабу про реалізацію Спільної рамкової програми 2016 року щодо протидії гібридним загрозам та Спільного повідомлення 2018 року з підвищення стійкості та зміцнення можливостей протидії гібридним загрозам. URL:https://eeas.europa.eu/.

6. Резолюція Генеральної Асамблеї ООН 57/329, прийнята на 78 пленарному засіданні 57 сесії. 20.12.2002. URL: https://documents-ddsny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement.

7. Довгань О. Д., Доронін І. М. (2017) Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту, Київ, 107 с.

8. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні. Матеріал для обговорення. URL: https://parlament.org.ua/wp-content/uploads/2017/12/au_White-book-on-cybersecurity-draft_5.pdf.

9. Директива Європейського Парламенту і Ради (IeS) 2016/1148 від 06.07. 2016 про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA.

REFERENCES:

1. Prevention against hybrid threats URL: https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnimzagrozam/index.html [in Ukrainian].

2. Speech to the European Parliament and Radiation about the joint framework program against hybrids

threatening the European Union. 2016. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52016JC0018.

3. Complimentary advice to the European Parliament and Radiation on the implementation of the Common Framework Program against hybrid threats – in support of the European Union. 2017. URL: https://eur-lex.europa.eu/
legalcontent/EN/TXT/?uri=CELEX%3A52017JC0030.

4. Speech for the European Parliament, for the sake of the European Parliament For the sake of implementing a joint framework program to counter hybrid threats from lime 2017 to earth 2018. URL: https://eurlex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2018:014:FIN.

5. A note about the joint working document to the headquarters on the implementation of the Joint Framework Program 2016 for the future against hybrid threats and the General information for 2018 against the future ї hybrid threats. URL: https://eeas.europa.eu/sites/eeas/.

6. Resolution of the UN General Assembly 57/329, adopted at the 78th plenary session of the 57th session. 12/20/2002. URL: https://documents-ddsny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement.

7. Dovgan O. D., Doronin I. M. (2017) Eskalatsiia kiberzahroz natsionalnym interesam Ukrainy ta pravovi aspekty kiberzakhystu [Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber defense], Kiev, 107 p. [in Ukrainian].

8. Propozytsii do polityky shchodo reformuvannia sfery kiberbezpeky v Ukraini. [Propositions for the policy of reforming cybersecurity in Ukraine.] Material for discussion. URL: https://parlament.org.ua/wp-content/uploads/2017/12/au_White-book-on-cybersecurity-draft_5.pdf [in Ukrainian].

9. Directive of the European Parliament and Radi (IeS) 2016/1148 of 06.07. 2016 about coming for a high-level level of security of mesh and information systems on the territory of the Union. URL: https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA [in Ukrainian].

Стаття надійшла до редакції: 20.05.2023

УДК 342.951
DOI: 10.36550/2522-9230-2023-14-147-152

Наливайко Олег Юрійович,
аспірант кафедри права та правоохоронної діяльності
Центральноукраїнського державного університету
імені Володимира Винниченка
e-mail: nalivaikooy@gmail.com
https://orcid.org/0000-0001-9660-1748

СПЕЦИФІКА СУБ'ЄКТІВ, ОБ'ЄКТІВ І НАПРЯМІВ ГРОМАДСЬКОГО КОНТРОЛЮ ЗА ДІЯЛЬНІСТЮ ОРГАНІВ СУДОВОЇ ВЛАДИ УКРАЇНИ

У статті на підставі аналізу норм чинного законодавства України визначено перелік і з'ясовано особливості головних суб'єктів, об'єктів і напрямів громадського контролю за діяльністю органів судової влади. Виділено суб'єктів загального, спеціального та спеціалізованого громадського контролю. До суб'єкти загального контролю віднесено громадян України, іноземців, осіб без громадянства; громадські організації, які здійснюють діяльність без статусу юридичної особи; громадські організації та громадські спілки зі статусом юридичної особи). Суб'єктами спеціального контролю є суб'єкти у сфері медіа та журналісти, а суб'єктами спеціалізованого контролю – Громадська рада доброчесності; Громадська рада при Раді суддів України; Громадська рада міжнародних експертів; Етична рада.

Визначено систему об'єктів громадського контролю за діяльністю органів судової влади, які виділено в такі групи: об'єкти контролю у сфері функціонування суддівського корпусу (сукупність суддів місцевих, апеляційних, вищими спеціалізованих судів, Верховного Суду); об'єкти контролю в організаційно-адміністративній сфері (апарати судів всієї системи судоустрою, ДСА України, ВККС України, Вища рада правосуддя); об'єкти контролю у сфері діяльності органів суддівського самоврядування (збори суддів різних рівнів, Рада суддів України, з'їзд суддів України).

Окреслено ключові напрямами громадського контролю за діяльністю органів судової влади, які відбивають відповідні сфери забезпечення належної ефективності та дієвості втілення судовими інституціями у практичну площину щодо: 1) врахування працівниками системи судоустрою засад судочинства, належної реалізації ними завдань правосуддя, виконання ними правових норм; реалізації гарантій незалежності судової влади, її функціонування на засадах соціально-правової відповідальності, діяльності доброчесного та високопрофесійного корпусу суддів; дотримання та виконання вимог антикорупційного законодавства; здійснення процедур проведення добору кандидатів для призначення на посаду судді вперше, проведення спеціальних перевірок і приймання кваліфікаційних іспитів; проведення кваліфікаційного оцінювання; створення умов функціонування Єдиної судової інформаційно-