УДК: 342.9:007
DOI: https://doi.org/10.32366/2523-4269-2020-70-1-89-97

Веселова Лілія Юріївна,
кандидат юридичних наук
(Одеський державний університет внутрішніх справ, м. Одеса)
ORCID: https://orcid.org/ 0000-0001-6665-0426

ЗМІСТ АДМІНІСТРАТИВНО-ПРАВОВИХ ЗАХОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В КІБЕРНЕТИЧНІЙ СФЕРІ

У статті розкрито зміст адміністративно-правових заходів забезпечення безпеки в кібернетичній сфері. Запропоновано власний перелік першочергових адміністративно-правових заходів забезпечення безпеки в кібернетичній сфері, а саме подальше посилення державного контролю; проведення виховної, роз'яснювальної роботи серед населення; державна підтримка науковців та створення необхідних умов для розвитку наукових досліджень у сфері забезпечення кібернетичної безпеки; ретельний відбір кадрів у спеціальні підрозділи, які протистоять кібернетичним загрозам; подальше вдосконалення законодавчої бази та посилення відповідальності за кібернетичні правопорушення (вивчення та запозичення зарубіжного досвіду).

Ключові слова: *адміністративно-правове забезпечення; адміністративно-правові заходи; кібернетична сфера; кібернетичний простір; адміністративний примус.*

Постановка проблеми. В умовах науково-технічної революції, яка призвела до інформатизації майже всіх сфер людського життя наша країна на належному рівні не може протистояти різним кібернетичним загрозам, у тому числі такому явищу, як «гібридна війна». Удала політика щодо припинення кібернетичних правопорушень неможлива без посилення та вдосконалення адміністративно-правових заходів забезпечення безпеки в кібернетичній сфері, направлених на запобігання, попередження та припинення зазначених вище протиправних діянь.

Аналіз останніх досліджень і публікацій. Проблематики реалізації адміністративно-правових заходів у різних сферах торкалися такі науковці, як Д. М. Бахрах, А. П. Клюшниченко, В. А. Лазаренко, Н. Г. Салищева, А. В. Самойленко, О. В. Ткаля, В. М. Хропанюк та багато інших, але при цьому питання стосовно адміністративно-правових заходів саме в кібернетичній сфері на належному рівні залишається ще не дослідженим.

Метою статті є визначення змісту адміністративно-правових заходів забезпечення безпеки в кібернетичній сфері.

Виклад основного матеріалу. Адміністративно-правове забезпечення національної (у тому числі й кібернетичної) безпеки починається з Конституції України [1], *у якій передбачається наявність певних прав та обов'язків для громадян, захист їхніх інтересів та гарантій щодо безпеки в різних сферах. Завдання із забезпечення кібернетичної безпеки покладається на державу, а держава своєю чергою через певні методи впливає на поведінку правопорушників (потенційних правопорушників) у кібернетичній сфері* (курсив мій. – *Л. В.*). У теорії права під методом розуміється сукупність прийомів та засобів (заходів), за допомогою яких утілюються в життя певні цілі [2, с. 47]. Таким чином, метод (у тій чи ін-

шій формі) зводиться до сукупності визначених правил, прийомів, способів, норм пізнання і діяльності. Він є системою принципів, вимог, які орієнтують суб'єкта на вирішення конкретного завдання, досягнення результатів у певній сфері діяльності [3]. Своєю чергою адміністративні методи забезпечують прямий вплив суб'єкта управління на керований об'єкт та поділяються на адміністративно-правові та адміністративно-організаційні методи, мають певну мету та здійснюють відповідний керуючий вплив [4]. Г. В. Грянка стверджує, що адміністративний метод повинен утілюватися в життя через застосування адміністративних (примусових) заходів, які часто мають обмежувальний та репресивний характер, при цьому його реалізація не потребує значних витрат як часу, так і фінансових ресурсів [5, с. 105]. *Тобто адміністративні методи втілюються через певні адміністративно-організаційні та адміністративно-правові заходи* (курсив мій. – *Л. В.*).

Визначимося зі змістом категорії «адміністративно-правові заходи» та її складовими. Слово «заходи» в академічному тлумачному словнику української мови означає сукупність дій або засобів для досягнення, здійснення чого-небудь [6, с. 380]. В адміністративному праві під заходом розуміють способи реагування оперативно-організаційного характеру, які за своїм змістом становлять зовнішній державно-правовий (психічний та фізичний) вплив на свідомість і поведінку людей у формі обмежень особистого, організаційного або майнового характеру, тобто тих чи інших несприятливих наслідків [7, с. 108].

В. М. Хропанюк стверджує, що правовий захід утворює цільний, системний юридичний механізм, який забезпечує врегульованість усієї сукупності суспільних відносин, що є предметом правового регулювання [8, с. 244]. В. А. Лазаренко, розглядаючи таку точку зору, доходить висновку, що правові заходи є механізмом правового регулювання. Загалом у юридичній науці під правовим заходом розуміють закріплені в нормах законодавства методи, прийоми, способи впливу на суспільні відносини з метою досягнення певного результату [7, с. 108]. Позиція Н. Г. Салищевої, А. П. Клюшниченка, А. В. Самойленка полягає в тому, що адміністративно-правові заходи забезпечення та захисту прав громадян характеризуються переважно у зв’язку з юрисдикційною діяльністю відповідних органів, тобто в обсязі діяльності, пов’язаної з вирішенням конкретних справ та використанням до правопорушників заходів примусу [9, с. 94]. О. В. Ткаля адміністративно-правові заходи визначає як систему державно-владних прийомів та способів здійснення адміністративно-правового впливу, що здійснюється в односторонньому порядку лише в передбачених правовими нормами випадках, спеціально уповноваженими на те суб’єктами, з метою запобігання, виявлення та припинення протиправної поведінки, відвернення можливих шкідливих наслідків, відновлення правового становища та в разі необхідності притягнення винних до відповідальності [10, с. 192].

Аналізуючи зміст адміністративно-правових заходів забезпечення безпеки в кібернетичній сфері, переконуємося, що вони зводяться не тільки до адміністративно-розпорядчих функцій спеціально уповноважених державою органів, а також об’єднують у собі виховні, профілактичні, попереджувальні методи та методи впливу, які використовуються з метою підтримання правопорядку в кібернетичному просторі. Також більшість науковців робить наголос на тому, що адміністративно-правові заходи реалізовуються через адміністративний примус (курсив мій. – *Л. В.*).

Адміністративна наука «адміністративний примус» трактує як особливий різновид державно-правового примусу, тобто визначені нормами адміністративного права способи офіційного фізичного або психологічного впливу уповноважених державних органів, а в деяких випадках і громадських організацій на фізичних та юридичних осіб у вигляді особистих, майнових, організаційних обмежень їхніх прав, свобод та інтересів у разі вчинення цими особами протиправних діянь (у сфері відносин публічного характеру) або в умовах надзвичайних обставин у межах окремого адміністративного провадження задля превенції та припинення протиправних діянь, забезпечення провадження у справах про правопору-

шення, притягнення винних осіб до відповідальності, попередження та локалізації наслідків надзвичайних ситуацій [11].

Адміністративний примус має велике значення в забезпеченні правопорядку. Завдяки застосуванню адміністративного примусу досягається мета попередження та припинення правопорушень, притягнення правопорушників до відповідальності, забезпечення громадського порядку та громадської безпеки в різноманітних сферах суспільного життя [12, с. 191]. Примус необхідний для охорони правопорядку, власності, прав та інтересів громадян і організацій, створення нормальних умов для діяльності апарату публічної влади. Це хоча й не головний, але важливий і необхідний метод панування [12, с. 192]. Адміністративіст Д. М. Бахрах пропонує примус трактувати як заперечення волі підвладного та зовнішній вплив на його поведінку. Оскільки команда не виконана, порушена воля того, хто панує, останній впливає на моральну, майнову, організаційну, фізичну сферу підвладного, щоб перетворити його волю, домогтися підпорядкування [13, с. 317]. *Тобто примус – це певний метод через який держава здійснює свою владу з метою управління суспільством* (курсив мій. – *Л. В.*).

М. І. Курочка вважає, що забезпечення законності й правопорядку, підтримання державної дисципліни потребують, щоб органи влади забезпечували втілення в життя державної волі, застосовуючи в разі необхідності до тих, хто не слідує цій волі, добровільні й примусові заходи, які допускаються законом [14, с. 133].

М. І. Єропкін заходи адміністративного примусу класифікував як заходи запобігання, заходи адміністративного припинення та адміністративні стягнення [15, с. 118]. Більшість науковців заходи адміністративного примусу в юридичні літературі традиційно умовно поділяють на три групи:

1) адміністративно-попереджувальні заходи (перевірка документів, огляд, унесення подання про усунення причин правопорушень тощо);

2) заходи адміністративного припинення (адміністративне затримання, вилучення речей та документів, примусове лікування, відсторонення від керування тощо);

3) адміністративні стягнення (попередження, штраф, позбавлення спеціального права, адміністративний арешт тощо). При цьому слід зауважити, що окремі заходи можуть мати чітко визначену мету застосування або багатоцільове призначення [16, с. 266–267].

У кібернетичній сфері примус як адміністративно-правовий захід застосовується за для забезпечення кібернетичної безпеки з метою покарання правопорушника чи попередження, припинення його протиправної поведінки в кіберпросторі. Зважаючи на специфічність правопорушень у кібернетичній сфері, юрисдикційні органи проводять виховну, роз'яснювальну роботу, здійснюють владно-примусові дії. Спеціально уповноважені органи в кібернетичній сфері використовують універсальні заходи переконання та примусу.

У нашій країні адміністративно-правові заходи забезпечення безпеки в кібернетичній сфері впливають, як правило, на економічні інтереси правопорушника, при цьому спеціально уповноважені державні органи не мають великого бажання розглядати справи про зазначені вище адміністративні правопорушення. Сказане вказує на необхідність запозичення норм іноземного досвіду інформаційного законодавства (що стосується кібернетичної сфери) та вдосконалення української законодавчої адміністративної бази із зазначеного питання (курсив мій. – *Л. В.*). Так, Закон Франції «Про інформатику, картотеки та свободи» до заходів припинення правопорушень, що вчиняються у сфері обігу інформації, зараховують: винесення суб'єкту діяльності у сфері телекомунікацій письмових приписів про усунення допущених порушень законодавства про інформатику, картотеки та свободи в галузі обігу інформації; блокування доменних імен суб'єкта інформаційної діяльності, який розміщує на своїх офіційних чи контрольованих вебсторінках заборонену інформацію чи таку, що порушує вимоги законодавства про захист суспільної моралі; тимчасове блокування доступу до баз персональних даних із можливістю подальшої заборони їхнього використання у зв'язку з порушенням законодавства про персональні дані; вклю-

чення електронного протоколу адреси сайту до реєстру заборонених інформаційних ресурсів з покладенням на його власника (управителя доменного імені) обов'язку з його видалення; надання суб'єктам телекомунікаційної діяльності обов'язкових приписів стосовно блокування доступу споживачів до конкретного інтернет-контенту [17].

Згідно з українським законодавством, за більшість проступків у кіберпросторі правопорушник притягається до кримінальної відповідальності. Кримінальний кодекс України містить велику кількість статей щодо злочинів у кібернетичній сфері: 6 статей об'єднані в один розділ – «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», усі інші статті «розкидано» по всьому нормативно-правовому акту, наприклад, ст. 190 КК України (частина щодо шахрайства, яке вчинене шляхом незаконних операцій з використанням інформаційно-телекомунікаційних систем), ст. 301 КК України (частина щодо збуту й розповсюдження порнографічних предметів саме через інформаційно-телекомунікаційні системи) [18] тощо. КУпАП також передбачає адміністративну відповідальність за правопорушення в кіберсфері. Стягнення за незаконні дії з використанням інформаційно-телекомунікаційних систем зводяться до накладення штрафу з конфіскацією незаконно збутих чи призначених для збуту копій баз даних, а також грошей, отриманих від їхнього продажу. До таких правопорушень належать: демонстрація та розповсюдження фільмів без державного свідоцтва на право розповсюдження та демонстрації фільмів (ст. 164^4), незаконне розповсюдження екземплярів аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних (ст. 164^9), здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем (ст. 212^6) [42] тощо. *Однак судова практика щодо розгляду адміністративних справ за правопорушення в кібернетичній сфері не сформована, відсутній чіткий алгоритм розгляду таких неправомірних дій, і, як підсумок, немає дієвого механізму захисту прав та інтересів інтернет-суспільства* (курсив мій. – *Л. В*.).

З огляду на сказане, під адміністративно-правовими заходами забезпечення безпеки в кібернетичній сфері пропонуємо розуміти сукупність правил, прийомів, способів, норм, які прописані законодавчими актами та існують для належної організації роботи спеціально уповноважених державою органів у кібернетичній сфері, що своєю чергою забезпечує кібернетичний порядок та має на меті попередження, припинення правопорушень та притягнення правопорушників до відповідальності. Так, усі адміністративно-правові заходи забезпечення кібернетичної безпеки складають цілісну систему. Для дієвого функціонування системи адміністративно-правових заходів забезпечення кібернетичної безпеки держава повинна дотримуватися чіткої дієвої політики щодо захисту об'єктів кіберпростору, а державні органи повинні чітко та на попередження реагувати у випадку кіберзагроз. До того ж вибір конкретних засобів і шляхів забезпечення кібернетичної безпеки України зумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру й масштабам реальних та потенційних кібернетичних загроз життєво важливим інтересам людини й громадянина, суспільства й держави [19, с. 300].

Наслідки після протиправних атак під час «війни нової генерації» можна зрівняти з наслідками після використання зброї масового ураження. Так, відомі непоодинокі інциденти, коли кібершахраї, впливаючи на свідомість через різні психологічні маніпуляції (соціальну інженерію, фішинг), ошукують громадян. Хакери дуже творчо використовують психологію під час створення нових кібератак та вірусів. Одним з останніх прикладів є проведення Росією розвідувальної кібероперації BugDrop у межах «гібридної війни», спрямованої на приватний сектор. Метою кібероперації було отримати віддалений доступ до персональних комп'ютерів, ноутбуків, смартфонів, планшетів та інших гаджетів працівників різних структур, унаслідок чого персональні дані та паролі працівників об'єктів критичної інфраструктури, засобів масової інформації і наукових установ викра-

далися і завантажувалися на файлообмінник Dropbox. Доступ до комп'ютерів зловмисники отримували, розсилаючи користувачам фішингові електронні листи, у яких закликали відкрити файл Microsoft Word, що містив шкідливий макрос. Тому одним натиском клавіші людина може наразити на небезпеку не лише свої дані, але й ті, які,у разі втрати, загрожують безпеці всієї держави. Подібні масштабні атаки, зазвичай, проводяться і організовуються не однією особою, а цілою групою хакерів за підтримки впливових організацій, зокрема силових структур. Організації та угруповання, які стоять за цими кібероперaціями, можна порівняти з митцем, який пише картину, використовуючи різні фарби, полотна та стилі [20]. Тож такі протизаконні дії в кіберпросторі, як вандалізм, збір інформації, пропаганда, порушення роботи інформаційно-телекомунікаційних систем та функціонування сайтів, протизаконний збір інформації із серверів та баз даних, атаки серверів стратегічних державних об'єктів та об'єктів критичної інфраструктури можуть призвести до найжахливіших наслідків для країни та суспільства. Для мінімізації ризиків від кіберзагроз необхідно застосовувати дієві та сучасні заходи забезпечення кібернетичної безпеки.

Першочерговими адміністративно-правовими заходами забезпечення безпеки в кібернетичній сфері повині стати:

1) подальше посилення державного контролю. Так, в Україні вже зроблено перші кроки – блокування інтернет-провайдерами доступу до вебресурсів інтернет-компаній «ВКонтакті», «Одноклассники», «Mail.ru», «Яндекс», «Лабораторія Касперського», «Dr.Web» [21], через які російські спецслужби мали можливість відслідковувати різну інформацію щодо українців. Наприклад, у США в публічних пунктах доступу до мережі Інтернет (бібліотеки, школи, інтернет-кафе тощо) примусово введено фільтри, які обмежують доступ до сайтів, що містять порнографію і екстремістські матеріали [22], що було б дуже доречним і в нашій країні;

2) проведення виховної, роз'яснювальної роботи серед населення, особливо серед найуразливіших категорій – дітей та літніх людей. Так, найчастіше діти страждають від булінгу в інтернет-просторі, тому необхідно розробити дієву антибулінгову програму «Стоп кібербулінг» із залученням психологів, викладачів, правоохоронців; проводити тренінги та курси з працівниками шкіл із зазначеної проблематики та семінари з батьками. За даними різних досліджень, майже кожен третій учень в Україні так чи інакше зазнавав булінґу в школі, потерпав від принижень і глузувань: 10 % – регулярно (раз на тиждень і частіше); 55 % – частково (з боку однокласників); 26 % батьків уважають своїх дітей жертвами булінґу [23]. Що стосується літньої категорії осіб, то вони найчастіше страждають від фішингу та соціальної інженерії. Також із подібною проблемою стикаються і працівники різних підприємств. З особами, які входять до групи ризику, необхідно проводити заняття (лекції, семінари), роз'яснювальні роботи, тренінги. Треба мати на увазі, що майже всі ми перебуваємо в єдиному мережевому просторі, і якщо навіть звичайний працівник або військовослужбовець постраждає від будь-якого вірусу, то по цьому ланцюжку може статися зараження на всіх рівнях [20];

3) державна підтримка науковців та створення необхідних умов для розвитку наукових досліджень у сфері забезпечення кібернетичної безпеки, поєднання сил, умінь, знань та доробок практиків і співпраця правоохоронців та кіберфахівців із науковцями в означеній сфері, налагодження контактів з установами інших держав, на зразок Інституту віртуальних досліджень у Великій Британії [24, с. 147];

4) ретельний відбір кадрів у спеціальні підрозділи, які протистоять кібернетичним загрозам та постійний моніторинг професіонального росту кіберфахівців, удосконалення їхніх навичок та знань (адже кількість різновидів кібернетичних загроз постійно зростає, методи боротьби з ними змінюються). Головним моментом тут також виступає оснащення фахівців сучасними технологіями для роботи та матеріальна підтримка як стимул доброчесно працювати на благо національних інтересів;

5) подальше вдосконалення законодавчої бази та посилення відповідальності за кібернетичні правопорушення (вивчення та запозичення зарубіжного досвіду).

Висновки. Адміністративно-правове забезпечення безпеки в кібернетичній сфері на сьогодні є одним із пріоритетних завдань державної політики, яке реалізується через сукупність адміністративно-правових заходів у кібернетичній сфері. Адміністративно-правові заходи забезпечення безпеки в кібернетичній сфері – це єдиний комплекс, який забезпечує своєчасну та організовану реакцію спеціально уповноважених державою органів на протиправну поведінку правопорушника. Усі елементи системи адміністративно-правових заходів забезпечення правопорядку в кібернетичній сфері тісно пов'язані між собою та є рівноцінно важливими під час забезпечення безпеки в кібернетичній сфері.

Список використаних джерел

1. Конституція України : прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 02.02.2020).
2. Тихомиров Ю. А. Курс административного права и процесса. Москва, 1998. 798 с.
3. Щерба С. П., Заглада О. А. Філософія : підручник. URL : https://pidruchniki.com/11080803/filosofiya/ponyattya_metoda_metodologiyi (дата звернення: 05.02.2020).
4. Адміністративні методи : [сайт]. URL : https://pidruchniki.com/1280052845142/pravo/administrativni_metodi (дата звернення: 05.02.2020).
5. Грянка Г. В. Поняття та класифікація адміністративно-правових заходів протидії корупції. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2009. Вип. 20. С. 103–110.
6. Словник української мови / за ред. І. К. Білодіда. У 11 томах. АН УРСР. Інститут мовознавства. Київ, 1972. Том 3. 380 с.
7. Лазаренко В. А. Адміністративно-правове регулювання екологічної безпеки в Україні : дис. ... канд. юрид. наук : 12.00.07. Держ. НДІ МВС України. Київ, 2010, с. 209.
8. Хропанюк В. Н. Теория государства и права : учебник для вузов. Москва : Омега-Л Интерстиль. 2008. 384 с.
9. Ієрусалімова І. О. Механізм адміністративно-правового забезпечення прав і свобод людини та громадянина : дис. ... канд. юрид. наук : 12.00.07. Інститут законодавства Верховної Ради України. Київ, 2006. 205 с.
10. Ткаля О. В. Проблеми поняття адміністративно-правових заходів. *Приватне право в умовах глобалізації : ключові проблеми модернізації сучасного права* : зб. наук. пр.; за ред. П. М. Шапірка, І. Г. Оборотова; МОН України, НУ ОЮА. Миколаїв : Іліон, 2015. С. 187–192.
11. *Бурбика* М. М., Солонар А. В., Янішевська К. Д. *Адміністративне право* України : навчальний посібник. URL : https://pidruchniki.com/79651/pravo/administrativniy_primus (дата звернення: 10.02.2020).
12. Іванникова В. В. Адміністративний примус, обумовлений необхідністю припинення правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2011. № 2. С. 190–197.
13. Бахрах Д. Н. Административное право : учебник для вузов. Москва : НОРМА. 2001. 443 с.
14. Курочка М. І. Адміністративний примус: суть та визначення. *Форум права.* 2015. № 4. С. 133–136.
15. Еропкин М. И. Управление в области общественного порядка. Москва : «Лениздат». 1973. 210 с.
16. Ткаля О. В. Класифікація заходів адміністративно-правового примусу. *Новітні кримінально-правові дослідження.* 2015. С. 264–267.
17. Об информатике, картотеках и свободах : Закон Франции от 06.01.1978 № 78–17. Iournal official de la Republique Fracaise. 7 januier 1978, 25 januier 1978.
18. Кримінальний кодекс України : прийнятий 5 квітня 2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. URL : https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 11.02.2020).

19. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 2 (28). С. 299–309.

20. Кібербезпека як важлива складова всієї системи захисту держави : [сайт]. URL : http://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html (дата звернення: 22.01.2020).

21. Рішення починає діяти : [сайт]. URL : https://tsn.ua/ukrayina/ukaz-pro-blokuvannya-rosiyskih-saytiv-ta-socmerezh-nabuv-chinnosti-930642.html (дата звернення: 04.02.2020).

22. Гусев А. В. Зарубежный опыт борьбы с преступлениями в сфере Интернета : [сайт]. URL : www.pravo.by/Conf2010/reports/Gusev.doc (дата звернення: 10.02.2020).

23. Протидія булінгу : [сайт]. URL : http://llt.multycourse.com.ua/ua/page/22/103#3 (дата звернення: 12.02.2020).

24. Демедюк С. В. Окремі питання адміністративно-правового та організаційного забезпечення кібербезпеки. *Південноукраїнський правничий часопис*. 2015. № 2. С. 144–147.

References

1. Konstytutsiia Ukrainy [Constitution of Ukraine] : pryiniata na piatii sesii Verkhovnoi Rady Ukrainy 28 chervnia 1996 r. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 [in Ukrainian].

2. Tihomirov, YU. A. (1998). Kurs administrativnogo prava i processa [Administrative Law and Process Course]. M., 798 s. [in Russian].

3. Shcherba S. P., Zahlada O. A. Filosofiia [Philosophy] : pidruchnyk URLhttps://pidruchniki.com/11080803/filosofiya/ponyattya_metoda_metodologiyi [in Ukrainian].

4. Administratyvni metody [Administrative methods] : [sait]. URL : https://pidruchniki.com/1280052845142/pravo/administrativni_metodi [in Ukrainian].

5. Hrianka, H. V. (2009). Poniattia ta klasyfikatsiia administratyvno-pravovykh zakhodiv protydii koruptsii. Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka) [Concept and classification of administrative and legal measures against corruption. Combating Organized Crime and Corruption (Theory and Practice)]. Vyp. 20. S. 103–110. [in Ukrainian].

6. Slovnyk ukrainskoi movy. (1972). [Dictionary of the Ukrainian language]. za red. I. K. Bilodida. [v 11 tomakh]. AN URSR. Instytut movoznavstva. K., Tom 3. 380 s. [in Ukrainian].

7. Lazarenko, V. A. (2010). Administratyvno-pravove rehuliuvannia ekolohichnoi bezpeky v Ukraini [Administrative and legal regulation of environmental safety in Ukraine] : dys. ... kand. yuryd. nauk : 12.00.07. Derzh. NDI MVS Ukrainy. Kyiv, s. 209. [in Ukrainian].

8. Hropanyuk, V. N. (2008). Teoriya gosudarstva i prava [Theory of State and Law] : uchebnik dlya vuzov. M. : Omega-L Interstil'. 384 s. [in Russian].

9. Iierusalimova, I. O. (2006). Mekhanizm administratyvno-pravovoho zabezpechennia prav i svobod liudyny ta hromadianyna [Mechanism of administrative and legal support of human and citizen's rights and freedoms] : dys. ... kand. yuryd. nauk : 12.00.07. Instytuti zakonodavstva Verkhovnoi Rady Ukrainy. Kyiv, 205 s. [in Ukrainian].

10. Tkalia, O. V. (2015). Problemy poniattia administratyvno-pravovykh zakhodiv. Pryvatne pravo v umovakh hlobalizatsii : kliuchovi problemy modernizatsii suchasnoho prava [Problems of the concept of administrative and legal measures. Private law in the context of globalization: key problems of modern law modernization] : zb. nauk. pr.; za red. P. M. Shapirka, I. H. Oborotova; MON Ukrainy, NU OIuA. Mykolaiv : Ilion, S. 187–192. [in Ukrainian].

11. *Burbyka, M. M., Solonar, A. V., Yanishevska, K. D. Administratyvne pravo Ukrainy* [Administrative law of Ukraine] *: navchalnyi posibnyk* URL : https://pidruchniki.com/79651/pravo/administrativniy_primus [in Ukrainian].

12. Ivannykova, V. V. (2011). Administratyvnyi prymus, obumovlenyi neobkhidnistiu prypynennia pravoporushennia [Administrative coercion due to the need to end the offense]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E. O. Didorenka*. № 2. S. 190–197. [in Ukrainian].

13. Bahrah, D. (2001). Administrativnoe pravo [Administrative law] : uchebnik dlya vuzov. M. : NORMA, 443 s. [in Russian].

14. Kurochka, M. I. (2015). Administratyvnyi prymus [Administrative coercion: essence and definition]: sut ta vyznachennia. *Forum prava*. № 4. S. 133–136. [in Ukrainian].

15. Eropkin, M. I. (1973).Upravlenie v oblasti obshchestvennogo poryadka [Public Order Management]. M. : «Lenizdat». 210 s. [in Russian].

16. Tkalia, O. V. (2015). Klasyfikatsiia zakhodiv administratyvno-pravovoho prymusu. Novitni kryminalno-pravovi doslidzhennia [Classification of measures of administrative and legal coercion. Recent criminal investigations]. S. 264–267. [in Ukrainian].

17. Ob informatike, kartotekah i svobodah [About computer science, file cabinets and freedoms] : Zakon Francii ot 06.01.1978 № 78 –17. Iournal official de la Republique Fracaise. 7 januier 1978, 25 januier 1978.

18. Kryminalnyi kodeks Ukrainy [Criminal codex of Ukraine] : pryiniatyi 5 kvitnia 2001 r. № 2341-III. *Vidomosti Verkhovnoi Rady Ukrainy*. 2001. № 25–26. URL : https://zakon.rada.gov.ua/laws/show/2341-14 [in Ukrainian].

19. Shelomentsev, V. P. (2012). Sutnist orhanizatsiinoho zabezpechennia systemy kibernetychnoi bezpeky Ukrainy ta napriamy yoho udoskonalennia. Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka) [The essence of organizational support of the cyber security system of Ukraine and directions of its improvement. Combating Organized Crime and Corruption (Theory and Practice)]. № 2 (28). S. 299–309. [in Ukrainian].

20. Kiberbezpeka yak vazhlyva skladova vsiiei systemy zakhystu derzhavy [Cybersecurity is an important component of the entire system of state protection] : [sait]. URL : http://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html [in Ukrainian].

21. Rishennia pochynaie diiaty [The decision takes effect] : [sait]. URL : https://tsn.ua/ukrayina/ukaz-pro-blokuvannya-rosiyskih-saytiv-ta-socmerezh-nabuv-chinnosti-930642.html [in Ukrainian].

22. Gusev A. V. Zarubezhnij opit bor'bi s prestupleniyami v sfere Interneta [Foreign experience in the fight against Internet crime] : [sajt]. URL : www.pravo.by/Conf2010/reports/Gusev.doc. [in Russian].

23. Protydiia bullinhu [Countering Bulling] : [sait]. URL : http://llt.multycourse.com.ua/ua/page/22/103#3 [in Ukrainian].

24. Demediuk, S. V. (2015). Okremi pytannia administratyvno-pravovoho ta orhanizatsiinoho zabezpechennia kiberbezpeky [Some issues of administrative and legal support for cybersecurity]. *Pivdennoukrainskyi pravnychyi chasopys*. № 2. S. 144–147. [in Ukrainian].

Veselova Liliya,
Phd in Law
(Odessa state university of internal affairs, Odessa)
ORCID: https://orcid.org/ 0000-0001-6665-0426

CONTENTS OF THE ADMINISTRATIVE AND LEGAL SECURITY IN THE CYBER SECTOR

During the study of the legislation and scientific developments on ensuring national (cyber) security through administrative and legal measures, it is observed that the task of ensuring cyber security is entrusted to the state, and the state in its turn influences the behavior of offenders (potential offenders) in the cyber sphere through certain methods. In the analysis of the content of administrative and legal means for security in the cybernetic field, it is concluded that they are reduced not only to administrative and administrative functions specially authorized by the state bodies, but also combine educational, preventive, preventive methods and means used for the purpose maintaining law and order in cyberspace. Thus, under the administrative and legal measures for cyber security, the article proposes to understand the set of existing rules, techniques, methods, norms that exist for the proper organization of work of specially authorized bodies in the cyber sphere, and rules, norms, requirements for cyber users. Given that the scientific world lacks a unified position on the systematization of administrative and legal means of security in the cybernetic sphere, because of the separation of various features, it is suggested to consider the main features of administrative and legal measures for security in the cybernetic sphere: spiritual and cultural guarantees (legal and cultural awareness) and legal safeguards (legal liability and legal control); certain (special) conditions for implementation of cyber security; complex methods of administrative prevention, prevention and administrative cessation of illegal behavior using information and telecommunication systems and Internet environment; is governed primarily by the rules of administrative law. The article goes on to say that for the effective functioning of the system of administrative and legal measures to ensure cyber security, the state must adhere to a clear effective policy for the protection of cyberspace objects, and the state authorities should respond clearly and in the case of cyber threats. The definition of a system of administrative and legal measures for ensuring security in the cybernetic sphere, as development, realization of public relations

occurring in the cybernetic environment and protected by specially authorized by the state bodies through a set of rules of law set of methods of protection of outlined relations in cybernetic space. As a result of the study of the above, it is said that Administrative and legal security of cyber security is now one of the priorities of public policy, which is implemented through a set of administrative and legal measures in the cyber sphere. Administrative and security measures in the cyber sphere are the only complex that provides timely and organized reaction of specially authorized by the state bodies to the illegal behavior of the offender. All elements of the cyber-law enforcement system are closely interconnected and are equally important in cyber security.

Key words: *administrative and legal support; administrative and legal measures; guarantee; cybernetic sphere; administrative coercion.*

Надійшла до редколегії 19.02.2020