ЩОДО ПИТАННЯ АДМІНІСТРАТИВНО-ПРАВОВОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ У СФЕРІ КІБЕРБЕЗПЕКИ

БОКОВ Іван Дмитрович - аспірант кафедри конституційного, адміністративного та фінансового права Академії праці, соціальних відносин і туризму

ORCID 0009-0000-4606-6943

УДК 347.83:34:002.1
DOI 10.32782/EP.2023.4.5

У статті здійснюється комплексний аналіз особливостей застосування адміністративної відповідальності за правопорушення у сфері кібербезпеки в Україні. Визначається, що під час розгляду правопорушень у сфері обігу інформації, що передбачені Кодексом України про адміністративні правопорушення, виникають певні складнощі, оскільки чинний Кодекс не має окремої глави, присвяченої саме вказаним проступкам, а правопорушення, які можна було б включити до цієї глави, розташовані у різних главах Особливої частини Кодексу. З'ясовано, що адміністративна відповідальність у сфері кібербезпеки може бути застосована за вчинення трьох груп правопорушень: пов'язаних із забезпеченням доступу фізичних та юридичних осіб до публічної інформації, необхідної для реалізації їх прав, свобод та законних інтересів; пов'язаних із забезпеченням обмеження доступу до певних відомостей, розповсюдження яких може спричинити негативний вплив правам та свободам громадян, законній діяльності юридичних осіб або національній безпеці; пов'язаних із забезпеченням безпеки у сфері медіаінформації". Запропоновано, з метою згуртування статей Кодексу України про адміністративні правопорушення, що стосуються застосування адміністративної відповідальності за правопорушення у сфері кібербезпеки, виділити окремий розділ у кодексі – "Адміністративні правопорушення, пов'язані із забезпеченням інформаційної безпеки".

Ключові слова: адміністративна відповідальність, інформація, безпека, кібератаки, кіберпростір, правопорушення.

Актуальність обраної теми

У сучасних умовах науково-технічної революції, що, у свою чергу, охопила процесами інформатизації всі сфери суспільного життя, Україна на достатньому рівні все ще не може протистояти різноманітним кібернетичним загрозам, особливо що стосується понять, пов'язаних з "гібридною війною". Вдала 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.

Проблематика правопорушень в інформаційній сфері стає все більш актуальною з розвитком інформаційних технологій. Дискусії ведуться навколо поєднання і співвідношення корпоративних норм обробки інформації, закріплених переважно у політиках конфіденційності або безпеки, з вимогами національного законодавства щодо цивільно-правової, адміністративно-правової, кримінально-правової охорони різних категорій інформації. Численні кібератаки та кіберінциденти як в Україні, так і у всьому світі зумовлюють підвищення уваги державних органів і, відповідно, науковців до проблематики боротьби з правопорушеннями в інформаційній сфері.

Крім того, під час розгляду правопорушень у сфері обігу інформації, що передбачені Кодексом України про адміністративні

правопорушення (далі – КУпАП), виникають певні складнощі, оскільки чинний КУпАП не має окремої глави, присвяченої саме вказаним проступкам, а правопорушення, які можна було б включити до цієї глави, розташовані у різних главах Особливої частини КУпАП.

Аналіз останніх досліджень та публікацій підтверджує актуальність обраної тематики в публікаціях наукової спільноти, серед яких можливо виділити праці: Юртаєва К.В., Пивоварова В.В., Лисенко С.Ю., Козирєвої В. П., Гаврилішина А. П., Педешко А.І., Перун Т.С., Веселова Л. Ю., Бараненко Р.В., Марущак А.І., Бухарєва В.В., Тарасюк А.В та інших.

Метою дослідження виступає здійснення комплексного аналізу особливостей застосування адміністративної відповідальності за правопорушення у сфері кібербезпеки в Україні.

Виклад основного матеріалу

Адміністративно-правове забезпечення національної (у тому числі й кібернетичної) безпеки регламентується перш за все положеннями основного Закону України – Конституції України, 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 у свою чергу, за допомогою певних методів впливає на поведінку правопорушників (чи/або потенційних правопорушників) у кібернетичній сфері. Також основним Законом закріплено право кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб, за винятком спеціально визначених у законі обставин (ст. 34 Конституції України). Таке обмеження здійснюється в межах правового інституту інформації з обмеженим доступом, що поділяється на таємну та конфіденційну [1]

На сьогодні можна із впевненістю констатувати, що одними із найпоширеніших правопорушень є порушення у кіберпросторі. Варто підкреслити, що вчинення таких правопорушень може не тільки мати негативні наслідки для кожного окремого громадянина, а й нести небезпеку для всієї держави взагалі. Саме тому важливого значення набуває інститут юридичної відповідальності за порушення законодавства у сфері кібербезпеки України. Взагалі ж "відповідальність" у науковій літературі в більшості випадків трактується лише як підзвітність (accountability) і усвідомлення осудності (immutability). У юридичній ж науці феномен відповідальності вивчається головним чином у плані покарання (punishability). Важливо також відзначити той факт, що термін "відповідальність" вперше ввів у науковий обіг Альфред Бен, який тлумачив її саме в значенні "покарання" [2].

На переконання Лук'янця Д.М., юридична відповідальність — це регламентована правовими нормами реакція з боку уповноважених суб'єктів на діяння фізичних або юридичних осіб (колективних суб'єктів), що проявляються в недотриманні встановлених законом заборон, невиконанні встановлених законом обов'язків, порушенні цивільно-правових зобов'язань, нанесенні шкоди або завданні збитків, і виражена в застосуванні до осіб, які вчинили такі діяння, засобів впливу, що тягнуть за собою позбавлення особистого, майнового або організаційного характеру [3, с. 15].

Відповідно до положень основного законодавчого акту, яким передбачено відповідальність за правопорушення у сфері кібербезпеки – Закон України "Про основні засади забезпечення кібербезпеки України", визначено, що "особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення злочину, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом" [4.].

Тобто із зазначеного положення випливає, що до суб'єктів, котрі вчинили правопорушення в зазначеній сфері, можуть застосовуватися такі види юридичної відпові-

дальності, як цивільна, адміністративна та кримінальньно-правова відповідальність. Самим же законодавчим актом не визначено вичерпного переліку правопорушень, за вчинення яких може наступати один із різновидів юридичної відповідальності.

Щодо загального поняття адміністративної відповідальності, то під такою відповідальністю зазвичай розуміють – застосування до осіб, які вчинили адміністративні проступки, адміністративних стягнень, що тягнуть для цих осіб обтяжливі наслідки майнового, морального, особистого чи іншого характеру і накладаються уповноваженими на те органами чи посадовими особами на підставах і в порядку, встановлених нормами адміністративного права [5, с.66].

Виходячи з досліджень провідного науковця в галузі адміністративного права В.К. Колпакова, адміністративна відповідальність – це специфічне реагування держави на адміністративне правопорушення, що полягає у застосуванні уповноваженим органом або посадовою особою передбаченого законом стягнення до суб'єкта правопорушення. Як явище правової дійсності, така відповідальність характеризується двома видами ознак: по-перше, це ознаки, властиві юридичній відповідальності в цілому (основні); по-друге, ознаки, що відмежовують адміністративну відповідальність від інших видів юридичної відповідальності (похідні). Основні ознаки адміністративної відповідальності, як зазначає автор, полягають у тому, що вона: 1) є засобом охорони встановленого державою правопорядку; 2) нормативно визначена і полягає в застосуванні (реалізації) санкцій правових норм; 3) є наслідком винного антигромадського діяння; 4) супроводжується державним і громадським осудом правопорушника і вчиненого ним діяння; 5) пов'язана з примусом, з негативними для правопорушника наслідками (морального або матеріального характеру), яких він має зазнати; 6) реалізується у відповідних процесуальних формах [6, с.121].

Важливість аналізу загальних понять, таких, як юридична відповідальність у цілому та адміністративна відповідальність, зокрема, пояснюється тим, що це є базисом, своєрідною основою для решти збірних понять, які стосуються відповідальності. Не є винятком і поняття адміністративної відповідальності за правопорушення у сфері кібербезпеки.

Складності аналізу адміністративної відповідальності за правопорушення у сфері кібербезпеки додає те, що в наукових колах не існує одностайної позиції щодо тих різновидів адміністративних правопорушень, які будуть зараховуватися до сфери кібербезпеки. Це пов'язано перш за все зі складністю поставлених завдань, що обумовлюється об'єктивними факторами, які пов'язані зі специфікою кіберправопорушень. Як зазначає К.В. Юртаєва, до них відносяться:

– транскордонний характер комп'ютерних правопорушень;

–неузгодженість юрисдикційних актів протидії кіберправопорушенням (позитивні і негативні конфлікти юрисдикцій);

– постійне вдосконалення ззасобів та методів вчинення кіберправопорушень;

– орієнтація кримінального і адміністративного законодавства на традиційні моделі вчинення та поширення правопорушень;

– складність та суперечливість процесу кваліфікації правопорушень;

– недоліки процесуального законодавства щодо отримання, фіксації та дослідження електронних правопорушень [7, с.221].

Важливим є також окреслення основних ознак адміністративної відповідальності у сфері кібербезпеки. Так, на думку С.Т. Гончарук, основними ознаками адміністративної відповідальності, як категорії загальної є: один із видів державного примусу, зокрема, адміністративний його різновид (одна із ланок заходів адміністративного примусу); це специфічна форма правового регулювання з боку держави в особі її компетентних органів на певну категорію протиправних проявів; своєрідні правовідносини між органами (посадовими особами), що її застосовують, та правопорушниками, причому в таких правовідносинах відсутні елементи службового під-

порядкування; юридичною підставою для настання адміністративної відповідальності, як правило, є окремий вид правопорушень – адміністративні проступки; один із самостійних видів правової відповідальності; державно-репресивний захід як результат протиправної поведінки особи; один із важливих адміністративно-правових інститутів, нормами якого значною мірою охороняється велика кількість суспільних відносин, урегульованих як адміністративно-правовими нормами, так і нормами інших галузей права; суб'єктами адміністративно-правової відповідальності можуть бути як фізичні, так і юридичні особи (наприклад, при порушенні правил пожежної безпеки, законодавства про об'єднання громадян, тощо) [8, с. 20–21].

Взагалі в КУпАП міститься близько сотні статей, за якими регулюються питання відповідальності щодо порушення порядку створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації. З цього приводу досить вдалою є думка Т.С. Перуна, який говорить про те, що "такі правопорушення можна поділити на три основні групи, а саме:

а) забезпечення доступу фізичних та юридичних осіб до публічної інформації, необхідної для реалізації їх прав, свобод та законних інтересів;

б) забезпечення обмеження доступу до певних відомостей, розповсюдження яких може спричинити негативний вплив правам та свободам громадян, законній діяльності юридичних осіб або національній безпеці;

в) забезпечення безпеки у сфері медіа-інформації" [9, с. 156].

Таким чином, можливо припустити, що адміністративна відповідальність у сфері кібербезпеки може наступати у випадку вчинення правопорушення: пов'язаного із забезпеченням доступу фізичних та юридичних осіб до публічної інформації, необхідної для реалізації їх прав, свобод та законних інтересів; пов'язаного із забезпеченням обмеження доступу до певних відомостей, розповсюдження яких може спричинити негативний вплив правам та свободам громадян, законній діяльності юридичних осіб або національній безпеці; пов'язаного із забезпеченням безпеки у сфері медіа-інформації".

Якщо виходити з позиції того, що адміністративна відповідальність за правопорушення у сфері кібербезпеки є збірним поняттям та різновидом адміністративної відповідальності, то її можливо визначити як застосування до особи, яка вчинила правопорушення, санкцій, що передбачені в нормах адміністративного права. Частіше за все, такі санкції відображають матеріальний (грошовий) характер. Принагідно зауважимо, що за чинним КУпАП окремо не виділяється розділ, який присвячується правопорушенням у сфері кібербезпеки. Проте, окремі науковці дають посилання на статті КУпАП, які таку відповідальність, безумовно, передбачають. Наприклад, однією з таких є ст.51-2 КУпАП, за якою "незаконне використання об'єкта права інтелектуальної власності (літературного чи художнього твору, їх виконання, фонограми, передачі організації мовлення, комп'ютерної програми, бази даних, наукового відкриття, винаходу, корисної моделі, промислового зразка, знака для товарів і послуг, топографії інтегральної мікросхеми, раціоналізаторської пропозиції, сорту рослин тощо), привласнення авторства на такий об'єкт або інше умисне порушення прав на об'єкт права інтелектуальної власності, що охороняється законом, – тягне за собою накладення штрафу від десяти до двохсот неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно виготовленої продукції та обладнання і матеріалів, які призначені для її виготовлення" [10].

У свою чергу, відповідно до ст. 164-9 КУпАП зазначається, що "розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних, упаковки яких не марковані контрольними марками або марковані контрольними марками, що мають серію чи містять інформацію, які не відповідають носію цього примірника, або номер, який не відповідає даним Єдиного реєстру одержувачів контрольних марок, – тягне за собою накладення штрафу від десяти до ста

неоподатковуваних мінімумів доходів громадян з конфіскацією цих примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних" [10] тощо.

На думку Веселової Л.Ю., 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) 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 [11, с. 92].

І наостанок варто зазначити, що протягом 2022 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано близько 58 мільярдів подій, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки, детектовано 181 мільйон підозрілих подій інформаційної безпеки (при первинному аналізі), опрацьовано 179 тисяч критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу), зафіксовано та оброблено безпосередньо аналітиками безпеки 415 кіберінцидентів. Порівняно з 2021 роком, кількість подій ІБ зросла: – у категорії «Шкідливий програмний код» у 18,3 рази; – у категорії «Збір інформації зловмисником» у 2,2 рази [12]. Це підтверджує те, що Україна є вразливою до правопорушень у сфері кібербезпеки, а тому потребує забезпечення належного рівня правового захисту, у тому числі заходів адміністративного захисту, серед яких важливе місце займає адміністративна відповідальність.

Висновки

Таким чином, адміністративна відповідальність може бути застосована за вчинення трьох груп правопорушень: пов'язаних із забезпеченням доступу фізичних та юридичних осіб до публічної інформації, необхідної для реалізації їх прав, свобод та законних інтересів; пов'язаних із забезпеченням обмеження доступу до певних відомостей, розповсюдження яких може спричинити негативний вплив правам та свободам громадян, законній діяльності юридичних осіб або національній безпеці; пов'язаних із забезпеченням безпеки у сфері медіаінформації".

Зважаючи на постійне збільшення кількості кібератак та наявності на території України з 2022 року запровадженого правового режиму воєнного стану, постійної військової агресії сусідньої держави, інформаційна сфера стала надзвичайно вразливим місцем України. У зв'язку з чим вважаємо за необхідне певним чином структурувати статті КУпАП з метою їхнього згрупування в одному розділі Особливої частини. Також можливе буде виділення окремого розділу – "Адміністративні правопорушення, пов'язані із забезпеченням інформаційної безпеки".

Література

1. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%8

2. Баранова Н. М. Етика: навч, посіб. Ніжин: НДУ ім. М. Гоголя, 2015. 323 с.

3. Лук'янець Д. М. Інститут адміністративної відповідальності: проблеми розвитку: монографія. Київ: Інститут

держави і права ім. В. М. Корецького НАН України, 2001. 136 с.

4. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

5. Педешко А.І. Адміністративна відповідальність за порушення митних правил: дис... канд. юрид. наук: 12.00.07 / Університет внутрішніх справ. Харків, 2000. 176 с.

6. Колпаков В. К. Адміністративне право України. Київ: Юрінком-Інтер, 2004. 724 с.

7. Юртаєва К.В. Проблеми криміналізації незалежного використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем чи їх частин. Ф. П. 2017. № 3. С. 221-227.

8. Перун Т. С. Адміністративна відповідальність в системі заходів забезпечення інформаційної безпеки. ІТ-право: проблеми і перспективи розвитку в Україні: збірник матеріалів II Міжнародної науково-практичної конференції (Львів, 17 листопада 2017 р.) Львів, Національний університет «Львівська політехніка». 2017. С. 155–160.

9. Гончарук С. Т. Адміністративна відповідальність за законодавством України. Київ: КМУЦА, 1995. 78 с.

10. Кодекс України про адміністративні правопорушення: Закон УРСР від 7 грудня 1984 року № 2755-VI: Закон України від https://zakon.rada.gov.ua/laws/show/80731-10

11. Веселова Л. Ю. Зміст адміністративно-правових заходів забезпечення безпеки в кібернетичній сфері. Правовий часопис Донбасу. 2020. № 1. С. 89–97. URL: http://nbuv.gov.ua/UJRN/pppd_2020_1_13.

12. ЗВІТ ПРО РОБОТУ СИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ ЗА 2022 рік. URL: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf

References

1. Constitution of Ukraine: Law of Ukraine of June 28, 1996 No. 254k/96-BP. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%8

2. Baranova N. M. Ethics: teach, guide. Nizhyn: NSU named after M. Gogol, 2015. 323 p.

3. Lukyanets D. M. Institute of administrative responsibility: problems of development: monograph. Kyiv: Institute of State and Law named after V. M. Koretsky National Academy of Sciences of Ukraine, 2001. 136 p.

4. On the main principles of ensuring cyber security of Ukraine: Law of Ukraine dated October 5, 2017 No. 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

5. Pedeshko A.I. Administrative responsibility for violation of customs rules: dis... candidate. law Sciences: 12.00.07 / University of Internal Affairs. Kharkiv, 2000. 176 p.

6. Kolpakov V. K. Administrative law of Ukraine. Kyiv: Yurinkom-Inter, 2004. 724 p.

7. Yurtaeva K.V. Problems of criminalizing the independent use of computer passwords, access codes or similar data that provide access to computer systems or parts thereof. F. P. 2017. No. 3. P. 221-227.

8. Perun T. S. Administrative responsibility in the system of information security measures. IT law: problems and prospects for development in Ukraine: collection of materials of the 2nd International Scientific and Practical Conference (Lviv, November 17, 2017) Lviv, Lviv Polytechnic National University. 2017. P. 155–160.

9. Honcharuk S. T. Administrative responsibility according to the legislation of Ukraine. Kyiv: KMUTSA, 1995. 78 p.

10. Code of Ukraine on Administrative Offenses: Law of the Ukrainian SSR dated December 7, 1984 No. 2755-VI: Law of Ukraine from https://zakon.rada.gov.ua/laws/show/80731-10

11. Veselova L. Yu. Content of administrative and legal measures to ensure security in the cyber sphere. Legal journal of

Donbass. 2020. No. 1. P. 89–97. URL: http://nbuv.gov.ua/UJRN/pppd_2020_1_13.

12. REPORT ON THE OPERATION OF THE SYSTEM FOR DETECTION OF VULNERABILITIES AND RESPONSE TO CYBER INCIDENTS AND CYBER ATTACKS FOR 2022. URL: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca111/sseb6a10-b7aa-4396-8b04-e0e4b7fca111.pdf

REGARDING THE ISSUE OF ADMINISTRATIVE AND LEGAL LIABILITY FOR OFFENSES IN THE FIELD OF CYBER SECURITY

The article provides a comprehensive analysis of the features of the application of administrative responsibility for offenses in the field of cyber security in Ukraine. It is determined that during the examination of offenses in the field of information circulation provided for by the Code of Ukraine on Administrative Offenses, certain difficulties arise, since the current Code does not have a separate chapter dedicated to the specified offenses, and offenses that could be include in this chapter, located in different chapters of the Special Part of the Code. It was found that administrative responsibility in the field of cyber security can be applied for the commission of three groups of offenses: related to ensuring access of individuals and legal entities to public information necessary for the realization of their rights, freedoms and legitimate interests; related to ensuring the restriction of access to certain information, the dissemination of which may cause a negative impact on the rights and freedoms of citizens, the legal activities of legal entities, or national security; related to ensuring security in the field of media information". It is proposed, in order to unify the articles of the Code of Ukraine on administrative offenses related to the application of administrative responsibility for offenses in the field of cyber security, to allocate a separate section in the code – "Administrative offenses related to ensuring information security".

Keywords: administrative responsibility, information, security, cyberattacks, cyberspace, offenses.