

УДК 342.9

Буканов Г.М.¹, Ковальська А.С.²

¹ д-р наук з держ. упр., проф. НУ «Запорізька політехніка»

² студ. гр. Ю-112 НУ «Запорізька політехніка»

КІБЕРБЕЗПЕКА ЯК ПРІОРИТЕТ ДЕРЖАВНОЇ ПОЛІТИКИ: АДМІНІСТРАТИВНО-ПРАВОВІ АСПЕКТИ РЕГУЛЮВАННЯ

Ефективна система забезпечення інформаційної безпеки в Інтернеті повинна об'єднувати зусилля як держави, так і користувачів. Роль держави полягає у розробці та впровадженні чіткої та комплексної політики, що охоплює всі аспекти суспільного та державного життя. Ця політика має спрямовуватися на підвищення рівня медіаграмотності серед населення та розробку ефективних систем фільтрації та блокування інформації, яка становить загрозу для національної безпеки.

Діяльність державних органів, уповноважених законом на проведення роботи із забезпечення інформаційної безпеки в інтернет просторі, спрямована на моніторинг інтернет простору з метою забезпечення безпеки людини та держави у сфері комп'ютерних технологій. Ці органи та їх посадові особи наділені всіма правами, необхідними для якісного виконання покладених на них обов'язків. Сюди можемо віднести: 1) Міністерство цифрової трансформації України, основним завданням якого є діджиталізація країни, забезпечення безпеки персональних даних кожного користувача інтернету; 2) силові відомства: СБУ, МВС, зокрема підрозділи кіберполіції, їх діяльність спрямована на реалізацію державної політики у сфері протидії кіберзлочинності [1].

Для забезпечення ефективної інформаційної безпеки в сучасному суспільстві існує ряд законодавчих актів, що визначають правову основу та регулюють заходи у цій сфері. Серед них можна виділити такі: ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах», ЗУ «Про державну таємницю», ЗУ «Про захист персональних даних», ЗУ «Про основні засади забезпечення кібербезпеки України», Постанова КМУ «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», Постанова КМУ «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію», тощо.

Під адміністративно-правовими заходами забезпечення безпеки в кібернетичній сфері слід розуміти комплекс правил, прийомів та норм, визначених законодавчими актами, які спрямовані на організацію діяльності спеціально уповноважених державних органів у цій сфері. Ця система має на меті забезпечення кібернетичного порядку, запобігання та припинення правопорушень і притягнення правопорушників до відповідальності.

Першочерговими адміністративно-правовими заходами забезпечення безпеки в кібернетичній сфері повинні стати: подальше посилення державного контролю, проведення виховної, роз'яснювальної роботи серед населення, особливо серед найуразливіших категорій – дітей та літніх людей, 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, ретельний відбір кадрів у спеціальні підрозділи, які протистоять кібернетичним

загрозам та постійний моніторинг професіонального росту кіберфахівців, удосконалення їхніх навичок та знань, подальше вдосконалення законодавчої бази та посилення відповідальності за кібернетичні правопорушення (вивчення та запозичення зарубіжного досвіду) [2].

Міжнародне співробітництво у сфері кібербезпеки спрямоване на досягнення кількох ключових цілей: розробка спільних стратегій протидії загрозам у інформаційному просторі, захист від протиправних дій, тощо

Співробітництво України з іншими державами світу у сфері забезпечення кібербезпеки може здійснюватись шляхом: 1) взаємодії на міжнародному рівні при протидії кіберзагрозам та кібератакам; 2) обміну досвідом побудови та функціонування національних систем кібербезпеки; 3) вироблення стандартів кібербезпеки [3].

Розвиток сучасних технологій та зростання кількості кіберзагроз створюють нові виклики у сфері інформаційної безпеки, які вимагають негайного відгуку та адаптації. Серед них - постійна еволюція методів кібератак, інтенсивний обмін інформацією в мережі та зростання кількості кіберзлочинів. Для ефективного протидії цим викликам, необхідно постійно оновлювати та удосконалювати законодавство в галузі інформаційної безпеки. Адміністративне право повинно розвиватися у напрямку введення більш жорстких заходів контролю за кіберпростором, створення ефективних механізмів виявлення та реагування на кіберзагрози, а також удосконалення процедур щодо захисту персональних даних та інформаційних систем.

Одним із ключових напрямків подальшого розвитку адміністративного права у цій сфері є збільшення співпраці між державними органами, приватним сектором та громадськістю у сфері інформаційної безпеки. Тільки через спільні зусилля можна ефективно впроваджувати інноваційні методи захисту інформації та запобігати кіберзагрозам.

У подальшому розвитку адміністративного права також важливо звернути увагу на впровадження новітніх технологій, таких як штучний інтелект та блокчейн. Ці технології можуть забезпечити додатковий рівень захисту інформації в кіберпросторі та підвищити ефективність боротьби з кіберзагрозами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бліхар М. М. Адміністративно-правове забезпечення інформаційної безпеки в інтернет просторі. Науковий вісник

Ужгородського національного університету. Серія: Право. 2021. Вип. 67. С. 345–349. <https://doi.org/10.24144/2307-3322.2021.67.65>

2. Веселова Л. Ю. Зміст адміністративно-правових заходів забезпечення безпеки в кібернетичній сфері [Електронний ресурс] / Л. Ю. Веселова // Правовий часопис Донбасу. - 2020. - № 1. - С. 89–97. - Режим доступу: http://nbuv.gov.ua/UJRN/pppd_2020_1_13

3. Артеменко Я. В. Адміністративно-правове забезпечення функціонування національної системи кібербезпеки України: автореф. дис. ... канд. юрид. наук: 12.00.07. Київ, 2020. 21 с.