АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

ЗЛЕНКО Анна Володимирівна - старший викладач кафедри конституційного, адміністративного та фінансового права Академії праці, соціальних відносин і туризму

ORCID: 0000-0002-2161-4023

ЛЕБІДЬ Тетяна Ігорівна - старший викладач кафедри конституційного, адміністративного та фінансового права Академії праці, соціальних відносин і туризму

ORCID: 0000-0002-9545-1036

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

ORCID: 0009-0000-4606-6943

УДК 342.7

DOI: https://doi.org/10.32782/LAW.UA.2024.3.5

У статті розглядаються теоретичні та практичні аспекти кібербезпеки, зокрема в контексті воєнного стану в Україні. Авторами проаналізовано основні поняття кібербезпеки, нормативно-правову базу, а також роль адміністративного права задля її забезпеченні. Особливу увагу автори приділяють аналізу впливу воєнного стану на кіберпростір, ключовим загрозам та реакції держави на ці виклики. У статті досліджено адміністративно-правові інструменти, органи та законодавчі ініціативи, які є спрямованими на посилення кібербезпеки під час військового стану. Крім цього, розглянутими є практичні заходи задля зміцнення інфраструктури, кіберполітику та підготовку кадрів. Останній розділ присвячений міжнародній співпраці України у сфері кібербезпеки та спільним зусиллям з міжнародними партнерами під час протидії кіберзагрозам. Ця робота пропонує комплексний підхід до розуміння сучасних викликів у сфері кібербезпеки під час військового стану та вказує на важливість координації зусиль на державному та міжнародному рівнях.

Ключові слова: кібербезпека, воєнний стан, кіберзагрози, адміністративне право, нормативно-правова база, кіберпростір, кіберполітика, інфраструктурні заходи, міжнародна співпраця, Україна.

Постановка проблеми

Кіберзахист у сьогоднішніх умовах має дуже важливе значення, особливо на фоні зростання цифрових загроз і військових конфліктів в Україні під час військового стану. Швидкий ріст інформаційних технологій та залежність державних, а також приватних установ від кіберінфраструктури значно підвищують ризик кібератак. Головна проблема – це забезпечити хороший захист національних інтересів в умовах безперервних кібератак, дезінформаційних кампаній та технічного саботажу, які стали складовою гібридної війни.

Стан дослідження

Відзначається також важливість міжнародного співробітництва та координації зусиль державного і приватного секторів, але детальних досліджень взаємодії між ними все ще бракує. Аналіз кіберзагроз у зв'язку з воєнними конфліктами привертає значну увагу, але потрібні додаткові дослідження ролі адміністративного права в забезпеченні кібербезпеки. Хоча

багато дослідників вивчали ефективність сучасних правових ініціатив, питання адаптації цих інструментів до сучасних викликів не було належним чином вирішено. Це дослідження має на меті заповнити ці прогалини шляхом аналізу адміністративно-правових інструментів, особливо під час війни.

Метою дослідження є аналіз адміністративно-правових механізмів забезпечення кібербезпеки в умовах воєнного стану в Україні та розробка рекомендацій щодо їх удосконалення з метою ефективної протидії сучасним кіберзагрозам.

Завдання дослідження.

1. Проаналізувати чинну нормативно-правову базу з питань кібербезпеки в Україні та її відповідність сучасним викликам.
2. Визначити вплив воєнного стану на розвиток кіберзагроз та стан захисту критичної інфраструктури.
3. Оцінити роль адміністративного права у забезпеченні кібербезпеки та розробці практичних заходів захисту.
4. Дослідити координацію між державними органами та приватним сектором у сфері кібербезпеки.
5. Підготувати рекомендації щодо вдосконалення правових та адміністративних інструментів для посилення кіберзахисту.

Наукова новизна роботи полягає в комплексному аналізі адміністративно-правових засад забезпечення кібербезпеки в Україні в умовах воєнного стану.

Виклад основного матеріалу

В умовах українсько-російської війни, а саме агресії з боку Росії, великою мірою збільшується роль кіберпростору як одного із ключових факторів національної безпеки. Кіберзагрози стають частиною гібридних війн. Країна часто стикається з різноманітними атаками які є спрямованими на критичну інфраструктуру. Ці деталі вимагають посилення адміністративно-правових заходів задля забезпечення кібербезпеки під час воєнного стану.

Кібербезпека — це сукупність заходів і процесів, спрямованих на захист інформаційних систем, мереж і даних від несанкціонованого доступу, кіберзагроз та атак. Вона охоплює як особисту, так і корпоративну інформацію та є ключовою для забезпечення національної безпеки, економіки й інфраструктури. З огляду на зростаючу залежність суспільства від інформаційних технологій, кіберзахист потрібно постійно вдосконалювати. Держава відіграє одну з ключових ролей у формуванні політики кіберзахисту. Вона розробляє нормативні правові акти, що забезпечують координацію між різними органами. Також важливу роль відіграє міжнародне співробітництво, оскільки загрози часто не знають кордонів. Таким чином, кібербезпека є динамічною галуззю, яка адаптується до нових викликів.

Нормативно-правова база кібербезпеки в Україні складається з низки законів, постанов та міжнародних угод. Основний документ, який регулює кібербезпеку, є Закон «Про основи забезпечення кібербезпеки в Україні», який є прийнятим у 2017 році і визначає ключові терміни, принципи та суб'єкти кібербезпеки. Також важливими є Закони України «Про інформацію»[3], що регулює особисті дані та їх захист, а також Закон « Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій « [5].

Діє Національна стратегія, яка окреслює основні завдання та цілі у сфері кіберзахисту. Порядок забезпечення кіберзахисту регулює постанова Кабінету Міністрів України. Задля розвитку нормативно-правової бази Україна співпрацює з такими організаціями, як ЄС та НАТО. Адаптація законодавства до умов воєнного стану є важливою та вимагає гнучких змін задля підвищення рівня кіберзахисту.

Адміністративне право має одну з основних ролей у забезпеченні кібербезпеки. Воно регулює діяльність державних органів та приватного сектору встановлює правила та процедури, які використовуються для захисту інформаційних систем від кіберзагроз. Зокрема, адміністративні норми

визначають обов'язки організації, які потрібні задля захисту даних та регулюють інциденти. Для того, щоб проводити перевірки та розслідування, є такий державний орган, як Кіберполіція. [2]

Окрім цього, адміністративне право передбачає різні санкції за порушення норм кіберзахисту, що передбачають відповідальність за кожен кіберзлочин. Також це право регулює співпрацю між приватними та державними установами під час обміну інформацією. Важливими нормами є ті, які забезпечують права громадян на захист їхніх особистих даних.

Завдячуючи адміністративному праву в Україні, є сформована система контролю за дотриманням вимог кібербезпеки. Хоча дані у цій сфері постійно оновлюються з урахуванням нових викликів.

У зв'язку з введенням воєнного стану в Україні значно збільшилась кількість кіберзагроз, які є спрямовані на елементи державної інфраструктури. Сьогодні кібератаки в більшості націлені на порушення функціонування критичних систем, таких як фінансовий сектор, енергетика, транспорт чи телекомунікації. Основною метою цих атак є дестабілізація управлінських секторів, а також створення хаосу в різних сферах життя. Найбільше від цього страждає оборонна сфера та державні установи, які відповідають за безпеку. У більшості ця кіберзагроза використовується задля крадіжки даних чи створення пропаганди.

Враховуючи те, що кількість кібератак збільшилася, то робота кіберзахисту є дуже ускладненою. Також під ударом опиняються засоби масової інформації, а саме: телебачення та соціальні мережі. Це створює великий ризик для дезінформації населення.

Кіберзлочини є однією зі складових частин гібридної війни, що ведеться проти України. Щоб кількість кібератак зменшилася або вони не набували все більшого впливу, потрібна велика кількість швидких та ефективних контрзаходів. Воєнний стан також спричинив підвищену залежність від цифрових технологій. І зараз це робить країну ще більш вразливою до цього виду загроз. В умовах воєнного стану забезпечення кібербезпеки є одним із пріоритетних завдань задля захисту національної безпеки.

Реакція української держави на кіберзагрозу під час воєнного стану була швидка та багатостороння. Задля моніторингу чи нейтралізації кібератак були використані такі державні органи, як Держспецзв'язок, Кіберполіція та Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони. Щоб підвищити рівень захисту критичної інфраструктури, впровадились нові протоколи безпеки, а також посилилися зв'язки з НАТО та ЄС. Також задля забезпечення швидкого реагування на кіберінциденти було створено Національний координаційний центр кібербезпеки.

Держспецзв'язок відповідає за захист державних інформаційних ресурсів і критичної інфраструктури. Він забезпечує надійність і безпеку телекомунікацій та урядового зв'язку [1].

Основною роботою Кіберполіції є розслідування кіберзлочинів та протидія хакерським атакам чи незаконному використанню інформаційних технологій [2].

Щоб здійснити координацію дій різних державних органів у сфері кіберзахисту, використовується Національний координаційний центр Кібербезпеки. Також він розробляє стратегії та політику кібербезпеки [1].

Окрім цього, СБУ також бере участь у протидії кіберзагрозам, які становлять небезпеку під час воєнного стану. Задля підвищення захисту від кіберзагроз Україна також співпрацює з приватними компаніями і міжнародними організаціями. Міністерство цифрової трансформації України координує впровадження нових різноманітних технологій у кіберзахисті та цифровій інфраструктурі. Таким чином кожен з цих органів забезпечує багатосторонній підхід до кіберзахисту в Україні.

Україна швидко відреагувала на кібератаки, використовуючи Держспецзв'язок, Кіберполіцію та Національний координаційний центр кібербезпеки. Було впроваджено нові протоколи безпеки та посилено співпрацю з НАТО і ЄС.

Задля того, щоб відповідати новим викликам, які є пов'язаними із кібератаками, покращилися норми регулювання кіберзахисту. Одним із ключових факторів стало вдосконалення Закону України «Про основні засади кібербезпеки», який визначає права та обов'язки органів, що займаються захистом інформаційного простору. У 2022 році було внесено зміни до законодавства України, які посилюють санкції за кібератаки і покращують механізми реагування на них.

Також додатково запровадили нові вимоги для підприємств критичної інфраструктури, які дозволяють захистити інформаційні системи та обов'язково почали впроваджувати протоколи безпеки. В умовах воєнного стану особливо важливим стало законодавче регулювання обміну інформацією між державними установами та приватними підприємствами. Це дозволяє краще протидіяти кібератакам. Окрім цього, також активізувалося міжнародне співробітництво, яке закріплюється в нормативно-правових актах, зокрема в угодах з ЄС та НАТО щодо обміну досвідом і технологіями кіберзахисту. Це дозволяє Україні вчасно та якісно реагувати на зростаючі кіберзагрози в інформаційному просторі.

Координації між державними та приватними структурами у сфері кібербезпеки – це один із ключових елементів захисту національної інфраструктури під час військового стану. Державні органи, такі як Держспецзв'язок і Кіберполіція, активно співпрацюють з приватними компаніями, що швидко реагують на кіберзагрози, а також обмінюються з ними важливою інформацією. Одну з найважливіших ролей впровадження новітніх технологій кіберзахисту та моніторингу можливих атак відіграють приватні структури, зокрема it-компанії.

Окрім цього, національний координаційний центр кібербезпеки забезпечує обмін даних між приватними організаціями і державними структурами. Це дозволяє краще реагувати на кіберзагрозу. Задля підвищення готовності до різних кібератак вони проводять регулярне спільне навчання і тренінги. На законодавчому рівні впроваджена обов'язкова участь приватних компаній у кібербезпеці та обміну інформацією з державними структурами. У воєнних умовах є важливим спільне використання ресурсів та технологій для захисту критичної інфраструктури. Така співпраця підвищує ефективність заходів із кіберзахисту та зміцнює їхню оборонну здатність у кіберпросторі.

Інфраструктурні заходи захисту включають впровадження брандмауерів, які контролюють вхідний та вихідний трафік і запобігають несанкціонованому доступу. Також одним із важливих пунктів є використання систем, що допомагають виявити та запобігти вторгненню, а саме IDS чи IPS що дозволяє вчасно реагувати на загрози. Окрім цього, важливо реалізувати шифрування даних, що захищає чутливу інформацію під час її передачі, а також зберігання. Щоб знизити ризик несанкціонованого доступу до облікових записів, бажано використовувати багатофакторну аутентифікацію. Також потрібно створювати резервну копію даних. Це дозволяє відновити інформацію після атаки. Навчання людей основам кібербезпеки дозволяє правильно сформувати обізнаність про потенційні загрози, а також методи їх уникнення.

В умовах війни кіберполітика є однією з невід'ємних частин національної безпеки держави, враховуючи те, що кібератаки є руйнівними для критичної інфраструктури економіки та інформаційної безпеки. Конфлікти у кіберпросторі мають руйнівні наслідки для економіки інфраструктури та інформаційної безпеки. Для того щоб цього не було, уряд повинен координувати дії між різними відомствами, щоб ефективно протидіяти загрозам. Одним із важливих аспектів є розвиток законодавства, що регулює кібербезпеку і відповідальність за кібератаку. Також потрібно інформувати населення щодо кіберзагроз. Це дозволить уникнути великої кількості атак. В умовах воєнного стану кіберполітика повинна бути адаптивною і оперативною. Вона повинна швидко відповідати на загрози і змінювані обставини.

Задля того, щоб покращити кіберзахист, потрібно вчасно та ефективно підготовлювати кадрів. Щоб це було ефективним, по-

трібно охоплювати як технічні аспекти, так і правові етичні та управлінські питання. Також задля кращої підготовки потрібно симулювати кібератаки для того, щоб фахівці були готові до реальних викликів. Щоб краще готувати працівників кіберзахисту, потрібна співпраця між державними органами, приватним сектором та університетами. Також потрібно, щоб спеціалісти щоразу підвищували кваліфікацію у зв'язку з розвитком технологій та еволюцією загроз.

Міжнародна співпраця у сфері кібербезпеки є необхідною. Це дозволяє ефективно протистояти глобальним загрозам. Україна часто долучається до міжнародних ініціатив, а саме: участі в програмах ЄС чи партнерство з НАТО.

Україна бере участь у програмі НАТО «Partnership for Peac» [7]. Це значною мірою покращує підготовку фахівців до кібератак. Також це дозволяє більш обмінюватись досвідом і розвивати цифрову інфраструктуру. Українська держава долучена до глобальних ініціатив з обміну інформацією про кіберзагрози. Одна з них – це Forum of Incident Response and Security Teams (FIRST) [6] Ця програма дозволяє швидше та оперативніше реагувати на кіберзагрози в міжнародному масштабі.

Також співпраця з міжнародними партнерами дозволяє добре обмінюватись технологіями та надає консультації, технічну та експертну підтримку. Створена двостороння угода, у рамках якої Україна отримує сучасне програмне забезпечення, що дозволяє ефективніше захищати критичну інфраструктуру. Також українські фахівці беруть участь у кібернавчаннях НАТО, а саме «Cyber Coalition». Це дозволяє підвищити рівень координації та реагування на кібератаки.

Висновок

У зв'язку з воєнним станом Україна почала більш активно покращувати систему кіберзахисту. Враховуючи те, що кіберпростір став місцем проведення гібридної війни, атаки на інфраструктуру стали значно більшими. Це заважає національній безпеці. Щоб зменшувати кількість кіберзагроз, було створено органи кіберзахисту. Окрім цього, було оновлено законодавство та посилено координації між державними та приватними установами. Також Україна почала ще більше співпрацювати з НАТО та ЄС. Сьогодні вона отримує технічну підтримку та досвід у кіберзахисті. Також почали адаптуватися захисні механізми країни задля загальної безпеки.

Література

1. Державна служба спеціального зв'язку та захисту інформації України. *Access Denied*. URL: https://cip.gov.ua/ua (дата звернення: 24.09.2024).

2. Новини – Департамент Кіберполіції. *Новини – Департамент Кіберполіції*. URL: https://cyberpolice.gov.ua (дата звернення: 24.09.2024).

3. Про внесення змін до статті 14 Закону України «Про інформацію» щодо захисту інформації : Закон України від 30.11.2010 р. № 2724-VI. URL: https://zakon.rada.gov.ua/laws/show/2724-17#Text (дата звернення: 24.09.2024).

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 28 черв. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 24.09.2024).

5. Про рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій» : Указ Президента України від 17.10.2023 р. № 695/2023. URL: https://zakon.rada.gov.ua/laws/show/695/2023#Text (дата звернення: 24.09.2024).

6. FIRST – Improving Security Together. *FIRST – Forum of Incident Response and Security Teams*. URL: https://www.first.org (date of access: 24.09.2024).

7. Partnership for Peace programme. *https://www.nato.int/cps/en/natohq/topics_50349.htm*. URL: https://www.nato.int/cps/en/natohq/topics_50349.htm (date of access: 23.09.2024).

ADMINISTRATIVE AND LEGAL PRINCIPLES OF CYBER SECURITY OF UKRAINE UNDER THE CONDITIONS OF MARITAL STATE

The article explores theoretical and practical aspects of cybersecurity, particularly in the context of martial law in Ukraine. The author analyzes the key concepts of cybersecurity, the regulatory framework, and the role of administrative law in ensuring it. Special attention is given to the analysis of the impact of martial law on cyberspace, major threats, and the state's response to these challenges. The article examines administrative and legal tools, authorities, and legislative initiatives aimed at strengthening cybersecurity during martial law. In addition, practical measures for infrastructure protection, cyber policy, and personnel training are considered. The final section is dedicated to Ukraine's international cooperation in the field of cybersecurity and joint efforts with international partners to counter cyber threats. This work offers a comprehensive approach to understanding modern challenges in the field of cybersecurity during martial law and highlights the importance of coordinating efforts at the national and international levels.

Keywords: cybersecurity, martial law, cyber threats, administrative law, regulatory framework, cyberspace, cyber policy, infrastructure measures, international cooperation, Ukraine.