Вісник Національного університету “Львівська політехніка”. Серія: “Юридичні науки”
№ 2 (42), 2024

УДК 342.95

Юрій ТРЕТЯК
Львівський університет бізнесу та права,
аспірант, адвокат
e-mail: tretyak.yura@gmail.com
ORCID iD: https://orcid.org/0009-0003-9888-6291

СИСТЕМА СУБ’ЄКТІВ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

http://doi.org/10.23939/law2024.42.197

Ця стаття аналізує роль адміністративних органів у забезпеченні кібербезпеки з правової та адміністративної перспективи. Розглядаються основні функції та завдання, які вони виконують для ефективного управління й захисту інформаційних ресурсів та кіберінфраструктури, а також висвітлюється важливість ролі суб’єктів адміністративно-правового забезпечення кібербезпеки у формуванні стратегій та політик, спрямованих на забезпечення кібербезпеки, та визначається їхній внесок у створення безпечного та стабільного кіберпростору.

Розглянуто аспекти, що сприяють кращому розумінню ролі державних структур у забезпеченні безпеки в кіберпросторі та підвищенню їх ефективності в цьому напрямку.

Описано нормативно-правові акти, що регулюють повноваження та функції суб’єктів адміністративно-правового забезпечення кібербезпеки, зокрема Закон України “Про основи забезпечення кібербезпеки України”, а також вплив адміністративно-правового забезпечення кібербезпеки на ефективність захисту інформаційних ресурсів та кіберінфраструктури.

Охарактеризовано, що система суб’єктів адміністративно-правового забезпечення кібербезпеки – це органічне поєднання спільною метою державних і недержавних інституцій, а також інших суб’єктів, які беруть участь у здійсненні заходів, спрямованих на забезпечення кібербезпеки.

Запропоновано координацію дій між різними суб’єктами, детальне та чітке розмежування компетенції державних органів, які є суб’єктами забезпечення кібербезпеки; встановлення обов’язкової системи сертифікації для оцінки та підтвердження рівня кібербезпеки для усіх суб’єктів, які мають критичне значення для інфраструктури або національної безпеки; співпрацю з приватним сектором та громадськістю; розроблення планів реагування на кіберінциденти та програм відновлення після їх виникнення для мінімізації збитків та перерв у роботі суб`єктів адміністративно-правового забезпечення кібербезпеки.

Ключові слова: адміністративний орган; суб’єкт забезпечення кібербезпеки; кібербезпека; кіберінфраструктура; кіберзахист.

Постановка проблеми. В умовах всеосяжного цифрового розвитку та зростання кіберзагроз стала актуальною проблема забезпечення кібербезпеки на національному та міжнародному рівнях.

Україна, як і багато інших країн, стикається з постійними викликами у забезпеченні безпеки в кіберпросторі. У цьому контексті роль суб'єктів адміністративно-правового забезчення кібербезпеки стає критично важливою. Адміністративно-правове забезпечення кібербезпеки в Україні має значний вплив на ефективність захисту інформаційних ресурсів і кіберінфраструктури. На сьогодні питання кібербезпеки, властиво, стає невід'ємною частиною національної безпеки, а заходи протидії кіберзагрозам розробляються і впроваджуються на державному рівні. Станом на зараз, особливо в умовах війни, питання кіберзагроз є актуальним практично для всіх суб'єктів, як для звичайних громадян, так і для великих підприємств, а також окремих галузей економіки та держави загалом, у зв'язку з чим ефективна організація системи органів адміністративно-правового забезпечення кібербезпеки набуває критичного значення.

Аналіз дослідження проблеми. Серед науковців, що досліджували систему суб'єктів забезпечення кібербезпеки в Україні та їх роль в адміністративному-правовму забезпеченні кібербезпеки варто виділити праці А. В. Тарасюка, Т. Ю. Ткачука, В. Л. Бурячка, С. О. Гнатюка, О. Г. Корченко.

Метою статті є аналіз функцій законодавчо визначеної системи суб'єктів адміністративно-правового забезпечення кібербезпеки в Україні, визначення ролі адміністративних органів в адміністративно-правовому забезпеченні кібербезпеки в контексті сучасних викликів та загроз в кіберпросторі, дослідження їхньої функціональної сфери, завдань та відповідальності у забезпеченні ефективного управління і захисту інформаційних ресурсів та кіберінфраструктури, аналіз стратегій та політик, які вони впроваджують для протидії кіберзагрозам та забезпечення безпеки в кіберпросторі.

Виклад основного матеріалу. Закон України "Про основні засади забезпечення кібербезпеки України" визначає перелік основних суб'єктів національної системи адміністративно-правового забезпечення кібербезпеки, а саме: Президент України через Раду національної безпеки і оборони України, яка ним очолюється, Кабінет Міністрів України, міністерства та інші центральні органи виконавчої влади, Національний координаційний центр кібербезпеки, місцеві державні адміністрації, органи місцевого самоврядування, правоохоронні, органи розвідки та контррозвідки, Збройні сили України та інші військові формування, що утворені та діють згідноз законом, Національний банк України, суб'єкти оперативно-розшукової діяльності, підприємства, установи, організації, що належать до об'єктів критичної інфраструктури, а також інші суб'єкти, які провадять діяльність, що пов'язана з національними інформаційними ресурсами, інформаційними електронними послугами, а також із здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [1].

Суб'єкти забезпечення кібербезпеки у межах компетенції вчиняють дії, що спрямовані на запобігання використання кіберпростору у воєнних, терористичних чи будь-яких інших незаконних і злочинних цілях; виявляють та реагують на кіберінциденти та кібератаки, ліквідують їх наслідки; здійснюють обмін інформацією щодо виявлених та потенційних кіберзагроз; розробляють і впроваджують заходи у сфері кібербезпеки, кібероборони та кіберзахисту, включно із запобіжними, організаційними, навчальними та іншими заходами; забезпечують проведення аудиту інформаційної безпеки, включаючи підпорядковані об'єкти та об'єкти, що перебувають в їх управлінні; виконують низку інших заходів, спрямованих на забезпечення розвитку та безпеки кіберпростору.

Згідно з вищезгаданим Законом, Кабінет Міністрів України відповідає за розробку і впровадження державної політики в галузі кібербезпеки, захист прав і свобод громадян, а також національних інтересів нашої держави в кіберпросторі та боротьбу з кіберзлочинністю. Крім того, на нього покладено завдання з організації і забезпечення необхідними ресурсами функціонування національної системи кібербезпеки, встановлення вимог до системи аудиту інформаційної безпеки

на об'єктах критичної інфраструктури і забезпечення його роботи, за винятком тих об'єктів, що входять до сфери регулювання Національного банку, операторів платіжних систем, а також технологічних операторів платіжних послуг.

Своєю чергою цим же нормативно-правовим актом на Президента України покладено завдання контролю за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони, інших державних органів [1].

Також треба зауважити, що Постанова Кабінету Міністрів України від 4 квітня 2023 р. № 299 "Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі" затвердила Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі.

Згідно з цим порядком, суб'єкти забезпечення кібербезпеки здійснюють реагування на кіберінциденти та кібератаки через заходи з кіберзахисту. Ці заходи спрямовані на оперативне виявлення кіберінцидентів та кібератак і захист від них, належне інформування про кіберзагрози, запобігання негативним наслідкам від них, їх мінімізацію та усунення, а також виправлення вразливостей. Крім того, документ передбачає послідовне виконання етапів реагування на кіберінциденти та кібератаки, зокрема, підготовку, виявлення та їх аналіз, запобігання, ліквідацію, відновлення, а також оцінку ефективності та надійності заходів реагування на кіберзагрози [2].

Важливим нормативним актом, що регулює питання завдань, покладених на суб'єктів забезпечення кібербезпеки, є Стратегія кібербезпеки України. Згідно з положеннями цієї стратегії її реалізація покладається на основних суб'єктів національної системи кібербезпеки, Міністерство закордонних справ України, Міністерство цифрової трансформації України, Міністерство освіти і науки України, а також інших суб'єктів забезпечення кібербезпеки в межах їх компетенції [3].

Міністерство оборони України та Генеральний штаб Збройних сил України відповідно до своїх повноважень відповідають за проведення заходів щодо підготовки країни до відстоювання військової агресії у кіберпросторі (кібероборони). Вони також координують військову співпрацю з НАТО, спрямовану на забезпечення безпеки кіберпростору та спільний захист від кіберзагроз. Крім того, їм доручено забезпечення співпраці з Державною службою спеціального зв'язку та захисту інформації України та Службою безпеки України щодо кіберзахисту власної інформаційної інфраструктури.

Національний координаційний центр кібербезпеки, який діє як робочий орган Ради національної безпеки й оборони України, відповідає за координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку. Цей центр також представляє Президентові України пропозиції, які безпосередньо стосуються формування та уточнення Стратегії кібербезпеки України.

Згідно із вже згаданою вище Стратегією Національний координаційний центр кібербезпеки відповідає за розроблення та затвердження процедур та порядку здійснення огляду державної системи кібербезпеки. Він також здійснює обов'язкове та негайне повідомлення про кіберзагрози, кібератаки та кіберінциденти до всіх відомчих і галузевих центрів кібербезпеки, забезпечує розгляд основних питань кібербезпеки на своїх засіданнях та системний контроль за виконанням ухвалених рішень. Крім того, він координує виявлення та виправлення вразливостей інформаційно-комунікаційних систем, сприяє заохоченню приватного сектору, наукової спільноти, громадських організацій і громадян до участі у заходах з кібербезпеки та щорічно оприлюднює публічні звіти про стан кібербезпеки за різними сферами відповідальності [3].

Ширше коло завдань Національного координаційного центру кібербезпеки визначає Указ Президента України "Про Національний координаційний центр кібербезпеки", яким затверджено Положення про вказаний центр. Серед основних завдань згідно з цим Указом – аналіз стану кібербезпеки, огляду національної системи кібербезпеки, оцінка готовності суб'єктів кібербезпеки до протидії кіберзагрозам та виконання вимог законодавства щодо кіберзахисту державних електронних ресурсів [4].

Під час засідання Національного координаційного центру кібербезпеки 22 вересня 2022 року одноголосно було затверджено Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки (далі – Порядок взаємодії або Порядок) [5].

Документ був розроблений робочою групою, створеною при вищезгаданому координаційному центрі, яка включала представників всіх основних суб'єктів національної системи кібербезпеки, а також Мінцифри, МЗС та Національного інституту стратегічних досліджень.

У межах цього документа передбачено створення постійної Об'єднаної групи для реагування на кіберінциденти та кібератаки, а також врегульовано питання обміну інформацією, координації та спільних дій між суб'єктами забезпечення кібербезпеки під час реагування на кіберінциденти та кібератаки.

Вищезгаданий Порядок взаємодії визначає основні принципи, на яких ґрунтується його застосування. Один з головних – спільна мета, адже приватний сектор і державні органи мають спільно забезпечувати безпеку власних інформаційно-комунікаційних систем та кібербезпеку держави загалом. Крім того, передбачається, що взаємодію треба здійснювати на засадах реагування з урахуванням можливих ризиків; поваги до усіх підприємств, установ та організацій, на яких стався кіберінцидент; єдності зусиль; пріоритетності та першочерговості заходів відновлення діяльності.

Залежно від ступеня негативних наслідків, що настають внаслідок реалізації кіберінциденту / кібератаки, впроваджено відповідно шість рівнів критичності, які розроблялись, ґрунтуючись на найкращих світових практиках: некритичний (білий), низький (зелений), середній (жовтий), високий (помаранчевий), критичний (червоний), а також надзвичайний (чорний). Відповідно до встановленого рівня критичності Порядком визначаються конкретні алгоритми взаємодії під час реагування на загрози [5].

Служба безпеки України (СБУ) в контексті забезпечення кібербезпеки також відіграє основну роль у захисті національних інтересів та інфраструктури країни в кіберпросторі. Це орган, який має широкі повноваження щодо збору й аналізу інформації про можливі кіберзагрози, а також проведення операцій з контролю та протидії цим загрозам.

Основні функції СБУ у сфері кібербезпеки, на нашу думку, містять:

- моніторинг інтернет-простору: СБУ веде постійний моніторинг інтернету для виявлення можливих загроз національній безпеці, таких як кібератаки, шпигунство, дестабілізаційні дії тощо;
- реагування на кіберзагрози: СБУ має можливість реагувати на кібернапади та інші загрози шляхом координації з іншими правоохоронними органами та кіберзахисними структурами;
- розслідування кіберзлочинів: СБУ веде розслідування кіберзлочинів, таких як кібертероризм, кібершпигунство, кібершахрайство та інші, з метою ідентифікації та притягнення винних до відповідальності;
- співпраця з міжнародними партнерами: СБУ співпрацює з іншими країнами та міжнародними організаціями у сфері кібербезпеки для обміну інформацією та спільної протидії загрозам;
- здійснення контррозвідувальних, а також оперативно-розшукових заходів, що своєю чергою спрямовані на боротьбу з кібертероризмом та кібершпигунством;
- забезпечення готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів;
- забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки [6].

На Національний банк України своєю чергою покладено завдання формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері. Оскільки банківська система є однією з найважливіших інфраструктурних галузей, яка підтримує економіку та фінансову стабільність, захист її від кіберзагроз є надзвичайно важливим завданням.

Можна виділити такі основні способи, якими Національний банк України забезпечує кібербезпеку в банківській системі:

- розробка та впровадження кіберзахисних стандартів: НБУ встановлює вимоги до кіберзахисту для банківських установ, включаючи вимоги до захисту даних клієнтів, інформаційних систем та мереж;
- моніторинг та аналіз кіберзагроз: НБУ веде постійний моніторинг кіберзагроз та аналіз потенційних ризиків для банківської системи, щоб вчасно виявляти та реагувати на них;
- співпраця з іншими суб'єктами кібербезпеки: НБУ взаємодіє з іншими урядовими та приватними суб'єктами кібербезпеки, зокрема правоохоронними органами, для обміну інформацією та спільної протидії загрозам [7].

Ще одним не менш важливим органом у сфері кібербезпеки, на нашу думку, є Державна служба спеціального зв'язку та захисту інформації України (ДСС України), діяльність якої регулює Закон України "Про Державну службу спеціального зв'язку та захисту інформації України".

Вищезгаданий Закон визначає роль ДСС України як органу, відповідального за розвиток і ефективне функціонування систем урядового зв'язку, захист конфіденційного обміну інформацією, телекомунікацій, криптографічну безпеку та управління радіочастотним ресурсом. ДСС України також відповідає за кібербезпеку, у тому числі за захист державних інформаційних ресурсів у мережі, критичної інфраструктури та реагування на кіберінциденти.

У сфері кібербезпеки ДСС України відповідає за розробку та впровадження політики щодо захисту державних інформаційних ресурсів та інформації, яка підпадає під вимоги закону. Вона також забезпечує кіберзахист об'єктів критичної інформаційної інфраструктури та здійснює державний контроль у цих сферах. Крім того, ДСС України координує діяльність інших учасників у сфері кібербезпеки, сприяючи їхній взаємодії щодо захисту. Вона також забезпечує створення та нормальне функціонування Національної телекомунікаційної мережі та впроваджує організаційно-технічні моделі для забезпечення кіберзахисту [8].

Від початку війни Державною служба спеціального зв'язку та захисту інформації виявила та дослідила близько 24 млрд подій у сфері інформації. Треба зауважити, що за останній період часу істотно збільшився об'єм зареєстрованих та опрацьованих кіберінцидентів від 65 до 120, порівняно з попередніми періодами та даними [9].

Розвідувальними органами, такими як Служба зовнішньої розвідки України, розвідувальними органами спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону, своєю чергою здійснюється розвідувальна діяльність щодо можливих загроз національній безпеці України у кіберпросторі, а також інших подій і обставин, що пов'язані зі сферою кібербезпеки та кіберпростору.

Постановою Кабінету Міністрів України від 13 жовтня 2015 р. № 831 "Про утворення територіального органу Національної поліції" було утворено Департамент кіберполіції як міжрегіональний територіальний орган Національної поліції [10].

Кіберполіція своєю чергою відповідає за розслідування кіберзлочинів, зокрема крадіжки особистих даних, шахрайство в інтернеті, кібертероризм та інші кіберзлочини. Вона також проводить превентивні заходи, спрямовані на попередження кіберзлочинності та підвищення кібербезпеки серед населення та підприємств; здійснює заходи протидії кіберзлочинам у сфері використання платіжних систем, таким як скімінг (шимінг), кардінг, кеш-трапінг; здійснює попереднє та завчасне інформування громадян щодо появи нових кіберзлочинців; впроваджує програмні засоби для систематизації кіберінцидентів; здійснює реагування на запити іноземних партнерів.

Окрім вже сказаного, Департамент кіберполіції також має забезпечувати участь у підвищенні кваліфікації працівників поліції у сфері застосування комп'ютерних технологій з метою протидії злочинності [11].

Під час дії воєнного стану більша частина державних органів активно долучилася до заходів протидії повномасштабному вторгненню російських військ на територію України. Хоча основні

завдання кіберполіції залишилися незмінними, внаслідок цього воєнного конфлікту деякі напрямки роботи стали більш активними, а також з'явилися нові, а саме:

- Активна протидія проросійським хакерським групам, які мають за мету атакувати інформаційні ресурси державних органів України.

- Запобігання масштабним ДДОС-атакам на приватний і державний сектори.

- Виявлення та реагування на антиукраїнську пропаганду в інтернеті, яка координується російськими ЗМІ та за допомогою ботів у соціальних мережах.

Ураховуючи різноманітність суб'єктів у сфері адміністративно-правового забезпечення кібербезпеки, можна підтримати думку А. В. Тарасюка, що подальше зростання їх кількості може призвести до дублювання їх повноважень, що своєю чергою ускладнює потребу вдосконалення системи регулювання цих суб'єктів. Також погоджуємось з позицією щодо важливості розвитку державно-приватного партнерства в галузі кібербезпеки з метою ефективного забезпечення потреби у цій сфері [12].

Т. Ю. Ткачук слушно зауважує, що суб'єкти, які забезпечують кібербезпеку, мають охоплювати не лише державні органи та їхніх представників. Коли йдеться про систему національної безпеки загалом, до її складу традиційно долучають різні сили та ресурси, що спроможні забезпечити національну безпеку [13, с. 42].

Також погоджуємось з думкою, що досвід іноземних держав та особливості сучасних українських реалій свідчать про те, що основні завдання кібербезпеки неможливо розв'язати без створення спеціального міжвідомчого структурного органу, який би був спроможний на постійній основі забезпечити координацію діяльності окремих відомств; правоохоронних і силових структур України, що відповідальні за забезпечення кібербезпеки; центральних органів у структурі певних відомств, правоохоронних і силових структур України, на яких покладено функції виявлення й оцінювання ступеня критичності зовнішнього кібервпливу, розробка основних принципів і надання відповідних рекомендацій, що стосуються боротьби з його проявами, а також належної протидії кібератакам конфронтуючих сторін і впливу на їх інформаційно-телекомунікаційні системи; органів власної інформаційної безпеки – державних установ (відомств) і комерційних структур, метою яких має бути тісна взаємодія із вищезгаданими центральними органами щодо побудови єдиної політики стосовно захисту власного та спільного національного інформаційного та кіберпросторів [14, с. 8–9].

З огляду назагрози кібербезпеці, які постійно зростають, вдосконалення системи суб'єктів адміністративно-правового забезпечення кібербезпеки стає критичним завданням. Ми вбачаємо такі шляхи реалізації цього завдання: розширення нормативно-правової бази, що регулює кібербезпеку на всіх рівнях – від державного до корпоративного; детальне та чітке розмежування компетенції державних органів, які є суб'єктами забезпечення кібербезпеки; встановлення обов'язкової системи сертифікації для оцінки та підтвердження рівня кібербезпеки для усіх суб'єктів, які мають критичне значення для інфраструктури або національної безпеки; впровадження обов'язкових регулярних аудитів для оцінки вразливостей та ефективності заходів з кібербезпеки, що здійснюються суб'єктами забезпечення кібербезпеки на державному рівні; розроблення планів реагування на кіберінциденти та програм відновлення після їх виникнення для мінімізації збитків та перерв у роботі суб'єктів адміністративно-правового забезпечення кібербезпеки. Крім того, сьогодні в умовах війни особливо важливим є посилення міжнародного співробітництва в галузі кібербезпеки для обміну інформацією та спільного реагування на кіберзагрози.

Висновки. Основними суб'єктами адміністративно-правового забезпечення кібербезпеки **є** Президент України через Раду національної безпеки і оборони України, яку він очолює, Національний координаційний центр кібербезпеки в статусі робочого органу Ради національної безпеки і оборони України, Кабінет Міністрів України, міністерства та інші центральні органи виконавчої влади, органи місцевого самоврядування, правоохоронні органи та органи розвідки,

суб'єкти оперативно-розшукової діяльності, Збройні сили України та інші військові формування, що утворені та діють відповідно до закону, Національний банк України, об'єкти критичної інфраструктури. Кожен з цих суб'єктів у межах своєї компетенції здійснює необхідні заходи з метою запобігання та протидії використанню кібернетичного простору у воєнних, розвідувально-підривних, терористичних та інших злочинних цілях, виявлення кіберінцидентів та кібератак і реагування на них, та вчиняє дії спрямовані на усунення спричинених ними негативних наслідків.

В умовах війни питання кіберзагроз є актуальним майже для всіх суб'єктів, як для звичайних громадян, так і для великих підприємств, а також окремих галузей економіки та держави загалом, у зв'язку з чим під час дії воєнного стану більша частина державних органів активно долучилася до заходів протидії кіберзагрозам, пов'язаним з повномасштабним вторгненням російських військ на територію України.

Для вдосконалення системи суб'єктів адміністративно-правового забезпечення кібербезпеки вбачаються такі заходи, як розширення нормативно-правової бази, що регулює кібербезпеку на всіх рівнях – від державного до корпоративного; детальне та чітке розмежування компетенції державних органів, які є суб'єктами забезпечення кібербезпеки; встановлення обов'язкової системи сертифікації для оцінки та підтвердження рівня кібербезпеки для усіх суб'єктів, які мають критичне значення для інфраструктури або національної безпеки; впровадження обов'язкових регулярних аудитів для оцінки вразливостей та ефективності заходів з кібербезпеки, що здійснюються суб'єктами забезпечення кібербезпеки на державному рівні; розроблення планів реагування на кіберінциденти та програм відновлення після їх виникнення для мінімізації збитків та перерв у роботі; посилення міжнародного співробітництва в галузі кібербезпеки з метою обміну інформацією та спільного реагування на наявні загрози кібербезпеці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від 04.04.2023 № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України; Стратегія від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

4. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text

5. Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти / кібератаки. URL: https://www.rnbo.gov.ua/ua/Diialnist/5765.html

6. Про службу безпеки України: Закон України від 25.03.1992 № 2229-XII.. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

7. Про національний Банк України: Закон України від 20.05.1999 № 679-XIV. URL: https://zakon.rada.gov.ua/laws/show/679-14#Text

8. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

9. Державна Служба спеціального зв'язку та захисту інформації. Офіційна веб-сторінка. URL: https://cip.gov.ua/ua

10. Про утворення територіального органу Національної поліції: *Постанова Кабінету Міністрів України* від 13.10.2015 № 831. URL: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text

11. Кіберполіція України. Офіційна веб-сторінка. URL: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text

12. Тарасюк А. В. Суб`єкти забезпечення кібербезпеки в Україні. Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки. 2020. С. 119–124. URL: https://doi.org/10.32838/2707-0581/2020.2-2/23

13. Ткачук Т. Ю. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. Jurnalul juridic national: teorie şi practică. 2017. № 6. С. 42–46.

14. Бурячок В. Л., Гнатюк С. О., Корченко О. Г. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки. Інформаційна безпека: виклики і загрози сучасності: зб. матеріалів наук.-практ. конф., 5 квітня 2013 р., м. Київ. Київ : Наук.-вид. центр НА СБ України, 2013. 416 с.

REFERENCES

1. ***Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy***: Zakon Ukrainy vid 05.10.2017 № 2163-VIII [On the Basic Principles of Cybersecurity in Ukraine: The Law of Ukraine dated October 5, 2017 No. 2163-VIII]. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text [In Ukrainian].

2. ***Deiaki pytannia reahuvannia subiektamy zabezpechennia kiberbezpeky na rizni vydy podii u kiberprostori***: Postanova Kabinetu Ministriv Ukrainy vid 04.04.2023 No. 299 [Some issues of response by cyber security entities to various types of events in cyberspace: Resolution of the Cabinet of Ministers of Ukraine dated April 4, 2023 No. 299]. Retrieved from: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text [In Ukrainian].

3. ***Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy***": Ukaz Prezydenta Ukrainy; Stratehiia vid 26.08.2021 No. 447/2021 [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine; Strategy dated August 26, 2021 No. 447/2021]. Retrieved from: https://zakon.rada.gov.ua/laws/show/447/2021#Text [In Ukrainian].

4**.** ***Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky***: Ukaz Prezydenta Ukrainy vid 07.06.2016 No. 242/2016 [About the National Coordination Center for Cyber Security: Decree of the President of Ukraine dated June 6, 2016 No. 242/2016]. Retrieved from: https://zakon.rada.gov.ua/laws/show/242/2016#Text [In Ukrainian].

5. ***Poriadok vzaiemodii subiektiv zabezpechennia kiberbezpeky pid chas reahuvannia na kiberintsydenty/ kiberataky*** [Procedure for interaction of cyber security entities during response to cyber incidents/cyber attacks]. Retrieved from: https://www.rnbo.gov.ua/ua/Diialnist/5765.html [In Ukrainian].

6. ***Pro sluzhbu bezpeky Ukrainy:*** Zakon Ukrainy vid 25.03.1992 No. 2229-XII [On Security Service of Ukraine: The Law of Ukraine dated March 25, 1992 No. 222-XII]. Retrieved from: https://zakon.rada.gov.ua/laws/show/2229-12#Text [In Ukrainian].

7. ***Pro natsionalnyi Bank Ukrainy***: Zakon Ukrainy vid 20.05.1999 No. 679-XIV [On the National Bank of Ukraine: The Law of Ukraine dated May 20, 1999 No. 679-XIV]. Retrieved from: https://zakon.rada.gov.ua/laws/show/679-14#Text [In Ukrainian].

8. ***Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy***: Zakon Ukrainy vid 23.02.2006 No. 3475-IV [On the State Service for Special Communications and Information Protection of Ukraine: The Law of Ukraine dated February 23, 2006 No. 3475-IV. Retrieved from: https://zakon.rada.gov.ua/laws/show/3475-15#Text [In Ukrainian].

9. ***State Service for Special Communications and Information Protection. Official web page***. Retrieved from: https://cip.gov.ua/ua [In Ukrainian].

10. ***Pro utvorennia terytorialnoho orhanu Natsionalnoi politsii***: Postanova Kabinetu Ministriv Ukrainy vid 13.10.2015 No. 831. [On the formation of a territorial body of the National Police: Decree of the Cabinet of Ministers of Ukraine dated October 13, 2015 No. 831]. Retrieved from: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text [In Ukrainian].

11. **Cyber police of Ukraine**. **Official web page**. Retrieved from: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text [In Ukrainian].

12. Tarasiuk, A. V. **Sub'iekty zabezpechennia kiberbezpeky v Ukraini** [Subjects of cyber security in Ukraine]. Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: yurydychni nauky (Academic notes of TNU named after V. I. Vernadsky. Series: legal sciences*)*. 2020. 119–124. Retrieved from: https://doi.org/10.32838/2707-0581/2020.2-2/23 [In Ukrainian].

13. Tkachuk, T. Y. **Sub'iekty zabezpechennia informatsiinoi bezpeky derzhavy**: **funktsionalnyi analiz** [Subjects of state information security: functional analysis]. Jurnalul juridic national: teorie şi practică. 2017. No. 6. 42–46 [In Ukrainian].

14. Buriachok, V. L., Hnatiuk, S. O., Korchenko, O. H. **Kharakterni oznaky ta problemni aspekty zabezpechennia kibernetychnoi bezpeky** [Characteristic features and problematic aspects of cyber security]. Informatsiina bezpeka: vyklyky i zahrozy suchasnosti: zb. materialiv nauk.-prakt. konf., 2013. 416 [In Ukrainian].

Дата надходження 17.04.2024 р.

Yurii Tretiak
Lviv University of Business and Law,
postgraduate student, lawyer
tretyak.yura@gmail.com
ORCID ID: https://orcid.org/0009-0003-9888-6291

SYSTEM OF SUBJECTS OF ADMINISTRATIVE AND LEGAL SUPPORT OF CYBERSECURITY

This article analyzes the role of administrative bodies in ensuring cyber security from a legal and administrative perspective. The key functions and tasks they perform for effective management and protection of information resources and cyber infrastructure are considered, as well as the importance of the role of subjects of administrative and legal protection of cyber security in the formation of strategies and policies aimed at ensuring cyber security is highlighted, and their contribution to the creation of a secure and stable cyberspace.

Aspects that contribute to a better understanding of the role of state structures in ensuring security in cyberspace and increasing their effectiveness in this direction are considered.

The normative legal acts regulating the powers and functions of subjects of administrative and legal protection of cyber security are described, in particular the Law of Ukraine "On the Basics of Cyber Security of Ukraine", as well as the impact of the administrative and legal protection of cyber security on the effectiveness of the protection of information resources and cyber infrastructure.

It is characterized that the system of subjects of administrative and legal support for cyber security is an organic combination with a common goal of state and non-state institutions, as well as other subjects that participate in the implementation of measures aimed at ensuring cyber security.

Proposed: development and implementation of relevant legislation; coordination of actions between various subjects, detailed and clear demarcation of the competence of state bodies that are subjects of cyber security; establishment of a mandatory certification system to assess and confirm the level of cyber security for all entities that are critical to infrastructure or national security; cooperation with the private sector and the public; developing cyber incident response plans and recovery programs after they occur to minimize damage and business interruptions.

Key words: administrative body; subject of cyber security; cyber security; cyber infrastructure; cyber protection.