УДК 341.2
DOI https://doi.org/10.32689/2617-9660-2025-2(34)-33-37

Лісовська Юлія Петрівна,
кандидат юридичних наук, заступник завідувача кафедри адміністративного, фінансового та банківського права ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Фрометівська, 2, м. Київ, 03039; ivsd@i.ua; https://orcid.org/0000-0001-9278-4487

Лісовський Петро Миколайович,
доктор філософських наук, доцент, професор кафедри конституційного і адміністративного права юридичного факультету Інституту управління, технологій та права Державного університету інфраструктури та технологій, вул. Кирилівська, 9, м. Київ, 04071; syngaipm@i.ua; https://orcid.org/0000-0002-0022-5483

Бортник Валентин Анатолійович,
кандидат юридичних наук, доцент, завідувач кафедри адміністративного, фінансового та банківського права ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Фрометівська, 2, м. Київ, 03039; Valentinbortnik1954@gmail.com; https://orcid.org/0000-0002-1226-6215

ІННОВАЦІЙНО-ІНТЕЛЕКТУАЛЬНИЙ ПОТЕНЦІАЛ ЯК СТРАТЕГІЧНА СКЛАДОВА ОБОРОНОЗДАТНОЇ ІНФРАСТРУКТУРИ КІБЕРСПЕЦСЛУЖБ СВІТУ

Анотація. *Зростання кіберзлочинності, використання засобів кібертероризму у гібридних війнах та необхідність розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці є надзвичайно актуальними в контексті розвитку інформаційного суспільства.*

Військова кібербезпека, також відома як військова кібербезпека або військовий кіберзахист, була розгорнута для захисту цифрових активів, комунікаційних мереж та IT-інфраструктури військових організацій і оборонних відомств. Основною метою цих процесів є захист життєво важливих військових даних для забезпечення безперервного виконання військових дій. Це включає захист військових мереж від зловмисних загроз і атак, а також забезпечення конфіденційності, точності та доступності критично важливих військових даних. Ці системи також включають процедури для створення та використання тактик виявлення, реагування та пом'якшення кіберінцидентів. Ці загрози включають спонсоровані державою кібератаки, хактивізм та операції, які проводять кіберзлочинці. У результаті цифрової трансформації, яка розширила потенційну поверхню атак, військові організації змушені інвестувати в рішення кібербезпеки, які відповідають суворим критеріям кібербезпеки, встановлених урядами та оборонними відомствами.

У нинішньому кліматі триваючої геополітичної напруженості та конфліктів кібербезпека набула першочергового значення для багатьох країн. Таким чином, ці обставини посилили увагу до кіберспроможностей, як оборонних, так і наступальних. Інвестиції в заходи кібербезпеки тепер захищають пов'язані з обороною технології та програмне забезпечення. Зараз головним пріоритетом є захист життєво важливих військових інфраструктур від кібератак. Зараз військові організації координують заходи кіберзахисту та обмінюються інформацією про загрози з комерційним сектором і своїми міжнародними партнерами.

Ключові слова: *кіберспецслужби світу, міжнародно-правовий рейтинг, обороноздатність, інфраструктура України, кібератаки, кібербезпека, антикорупційна політика, кіберзлочинність, повоєнна Україна.*

Lisovska Yuliia Petrivna,
PhD in Law, Deputy Head of the Department of Administrative, Financial and Banking Law, Interregional Academy of Personnel Management, 2, Frometivska Str., Kyiv, 03039; ivsd@i.ua; https://orcid.org/0000-0001-9278-4487

Lisovskyi Petro Mykolayovych,
Doctor of Philosophy, Associate Professor, Professor at the Department of Constitutional and Administrative Law, Faculty of Law, Institute of Management, Technologies and Law, State University of Infrastructure and Technologies, 9, Kyrylivska Str., Kyiv, 04071; syngaipm@i.ua; https://orcid.org/0000-0002-0022-5483

Bortnyk Valentin Anatoliyovych,
PhD in Law, Associate Professor, Head of the Department of Administrative, Financial and Banking Law, Interregional Academy of Personnel Management, 2, Frometivska Str. Kyiv, 03039; Valentinbortnik1954@gmail.com; https://orcid.org/0000-0002-1226-6215

INNOVATIVE AND INTELLECTUAL POTENTIAL AS A STRATEGIC COMPONENT OF THE DEFENSIVE INFRASTRUCTURE OF THE WORLD'S CYBER SPECIAL SERVICES

Abstract. *The growth of cybercrime, the use of cyberterrorism tools in hybrid wars, and the need to develop a system for ensuring Ukraine's cyber security in accordance with the defined strategic directions, taking into account the trends in the development of cyberspace, modern challenges and threats to its security, are extremely relevant in the context of the development of the information society.*

Military cybersecurity, also known as military cybersecurity or military cyber defense, was deployed to protect digital assets, communication networks, and IT infrastructure of military organizations and defense departments. The main goal of these processes is to protect vital military data to ensure the continuous execution of military operations. This includes protecting military networks from malicious threats and attacks, as well as ensuring the confidentiality, accuracy, and availability of critical military data. These systems also include procedures for creating and using tactics for detecting, responding to, and mitigating cyber incidents. These threats include state-sponsored cyberattacks, hacktivism, and operations conducted by cybercriminals. As a result of digital transformation, which has expanded the potential attack surface, military organizations are forced to invest in cybersecurity solutions that meet the stringent cybersecurity criteria set by governments and defense agencies.

In the current climate of ongoing geopolitical tensions and conflicts, cybersecurity has become a top priority for many countries. As such, these circumstances have increased the focus on cyber capabilities, both defensive and offensive. Investments in cybersecurity measures now protect defense-related technologies and software. The top priority is now to protect critical military infrastructure from cyberattacks. Military organizations are now coordinating cyber defense measures and sharing threat intelligence with the commercial sector and their international partners.

Key words: *cyber special services of the world, international legal rating, defense capability, infrastructure of Ukraine, cyberattacks, cybersecurity, anti-corruption policy, cybercrime, post-war Ukraine.*

Постановка проблеми. У кіберсучасній повоєнній Україні варто озвучити інтелектуальні знання із поколінь в покоління, що системно висвітлюють ритмодинаміку російсько-української війни. За особливих обставин необхідно висвітлити і фахові показники всім відомого із інформаційних джерел Інтернету – Британського Інституту вивчення війни. Така установа рейтингового значення, аналітичний центр якого спеціалізується на проблемах міжнародної безпеки та військової справи, в кіберсучасності є об'єднаною королівською інституцією з проблем оборони та безпеки, що заснована 1831 року за ініціативи фельдмаршала Артура Велсі.

Результати аналізу наукових публікацій. В основу написання даної статті покладено аналіз чинного інформаційного законодавства, законопроекти, які стосуються предмета дослідження, а також творчий доробок відомих вчених, зокрема В. Білоуса, В. Брижка, О. Довганя, І. Дороніна, Є. Захарова, М. Присяжнюка, В. Рубана, Т. Ткачука, В. Фурашева та ін.

Метою статті є визначення концептуальних засад обороноздатної інфраструктури України з урахуванням сучасних загроз та перспектив розвитку.

Виклад основного матеріалу. З цього приводу, як свідчать відкриті інформаційні джерела, у січні 2023 року Рада з геостратегії (Велика Британія), Польський інститут міжнародних відносин та Рада зовнішньої політики «Українська призма» створили комісію

експертів із трьох країн, яка включала дипломатів, експертів та політиків із метою якісної оцінки тристоронніх відносин та визначення, як їх можна переформувати у геополітичному середовищі, дискурсивним за змістом.

Саме такий тристоронній формат залишається актуальним не лише як доповнення до наявних, багатосторонніх форматів (НАТО і ЄС), а й як спосіб посилення голосів країн, що намагаються протистояти російській агресії. Адже співпраця між Польщею, Україною та Великою Британією зміцнює європейську безпеку у період можливих внутрішньополітичних потрясінь у США, що відбуваються на тлі президентської політики США, яка послаблює здатність США гарантувати українську та європейську оборонну ініціативу. У цьому напрямку, як додатковий запобіжний механізм світової безпеки, тристороння співпраця між Польщею, Україною та Великою Британією має сприяти обороноздатній допомозі Україні як пришвидшення перемоги України над рашистами. Це, у свою чергу, передбачає: допомогу Україні у розбудові спроможностей стримування на передодні вступу її у членство НАТО; посилення національної стійкості трьох країн; консолідація двосторонньої та багатосторонньої військово-промислової співпраці; підготовка до надійного та стресостійкого післявоєнного миру. Ці сфери залишаються пріоритетними з огляду на те, як російська федерація застосовує терористичну кібердіяльність проти України та країн-членів НАТО. Адже путінсько-російський режим продовжує і надалі зловмисно маніпулювати медійним висвітленням з метою заплутування громадської думки стосовно власної діяльності та підриву довіри громадськості до національних інституцій.

Таким чином, Україна показує, як можна поєднувати усі виміри держави і громадянського суспільства на підтримку воєнних зусиль. Адже витривала морально-психологічна стресостійкість та войовничий дух самовідданості українських громадян слугує яскравим прикладом і для НАТО як ціннісно-смислова настанова мудрості. Про це і свідчать численні ініціативи Альянсу, які звертають вагу на ефективно діючі практики інтелектуальної особи в повоєнній Україні. Тому, Польща і Велика Британія можуть разом знаходити і оцінювати висновки з українського бойового досвіду, які згодом можна застосувати ширше в структурі НАТО, що якісно впливатиме на міжнародно-правовий рейтинг. Звідси випливає, що створення тристоронньої комісії між трьома урядами для впорядкування та посилення євроатлантичних стратегічних комунікацій перед Україною дозволить визначити потенційний масштаб, який може бути досягнутий на тристоронньому рівні. Це, зокрема, щодо переходу до спільного виробництва боєприпасів, безпілотників та іншого військово-технічного обладнання, необхідного Україні для перемоги над рашистами. Це також втілює спільні навчання та освітньо-наукові проєкти, що значною мірою сприяють міжнародно-правовому рейтингу як шляхетно цивілізованому формуванню поліетнічного українства. Так, наприклад, цьому слугує приєднання Великої Британії до литовсько-польсько-української бригади, а також воєнно-оборонна співпраця з авангардними науково-дослідними інститутами міжнародної спільноти.

Крім того, російсько-українська війна показала слабкість колективної безпеки ООН і відсутність зобов'язань НАТО щодо країн, які не є його членами. На такому тлі відсутності колективної системи оборони в Азії створюється ризик для регіону, зокрема для Тайваню, який потенційно може постати наступною ціллю агресії Китаю. За таких обставин саме створення азійської версії НАТО має важливе значення для стримування КНР.

Адже в основу «азійського НАТО» можуть лягти існуючі альянси, такі як: США, Японія, Австралія, південна Корея, Канада, Філіппіни, Індія. Центральним елементом цієї структури може стати японсько-американський та український альянс. Також азійська версія НАТО повинна передбачати обмін американською ядерною зброєю або введенням ядерної зброї в регіон.

Мобілізація вітчизняної науки як інтелектуальний тренд у воєнно-нейромережевій криптосистемі державотворення. У наукових колах питання мобілізації їх інтелекту та самовизнання у світовий простір, як репутаційного розвитку міжнародної спільноти, ще з історичних часів минулого століття активно обговорювалося в 1960-х роках. Це був час, коли руйнувалися останні імперські проєкти у світі, а саме: у Африці, Азії, Латинській Америці, а нації тим часом здобували демократично-правову незалежність. Згідно з цим інтелектуальний капітал, який був зосереджений у наукових середовищах цих суспільств, ентропійно виплеснувся у нове дискурсивне поле, яке фокусувалося на питанні деколонізації вище означених держав.

Однак, умовно кажучи, у західноєвропейських університетах слов'янські студії переважно розбудовувалися на візіях саме російських наукових середовищ. Адже, на наш погляд, радує те, що загалом Канада здійснює затребуваний за вимогами реального часу національний проєкт, коли йдеться про нагальне питання співжиття, співпраці всіх народів, культур, із яких складається канадська спільнота. *Так, у кіберсучасності повоєнної України активно діє видавнича програма Гарвардського українського інституту.* Саме цей академічний рейтинг глобально-регіонального характеру є інтелектуальним показником релевантності як співпраці західноєвропейських інституцій з українськими, а також з видавничими проєктами світу. Адже такий науковий розвиток українських студій світового рівня є складовою державної політики України як інтелектуальна артикуляція фундаментальних знань про Україну. Оскільки наша держава має і в подальшому активно просувати затребувані воєнним часом знання, зокрема, у сфері філософії, права, міжнародних відносин.

Отже, виходячи із міжнародно-правового рейтингу в глобально-регіональному вимірі кіберспецслужби світу розпочали предметно та змістовно свою як латентну (приховану, негласну тощо), так і явну, прозору кібердіяльність як контрольно-координуючий моніторинг у світлі єдиного електронного реєстру світового рівня. На наш погляд, означений конкурентноздатний рейтинг академічних осіб західноєвропейської та західноазійської цивілізацій, безсумнівно, свідчить про достовірну наявність інтелектуальних здобутків на рівні особи, держави та суспільства як результативної моделі кіберспецслужб світу в шляхетних намірах (благородних, лицарських, войовничих тощо) постсучасності. Саме завдяки таким кіберспецслужбам світу стрімко розпочався корпускулярно-хвильовими темпами (квантовий стрибок) у вигляді новітнього циклу популяризації як репутації (самовизнання) україністики за кордоном, зокрема, у сфері юридичних досліджень. Проте, ще сьогодні вбачається пожвавлення пропагандистських антиукраїнських наративів в ідейному колі Канади. Знову ж таки не варто забувати, що в кіберсучасності повоєнна Україна також живе у контексті ізраїльської війни з ХАМАСом та ХАСБУЛою (фінансованою Іраном), що на «руку» російському агресору, який зловмисно, відволікаючи увагу, закидає пропагандистські наративи в іще геополітичне поле інформаційної війни. Тому, потрібно постійно та одностайно створювати у сучасних життєво необхідних сферах кібердіяльності інтелектуальну міць передового фронту як драйверу Перемоги України над путінсько-російським ворогом.

Кіберспецслужби України як злагоджений моніторинг та представництво міжвідомчо-силових структур щодо механізму адміністративно-правового забезпечення протидії корупції. У сучасну епоху цифровізації розв'язання проблем протидії корупції є одним із пріоритетних завдань в обороноздатній інфраструктурі України. Адже корупція, як визначено у стратегії національної безпеки, затвердженої Указом Президента України від 26.05.2015 № 287/2015, визнана актуальною загрозою національної безпеки. За особливих обставин значний рівень корупції в Україні як складного деструктивного явища обумовлений відсутністю дієвих реформ у сфері протидії корупції та неякісною діяльністю органів правопорядку щодо виявлення корупційних правопорушень та притягнення винуватців до відповідальності. Саме тому запобігання і протидія корупційним та пов'язаним із корупцією правопорушенням є одним із пріоритетних завдань кіберспецслужб України, в якій нагальне місце посідає контррозвідка. При цьому, за наявності в конкретних випадках, із негласними повноваженнями, покладаються ці функції на внутрішню безпеку у відповідних установах (підрозділах, структурах, організаціях тощо).

Особливої питомої ваги набуває ефективність антикорупційної політики в органах прокуратури, заходи якої в обороноздатній інфраструктурі України цілеспрямовані не лише на виявлення і притягнення до відповідальності осіб, які вчинили корупційні правопорушення, а на усунення причин виникнення та розповсюдження корупції серед її працівників. Це вимагає більш ретельної кібердіяльності «з боку керівництва органів прокуратури щодо створення праводієвого механізму комплексних заходів організаційного, профілактичного, навчального, науково-методологічного та дисциплінарного характерів щодо недопущення корупційних правопорушень в органах прокуратури та створення корупційних ризиків, а також зростання рівня свідомості працівника щодо не сприйняття корупції» [1, 3]. Тому система адміністративно-правового забезпечення протидії корупції повинна відповідати соціально-економічним умовам, за яких матиме ефективний результат.

Висновки. Таким чином, комплексне дослідження обраної проблематики з урахуванням оновленого законодавства, зокрема, про прокуратуру та протидію корупції не проводилось у воєнно-оборонній інфраструктурі саме інтелектуального капіталу України. Це негайно потребує системного наукового аналізу сучасного стану адміністративно-правового забезпечення протидії корупції в органах прокуратури України, що цілком сприятиме міжнародному рейтингу держави у західноєвропейській цивілізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Подоляка С. А. Адміністративно-правове забезпечення протидії корупції в органах прокуратури в Україні. автореферат дисертації на здобуття наукового ступеня доктора юридичних наук. К. 2019. 38 с.
2. Лісовський П. М., Подоляка С. А., Лісовська Ю. П. Спецслужби держав світу: ентропія, балістика, логістика: навчальний посібник. К.: Видавничий дім «Кондор». 2019. 289 с.
3. Лісовський П. М. Контррозвідка: квантова безпека та громадськість: навчальний посібник. К.: Видавничий дім «Кондор». 2020. 188 с.
4. Лісовський П. М., Лісовська Ю. П. Воєнна квантова безпека як інституційне кіберчислення а адміністративно-правовому режимі: монографія. Київ: Видавництво Ліра-К, 2023. 114 с.
5. Лісовський П. М., Лісовська Ю. П. Воєнна мережева криптосистема: державотворчий інноваційний контекст: монографія. Київ: Видавництво Ліра-К, 2024. 114 с.
6. Лісовський П. М., Бортник В. А., Лісовська Ю. П. Адміністративне право України: воєнний режим, відповідальність, територіальна цілісність6 навчальний посібник. К.: Видавничий дім «Кондор», 2024. 300 с.

REFERENCES:

1. Podolyaka, S. A. (2019). Administratyvno-pravove zabezpechennya protydiyi koruptsiyi v orhanakh prokuratury v Ukrayini [Administrative and legal support for combating corruption in prosecutorial bodies in Ukraine]. Avtoreferat dysertatsiyi na zdobuttya naukovoho stupenya doktora yurydychnykh nauk. K. 38 p.
2. Lisovs'kyy, P. M., Podolyaka, S. A., Lisovs'ka, Yu.P. (2019). Spetssluzhby derzhav svitu: entropiya, balistyka, lohistyka: navchal'nyy posibnyk [Special services of the world: entropy, ballistics, logistics: a textbook]. K.: Publishing house "Kondor". 289 p.
3. Lisovs'kyy, P. M. (2020). Kontrrozvidka: kvantova bezpeka ta hromads'kist': navchal'nyy posibnyk. [Counterintelligence: quantum security and the public: a textbook]. Kyiv: Publishing house "Kondor". 188 p.
4. Lisovs'kyy, P. M., Lisovs'ka, Yu. P. (2023). Voyenna kvantova bezpeka yak instytutsiyne kiberchyslennya a administratyvno-pravovomu rezhymi: monohrafiya [Military quantum security as institutional cyber computing in the administrative-legal regime: monograph]. K.: Lira-K Publishing House. 114 p.
5. Lisovs'kyy, P. M., Lisovs'ka, Yu. P. (2024). Voyenna merezheva kryptosystema: derzhavotvorchyy innovatsiynyy kontekst: monohrafiya [Military network cryptosystem: state-building innovative context: monograph]. K.: Lira-K Publishing House. 114 p.
6. Lisovs'kyy, P. M., Bortnyk, V. A., Lisovs'ka, Yu. P. (2024). Administratyvne pravo Ukrayiny: voyennyy rezhym, vidpovidal'nist', terytorial'na tsilisnist' navchal'nyy posibnyk [Administrative law of Ukraine: military regime, responsibility, territorial integrity, textbook.]. Kyiv: Publishing house "Kondor". 300 p.

Дата надходження статті: 20.06.2025
Дата прийняття статті: 20.07.2025
Опубліковано: 10.10.2025