Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2025. № 12.

DOI: http://doi.org/10.32702/2307-2156.2025.12.19
УДК 354.1

В. М. Кучерявий,
доктор філософії зі спеціальності 281 – публічне управління та адміністрування, доцент,
проректор з навчальної роботи,
Таврійський національний університет ім. В. І. Вернадського
ORCID ID: https://orcid.org/0009-0000-3250-2126
Н. В. Добрянська,
к. ю. н., професор,
професор кафедри державно-правових і гуманітарних наук навчально-наукового гуманітарного інституту,
Таврійський національний університет ім. В. І. Вернадського
ORCID ID: https://orcid.org/0000-0002-6319-0409

НАПРЯМИ ПОКРАЩЕННЯ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

V. Kucheriavyi,
Doctor of Philosophy in Specialty 281 – Public Management and Administration, Associate Professor, Vice-Rector for Academic Affairs,
V.I. Vernadsky Taurida National University
N. Dobrianska,
PhD in Law, Professor, Professor of the Department of State Law and Humanities, Educational and Scientific Humanitarian Institute,
V.I. Vernadsky Taurida National University

DIRECTIONS FOR IMPROVING PUBLIC ADMINISTRATION IN THE FIELD OF ENSURING CYBERSECURITY UNDER MARTIAL LAW

На сьогоднішній день наша держава знаходиться в епіцентрі гібридної агресії, де одночасно з традиційними воєнними операціями триває настільки ж жорстоке протистояння в кібернетичній сфері. Повномасштабна російсько-українська війна загострила проблему забезпечення кібербезпеки до рівня визначальної складової національної безпеки та обороноздатності будь-якої країни. Кібернетичний простір більше не обмежується тільки технічними аспектами; він став невід'ємним та життєво важливим елементом сучасної війни. Цілеспрямовані дії проти об'єктів критичної інфраструктури та урядових інформаційних платформ, систем управління військами, а також масштабні кампанії з розповсюдження неправдивої інформації на даний час вважаються невід'ємною складовою стратегії агресора, спрямованою на дестабілізацію ситуації в державі та нашого супротиву. За таких умов забезпечення ефективної кібербезпеки потребує не просто оперативної реакції на поточні випадки, а комплексного, проактивного підходу та безперервного удосконалення існуючих механізмів захисту. В статті наведено основні напрями покращення забезпеченні кібербезпеки в сучасних воєнних умовах в Україні, реалізація яких дасть можливість значно підвищити стійкість національної кіберсистеми, а також створити надійну основу для подальшого повоєнного відновлення та цифрової трансформації.

Today, our state is at the epicenter of hybrid aggression, where, simultaneously with traditional military operations, an equally brutal confrontation in the cyber sphere continues. The full-scale Russian-Ukrainian war has exacerbated the problem of ensuring cybersecurity to the level of a defining component of the national security and defense capability of any country. Cyberspace is no longer limited to technical aspects; it has become an integral and vital element of modern warfare. Targeted actions against critical infrastructure facilities and government information platforms, military command

systems, as well as large-scale campaigns to disseminate false information are currently considered an integral part of the aggressor's strategy aimed at destabilizing the situation in the state and our resistance. Under such conditions, ensuring effective cybersecurity requires not just a prompt response to current cases, but a comprehensive, proactive approach and continuous improvement of existing protection mechanisms. The article outlines the main directions for improving cybersecurity in modern military conditions in Ukraine, in particular, ensuring the stability of vital information systems; mastering the latest technical means; activating counterintelligence activities, international cooperation and harmonization of legislation; ensuring professional improvement and increasing cyber awareness; activating the development of public-private partnerships; establishing coordinated leadership and a reporting system, as well as improving asymmetric capabilities to deter the aggressor. Implementation of the above directions will make it possible to significantly increase the stability of the national cyber system (the number of successful cyberattacks and their destructive consequences for the state, society and business will decrease), as well as create a reliable basis for further post-war recovery and digital transformation (ensuring a high level of cybersecurity will become a decisive prerequisite for the further sustainable development of Ukraine as a modern digital state). Therefore, in general, it should be considered that ensuring cybersecurity in modern military conditions in Ukraine requires a continuous, comprehensive and flexible approach, which includes the introduction of technological innovations, effective coordination, legislative regulation and international assistance to effectively confront the aggressor in cyberspace.

Ключові слова: *публічне управління, кібербезпека, забезпечення кібербезпеки, держава, бізнес, напрями покращення кібербезпеки, війна, повоєнне відновлення.*

Keywords: *public administration, cybersecurity, ensuring cybersecurity, state, business, areas for improving cybersecurity, war, post-war recovery.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Повномасштабне вторгнення російської федерації на територію нашої держави внесло докорінні зміни у сектор безпеки, вивівши кібернетичний простір на рівень головного фронту гібридного протистояння. Так, Україна постійно переживає інтенсивні та систематичні кібератаки зі сторони російської федерації, мета яких полягає у порушенні діяльності критичної інфраструктури, дестабілізації сфери державного управління, а також у здійсненні розвідувальної діяльності та розповсюдженні неправдивої інформації. В сучасних умовах кібернетичний простір став невід'ємним елементом традиційних бойових дій, де кінетичні удари неодноразово супроводжуються чи передують кібернетичним атакам на системи управління, зв'язку та логістики. Крім цього, на сьогодні спостерігається критична залежність держави від інформаційних технологій, оскільки на рівень ефективності державного управління, розвитку економіки та обороноздатності держави критично впливає стійкість інформаційно-комунікаційних систем. Все це визначає потребу у здійсненні даного дослідження.

Аналіз останніх досліджень і публікацій. Дану проблематику досліджували такі науковці як Д. Березовський, О. Бодунова, Ю. Деркаченко, Д. Кисленко, С. Красніков, С. Кухтик, А. Лисеюк, Т. Свінцицька, В. Столбовий, В. Топчій, Ю. Яковенко та інші. Дані науковці засвідчують, що вдале протистояння кіберагресії можливе тільки при систематичному розвитку технічних можливостей, удосконалення законодавства та активної інтеграції в міжнародну систему кібербезпеки. Однак на сьогоднішній день відчувається гостра недостача досліджень в сфері забезпечення кібербезпеки в сучасних воєнних умовах в Україні.

Формулювання цілей статті (постановка завдання). Метою даної статті є визначення напрямів покращення публічного управління у сфері забезпечення кібербезпеки в умовах військового стану.

Виклад основного матеріалу дослідження. Задовго до лютого 2022 року експертна спільнота у сфері забезпечення кібернетичного захисту вже очікувала та готувалася до потенційних кібернетичних атак зі сторони російської федерації. Військові дії на території нашої держави стали головним важелем світового розвитку кіберзахисту та необхідності посилення заходів кібербезпеки на міжнародному рівні. Кіберпростір став таким же важливим полем битви, як і традиційне поле бою. Силу вітчизняних кібернетичних військ визнають на міжнародному рівні. Фактично, на даний час людство має змогу спостерігати за першою глобальною цифровою війною, на перебіг якої прямо відбиваються новітні технології. У 2022 році державою-агресорам було значно збільшено кількість кібератак на нашу державу. Під прицілом у ворога постійно знаходяться цивільні об'єкти, а саме: енергетичний та логістичний сектори, а також державні інформаційні системи. Тому слід вважати, що покращення забезпечення кібербезпеки в сучасних воєнних умовах в Україні є найважливішим пріоритетом та потребує систематичного удосконалення існуючих механізмів захисту та введення інноваційних підходів.

Україна під час широкомасштабної агресії зустрічається з різними видами кібератак та кіберзлочинів, країна-агресор прагне заблокувати надання електронних послуг наслідком чого є непоодинокі випадки порушення прав громадян, порушуються цілісність та конфіденційність персональних відомостей, здійснюються фішингові атаки, провокується інформаційно-психологічний натиск на людей. Тож, захист кіберпростору в умовах зазначених викликів виступає стратегічно важливим пріоритетом у системі національної безпеки України. Підкреслимо, що в умовах тривання воєнних дій на території України внаслідок широкомасштабного вторгнення росії питання захисту національних інтересів та критичної інформаційної інфраструктури набувають особливо гострої актуальності. Тож, для відвернення кіберзагроз та захисту території й інформаційного простору держави наразі потрібна концентрація всіх видів ресурсів та впорядкування

повноважень відповідних суб’єктів забезпечення кібербезпеки у поєднанні з дієвою державною політикою та ефективним нормативно-правовим забезпеченням зазначеної сфери [1, с. 33-34].

Забезпечення кібербезпеки в Україні є актуальним завданням у контексті зростання кіберзагроз, пов’язаних із війною, активізацією хакерських атак і поширенням кіберзлочинності. Відповідно до сучасних викликів, Україна реалізує низку стратегічних та оперативних заходів для забезпечення кібербезпеки. Основними напрямами забезпечення кібербезпеки в Україні є: розробка законодавчих актів, спрямованих на конкретні аспекти запобігання кіберзлочинності; інвестиції в інфраструктуру кібербезпеки; розширення міжнародної співпраці у сфері боротьби з кіберзлочинністю; зміцнення освітніх програм для підготовки кадрів у сфері кіберзахисту; створення регіональних центрів кібербезпеки для оперативного реагування на загрози [2, с. 666].

Впровадження заходів із забезпечення кіберзахисту в державному та приватному секторах в умовах тотальної цифровізації виступає невідкладною проблемою, яка прямо позначається на надійності роботи об’єктів критичної інфраструктури, впровадженні безпечного функціонування органів державної влади та підтримці відповідної суспільної діяльності. Беручи до уваги постійне зростання кількості кібернетичних атак, усвідомлення та ефективне правління кіберзагрозами стає обов'язковою передумовою для гарантування національної, корпоративної та приватної безпеки.

Держава робить важливі кроки з посилення стану забезпечення кібербезпеки як на нормативному, так і методичному рівнях. Така системна робота дозволить врегулювати питання реагування на різні види подій у кіберпросторі, значно посилити захищеність від кібератак державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури. З метою забезпечення кібербезпеки України необхідно посилювати взаємодію між основними суб’єктами національної системи кібербезпеки України, налагоджувати конструктивне і паритетне співробітництво.

Посилення стану забезпечення кібербезпеки також передбачає: підготовку та виконання Плану заходів із реалізації Стратегії кібербезпеки на 2023 рік; впровадження та адаптацію законодавства ЄС у національні стандарти у сфері кібербезпеки. Все ще проблемними питаннями залишаються: не достатня імплементація у чинне законодавство положень Конвенції Ради Європи про кіберзлочинність щодо обов'язкового зберігання та надання на вимогу правоохоронних органів операторами та провайдерами телекомунікацій інформації, необхідної для розслідування кіберзлочинів; використання провайдерами телекомунікаційних послуг механізму перетворення мережевих адрес за технологією NAT (Network Address Translation) без застосування механізмів логування, що ускладнює процес ідентифікації абонентів; використання зловмисниками Інтернет-сервісів та цифрових технологій, а також окремих послуг, що надають провайдери телекомунікацій та хостери, які унеможливлюють ідентифікацію злочинця або ускладнюють отримання іншої інформації, необхідної для розкриття злочину (використання методів TOR та I2P, криптовалют, виділених комунікаційних серверів, т. зв. "куленепробивних хостингів" тощо) [3, с. 121-122].

Вирішення зазначених проблем потребують комплексного підходу. Система забезпечення протидії кіберзлочинності повинна мати загальнодержавний характер. Як зазначалось вище, вона має охоплювати одразу декілька напрямків активної діяльності: юридичний (вдосконалення законодавства), міжнародний (розширення міжнародної співпраці), освітній (просвітницькі кампанії та відповідні навчальні програми у вищих навчальних закладах), політичний (активні дії з боку держави, спрямовані на захист свого інформаційного простору, цінностей), організаційний (передбачає активне державно-приватне партнерство), науково-технічний (вдосконалення інформаційних технологій). Найкращі світові практики зі створення безпечного кіберпростору мають бути використані в нашій країні. Доцільно запровадити галузеві регуляції, розроблені в інших державах.

Важливим кроком є створення єдиної інтелектуальної системи кібербезпеки для надійної охорони об’єктів у сфері державного управління та оборони. забезпечити її гнучкість та здатність швидко реагувати на загрози та зміни у технологіях [4, с. 89].

Основними підходами до підвищення кібербезпеки можна визначити: аутсорсинг, аналіз та моніторинг технологій кібератак, технічні інновації, реалізацію державних стратегій кібербезпеки, співпрацю з міжнародними інституціями та ін. Удосконалення існуючих підходів у розробці стратегій підвищення кібербезпеки на державному та корпоративному рівнях, передбачає врахування перспективних напрямів, які слід використовувати при формуванні політики кібербезпеки. Подальший розвиток сфери кібербезпеки на державному та корпоративному рівнях передбачає вдосконалення законодавства щодо кібербезпеки, політик та стратегій, спрямованих на забезпечення безпеки в цифровому середовищі. Крім того, існує необхідність співпраці між державними органами, корпоративним сектором, науково-дослідними установами та громадянським сектором для ефективного протистояння кіберзагрозам [5, с. 180-181].

На основі вище наведеного можна зробити наступні ключові висновки. По-перше, на даний час кібернетичний простір набув статусу справжнього поля бою. Російсько-українська війна абсолютно засвідчила, що кіберсфера є не допоміжним інструментом, а вирішальним фронтом протистояння. Застосування кібернетичних атак агресором є невід'ємним елементом загальної військової стратегії, спрямованого на дестабілізацію тилу, порушення логістики та управління військами.

По-друге, захист критичної інфраструктури є найголовнішим пріоритетом сучасності, оскільки спостерігається прямий зв'язок між ефективністю кіберзахисту та надійністю діяльності критичної інфраструктури (енергетичної системи, фінансового сектору, транспорту, зв'язку тощо). Введення новітніх технологічних рішень (моделі безпеки «нульової довіри» (Zero Trust) та системи виявлення загроз із використанням

штучного інтелекту), є обов'язковим в процесі забезпечення їх безперервного функціонування.

По-третє, на даний час існує гостра необхідність у проактивній та комплексній моделі оборони, оскільки пасивний захист є недостатньо ефективним. Покращення потребує переходу до моделі проактивного кіберзахисту (Threat Hunting), оперативного та обов'язкового реагування на випадки за допомогою централізований органів та розвитку власних асиметричних кіберспроможностей стримування.

По-четверте, поглиблення міжнародних зв'язків дозволяє зміцнити національну обороноздатність. Так, активізація міжнародного співробітництва з партнерами з НАТО та Європейського Союзу, обмін розвідувальними даними та гармонізація нормативно-правової бази з міжнародними стандартами відіграє критично важливу роль в процесі одержання технічної підтримки та підвищення загального рівня кіберстійкості держави. Водночас, варто відмітити, що вирішальним фактором перемоги в кібернетичній війні вважається високий рівень підготовки спеціалізованих кадрів. Тому нарощення інвестицій в освіту, підвищення кваліфікації військових та цивільних кібернетичних фахівців, а також ефективна взаємодія з бізнесом є визначальними напрямами для наступного покращення.

Відтак, загалом слід вважати, що забезпечення кібербезпеки в сучасних воєнних умовах в Україні потребує безперервного, комплексного та гнучкого підходу, що включає в себе впровадження технологічних інновацій, ефективну координацію, законодавче регулювання та міжнародну допомогу для ефективного протистояння агресору в кіберпросторі.

Висновки та перспективи подальших розвідок у даному напрямі. Таким чином, напрями покращення забезпечення кібербезпеки в сучасних воєнних умовах в Україні охоплюють:

1. Забезпечення стійкості життєво важливих інформаційних систем (необхідно зосередитися на забезпеченні безперебійності діяльності об'єктів

критичної інфраструктури, що перебувають під прицілом російських кібератак).

2. Освоєння новітніх технічних засобів (застосування інтелектуальних систем ідентифікації небезпек, моделей «нульової довіри» (Zero Trust), новітніх методів шифрування та засобів реагування на кінцевих пристроях задля запобігання несанкціонованим вторгненням та оперативного усунення наслідків інцидентів).

3. Активізація контррозвідувальної діяльності (систематична реалізація заходів, пов’язаних з виявленням, попередженням та припиненням актів кібершпигунства та кібертероризму зі сторони зарубіжних держав).

4. Активізація міжнародного співробітництва та гармонізації законодавства (поглиблення співробітництва з партнерами з Європейським Союзом та НАТО, обмін досвідом та розвідданими про небезпеки, а також пристосування вітчизянного законодавства до міжнародних стандартів кібербезпеки з метою одержання додаткової фінансової та технічної підтримки).

5. Забезпечення професійного удосконалення та підвищення кіберобізнаності (розвиток освітніх програм для підготовки висококваліфікованих спеціалістів з кібербезпеки та підвищення рівня поінформованості населення та бізнес-середовища про кіберзагрози і способи захисту).

6. Активізація розвитку державно-приватного партнерства (залучення бізнесу, наприклад вітчизняних та міжнародних технологічних компаній, до зміцнення кіберстійкості держави).

7. Налагодження координованого керівництва та системи звітування (забезпечення ефективної координації між усіма суб'єктами кібербезпеки (Державною службою спеціального зв'язку та захисту інформації України, Службою безпеки України, Радою національної безпеки і оборони України) та обов'язкове інформування Урядової команди реагування на кіберінциденти CERT-UA про всі випадки кібератак з метою швидкого

реагування та усунення наслідків).

8. Удосконалення асиметричних спроможностей для стримування агресора (необхідно розробити та впровадити інноваційні підходи з метою стримування потенційного агресора у кіберпросторі).

Виконання вище наведених напрямів необхідно здійснювати відповідно до Стратегії кібербезпеки України та планів заходів, які затверджені Кабінетом Міністрів України. Це дасть можливість значно підвищити стійкість національної кіберсистеми (зменшиться кількість вдалих кібератак та їх руйнівні наслідки для держави, суспільства та бізнесу), а також створити надійну основу для подальшого повоєнного відновлення та цифрової трансформації (забезпечення високого рівня кібербезпеки стане визначальною передумовою для наступного сталого розвитку України як новітньої цифрової держави).

Література

1. Лисеюк А. М., Свінцицька Т. В. Правове забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції. *Право та інновації.* 2024. № 4 (48). С. 32-38. DOI: https://doi.org/10.37772/2518-1718-2024-4(48)-4.

2. Топчій В. В., Бодунова О. М. Проблемні питання забезпечення кібербезпеки в Україні. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2025. Випуск 1. С. 664-669. DOI: https://doi.org/10.24144/2788-6018.2025.01.110.

3. Красніков С. А. Шляхи посилення стану забезпечення кібербезпеки в умовах воєнного стану. *Інформація і право.* 2023. № 3 (46). С. 118-128. DOI: https://doi.org/10.37750/2616-6798.2023.3(46).287214.

4. Яковенко Ю. Л., Деркаченко Ю. В., Кухтик С. В., Березовський Д. О. Шляхи удосконалення системи кібербезпеки в Україні. *Проблеми сучасних трансформацій.* 2021. № 1. С. 87-93. DOI: https://doi.org/10.54929/pmtl-issue1-2021-13.

5. Столбовий В. М., Кисленко Д. П. Заходи з підвищення кібербезпеки на державному та корпоративному рівнях в умовах діджиталізації суспільства. *Наукові записки Львівського університету бізнесу та права.* 2023. Випуск 37. С. 175-183. DOI: http://dx.doi.org/10.5281/zenodo.8019971.

References

1. Lyseiuk, A. M. and Svintsytska0 T. V. (2024), "Legal support for Ukraine's cybersecurity under martial law and European integration", Pravo ta innovatsii, vol. 4 (48), pp. 32-38. DOI: https://doi.org/10.37772/2518-1718-2024-4(48)-4.

2. Topchii, V. V. and Bodunova, O. M. (2025), "Problematic issues of ensuring cybersecurity in Ukraine", *Elektronne naukove vydannia «Analitychno-porivnialne pravoznavstvo»,* vol. 1, pp. 664-669. DOI: https://doi.org/10.24144/2788-6018.2025.01.110.

3. Krasnikov, S. A. (2023), "Ways to strengthen the state of ensuring cybersecurity in conditions of martial law", *Informatsiia i pravo,* vol. 3 (46), pp. 118-128. DOI: https://doi.org/10.37750/2616-6798.2023.3(46).287214.

4. Iakovenko, Yu. L., Derkachenko, Yu. V., Kukhtyk, S. V. and Berezovskyi D. O. (2021), "Ways to improve the cybersecurity system in Ukraine", *Problemy suchasnykh transformatsii,* vol. 1, pp. 87-93. DOI: https://doi.org/10.54929/pmtl-issue1-2021-13.

5. Stolbovyi, V. M. and Kyslenko, D. P. (2023), "Measures to improve cybersecurity at the state and corporate levels in the context of digitalization of society", *Naukovi zapysky Lvivskoho universytetu biznesu ta prava,* vol. 37, pp. 175-183. DOI: http://dx.doi.org/10.5281/zenodo.8019971.

Стаття надійшла до редакції 15.12.2025 р.