СЕКЦІЯ 4
ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

АКТУАЛЬНІСТЬ ПОСИЛЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ДІЇ ВОЄННОГО СТАНУ В КОНТЕКСТІ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

THE RELEVANCE OF STRENGTHENING CYBER SECURITY OF UKRAINE UNDER THE CONDITIONS OF MARITAL STATE IN THE CONTEXT OF EUROPEAN INTEGRATION

УДК 351:862
DOI https://doi.org/10.32782/pma2663-5240-2023.34.14

Костенко В.О.
к. наук з держ. упр.,
ст. викладач кафедри управління у сфері цивільного захисту
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України

Кринична І.П.
д. наук з держ. упр., професорка,
професорка кафедри менеджменту освіти та права
Центральний інститут післядипломної освіти Державного вищого навчального закладу «Університет менеджменту освіти» Національної академії педагогічних наук України

Журбинський Д.А.
к. тех. наук, доцент,
доцент кафедри організації заходів цивільного захисту
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України

Дана стаття присвячена надзвичайно актуальній на сьогодні проблемі удосконалення державного управління у сфері національної безпеки України в умовах інформаційних небезпек та загроз, пов'язаних із повномасштабною агресією Російської Федерації проти нашої держави. У ній висвітлюються основні напрями державної політики, законодавчі та нормативно-правові акти стосовно забезпечення ефективних механізмів державного управління у сфері кібербезпеки, як надзвичайно важливого аспекту кіберзахисту державних інституцій в умовах особливого періоду. Розглянуто питання інформаційної безпеки України та заходи здійснювані державою, які спрямовані на поліпшення її стану для забезпечення обороноздатності країни. Відмічається динаміка стрімкого зростання скоєних злочинів у сфері кібербезпеки держави, які обліковуються в Україні з початку широкомасштабної війни в Україні. Проаналізовано ключові здобутки та прогалини у сфері кіберзахисту, подальші кроки, які дозволять посилити національну систему кібербезпеки і ефективніше протидіяти загрозам у кіберпросторі в контексті євроатлантичної інтеграції. Зазначається, що значне поширення кіберзагроз на усі сфери життєдіяльності та вдосконалення інструментарію їх реалізації в умовах гібридної війни зумовлює необхідність зміни та удосконалення стратегії і тактики протидії ним. Акцентується увага на необхідності посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Визначено пріоритетні напрями і практичні кроки щодо посилення кіберзахисту України. Акцентавано увагу на важливості міжнародної співпраці у сфері кібербезпеки. Окрему увагу приділено питанням реалізації Стратегії кібербезпеки України на найближчу перспективу з урахуванням загроз воєнного характеру.

Ключові слова: *кіберзахист, кібербезпека, кіберзагроза, кібератака, національна безпека, воєнний стан.*

This article is devoted to the currently extremely urgent problem of improving public administration in the sphere of national security of Ukraine in the conditions of informational dangers and threats associated with the full-scale aggression of the Russian Federation against our state. It highlights the main directions of state policy, legislative and regulatory acts regarding the provision of effective mechanisms of state management in the field of cyber security, as an extremely important aspect of cyber protection of state institutions in the conditions of a special period. The issue of information security of Ukraine and the measures taken by the state aimed at improving its condition to ensure the country's defense capability were considered.
The dynamics of the rapid growth of crimes committed in the field of cyber security of the state, which have been registered in Ukraine since the beginning of the large-scale war in Ukraine, are noted. Key achievements and gaps in the field of cyber protection, further steps that will allow strengthening the national cyber security system and more effectively counter threats in cyberspace in the context of Euro-Atlantic integration are analyzed. It is noted that the significant spread of cyber threats to all spheres of life and the improvement of the toolkit for their implementation in the conditions of hybrid warfare necessitates the need to change and improve the strategy and tactics of countering them. Attention is focused on the need to strengthen the capabilities of the national cyber security system to counter cyber threats in the modern security environment. Priority directions and practical steps to strengthen Ukraine's cyber defense have been determined. Attention was focused on the importance of international cooperation in the field of cyber security. Particular attention was paid to the issues of implementing the Cyber Security Strategy of Ukraine for the near future, taking into account threats of a military nature.

Key words: *cyber defense, cyber security, cyber threat, cyber attack, national security, martial law.*

Постановка проблеми у загальному вигляді **та її зв'язок з важливими науковими чи практичними завданнями**. Національна безпека України в умовах дії воєнного стану істотно залежить від ефективності забезпечення кібербезпеки. Під час війни ворог постійно здійснює цілеспрямовані атаки, використовуючи інформаційний простір для завдання шкоди обороноздатності України. Відсутність ґрунтовного законодавчого і організаційно-управлінського забезпечення кібербезпеки в Україні в умовах гібридної війни значно підвищує ризики руйнування національної системи. Ця проблема погіршується

ще й тим, що на сьогодні в державі відсутній єдиний центр координації роботи щодо законодавчого та нормативно-правового забезпечення системи кібербезпеки, яка б базувалась на комплексному реальному аналізі стану в цій сфері, існуючих реальних і потенційних загроз, інтегрувалась в європейську і глобальну систему кібернетичної безпеки, мала б достатнє організаційне, фінансове, технічне та кадрове забезпечення.

Зазначена проблема значно посилилась ще із початком гібридної війни Росії проти України із 2014 року. Ключовим гібридним інструментом агресор використовує інформаційні технології та системи комунікацій у кіберпросторі. Масовані кібератаки тривають і в умовах ведення бойових дій. За офіційними даними Офісу Генерального прокурора лише протягом перших дев'яти місяців війни кіберзлочинність в Україні стабільно зростає [1].

Такого роду кібератаки стали можливими лише через те, що не був забезпечений надійний та досконалий захист інформаційних ресурсів такої надважливої сфери діяльності держави, як національна кібербезпека. Тому, удосконалення державного управління у сфері забезпечення національної кібербезпеки в сучаних умовах є актуальною тематикою наукових досліджень.

Аналіз останніх досліджень і публікацій. Питанню кібербезпеки були присвячені численні дослідження закордонних та вітчизняних науковців, які висвітлювали різні аспекти цієїпроблематки, від безпекових особливостей інформаційних технологій та кіберзлочинів до інформаційних війн. Серед зарубіжних дослідників слід зазначити Е. Грінберга, Л. Стрельцова, Л. Керулуса Р. Мудіта ін. Серед вітчизняних науковців відзначається відсутність єдиного підходу до системного аналізу проблеми кібербезпеки. Так, підходи варіюються від правових аспектів до стратегій силових відомств та військових ініціатив. Л.С. Харченко, В.А. Ліпкан, О.В. Логінов описують кібербезпеку як складову національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України.

Системний характер кібербезпеки дозволяє визначити її забезпечення як складний та комплексний вид діяльності уповноважених органів. Результати аналізу останніх джерел свідчать про недостатню розробленість забезпечення кібербезпеки в Україні, особливо в умовах військової агресії.

Мета статті – розглянути питання національного кіберзахисту в світлі російської агресії та пріоритетні напрямки забезпечення кібербезпеки України в умовах дії воєнного часу в контексті євроатлантичної інтеграції.

Виклад основного матеріалу дослідження. З початком повномасштабної війнимайже всі українські державні сайти, банківські сервіси, системи та інфраструктура зазнали величезної кількості ворожих кібератак та збоїв.Почалися атаки на офіційні сайти Верховної Ради України, Кабінету Міністрів України, Міністерства закордонних справ України, Служби безпеки України, Міністерства оборони України, Міністерства України з питань реінтеграції тимчасово окупованих територій, ПриватБанку та Ощадбанку, а також великої кількості інших установ [2].

Загалом, кібератаки були націлені на приховане викрадення важливої інформації, ймовірно, для надання Росії стратегічної переваги на полі бою. Все цевідбувається для того, аби здійснювати психологічний тиск на громадян, дестабілізувати ситуацію всередині країни, посіяти паніку і хаос, паралізувати засоби комунікації й зв'язку у нашій державі. Посилюється тенденція здійснення розвідувально-підривної діяльності у кіберпросторі шляхом залучення різними спеціальними службами окремих держав, насамперед Росії, міжнародних хакерських угруповань для реалізації кібервпливу [3].

У наш час війна в інформаційному просторі може завдати не меншої шкоди, аніж війна на полі бою. Загроза кібератак з боку РФ як на українські системи, так і на європейських партнерів залишається високою. Кібербезпека наразі є ключовим питанням в економічному, політичному, соціальному та військовому аспектах. Сьогодні Україна змушена відстоювати своє право на незалежність, на власний вектор розвитку та мирне і вільне майбутнє. Тобто, перед вітчизняними правоохоронними органами постає все більше завдань із пошуку нових засобів та методів дієвої боротьби з кіберзлочинністю.

З початку війни Україна стала ціллю чисельних кібератак, які охопили державні установи, приватні організації та громадян. Ті підприємства, які є частиною критичної інфраструктури, зокрема енергетичні, телекомунікаційні, медіа та фінансові компанії, також мають бути у режимі підвищеної готовності, оскільки саме ці галузі часто вважаються пріоритетними цілями у період війни. Бізнес має бути готовий протидіяти цим викликам – компанії повинні оцінити свою готовність до кіберінцидентів і свою здатність відновити діяльність.

З 2014 року Росія активно використовує кіберпростір у гібридній агресії проти України

шляхом здійснення деструктивного впливу на органи державної влади, системи управління військами та зброєю сил оборони, а також на об'єкти критичної інфраструктури. Держава-агресор невпинно нарощує свій арсенал кіберзброї наступального, розвідувального, а такожпідривного призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Зазначені чинники вимагають постійного нарощування в Україні можливостей забезпечення кібербезпеки органами сектору безпеки і оборони.

На сьогодні Російська Федерація залишається одним із основних джерел загроз національній та міжнародній кібербезпеці, яка дуже активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно і широко застосовуються у гібридній війні проти української держави. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій щодоукраїнської національної інформаційної інфраструктури [4].

В Україні діє Закон «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [5].

Незадовго до широкомасштабного вторгнення Росії в Україну Указом від 26.08.2021 року № 447 Президент України затвердив рішення Ради національної безпеки і оборони України від 14.05.2021 року «Про Стратегію кібербезпеки України», яка визначає пріоритети національних інтересів у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози, цілі та завдання забезпечення кібербезпеки з метою створення належних умов для безпечного функціонування кіберпростору, його використання в інтересах суспільства і держави [4].

Указом Президента України від 01.02.2022 року № 37 було уведено в дію рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України» [6].

Проте, значне поширення кіберзагроз на усі сфери життєдіяльності та вдосконалення інструментарію їх реалізації в умовах гібридної війни зумовлює необхідність зміни та удосконалення стратегії і тактики протидії ним. Набуває значимості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди.

Незважаючи на наявність цілої низки чинних нормативно-правових документів щодо проблем забезпечення безпеки кіберпростору держави, вони не охоплюють усього спектра сучасних загроз кібербезпеці держави. Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету повинна здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Кіберскладова є важливим елементом у війні України проти Росії. Ефективність кібербезпеки та відбиття кібератак в умовах воєнного стану полягає у максимальній координації та командній роботі.

Тож ефективна протидія загрозам національній безпеці у кіберсфері можлива лише за умови комплексного використання всього арсеналу правових засобів забезпечення кібербезпеки, за всіма структурними елементами державного управління та на всіх етапах обігу інформації. Крім того, максимального ефекту у взаємодії суб'єктів забезпечення кібербезпеки України можливо досягти виключно шляхом використання цілісного системного механізму адміністративно-правових методів та засобів, завдяки якому здійснюється реалізація державної політики у сфері забезпечення кібербезпеки як складового елементу національної безпеки.

Для України сьогодні являється надзвичайно актуальним впровадження міжнародного досвіду у сфері адміністративно-правового забезпечення кібербезпеки, який є необхідним у якості успішного прикладу щодо формування відповідної політики та побудови власної системи правового та організаційного забезпечення кібербезпеки, у першу чергу, в умовах сучасної гібридної війни. Ефективність адміністративно-правового забезпечення кібербезпеки забезпечується одночасними заходами, спрямованими як у напрямі співпраці з фаховими міжнародними інституціями стосовно забезпечення кібербезпеки, так і у напрямі формування адекватного викликам гібридної війни національного законодавства у цій сфері.

У 2022 році ухвалено низку важливих законів. Законодавчі зміни, зокрема, стосуються активної протидії агресії у кіберпросторі,

хмарних послуг та розміщення у «хмарах» державних інформаційних ресурсів, захисту критичної інфраструктури України. Триває робота і над іншими нормативно-правовими актами, які дозволять врегулювати питання реагування на різні види подій у кіберпросторі, посилити захищеність від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури та інших [7].

При цьому,слід акцентувати увагу на посиленні міжнародної співпраці. Серед надійних партнерів Держспецзв'язку – Агентство з кібербезпеки та безпеки інфраструктури США (CISA), Агентство ЄС з питань кібербезпеки (ENISA), Команда реагування на комп'ютерні надзвичайні події CERT-EU [7].

На сьогодні розроблено проєкт Стратегії кібербезпеки України на 2021 – 2025 роки. Дана Стратегія визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Кібербезпека є одним із пріоритетів у системі національної безпеки України. Вона передбачає посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Пріоритетами забезпечення кібербезпеки України є: убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки. Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації Стратегії [8].

Висновки. Долучення України, її цивільних та військових органів до європейських та євроатлантичних ініціатив створить надійне підґрунтя для цілеспрямованого процесу розвитку кібернетичної стратегії на державному та приватному рівнях. Необхідно негайно посилювати взаємодію між основними суб'єктами національної системи кібербезпеки України, а також налагоджувати конструктивне та швидке співробітництво. В умовах воєнного стану головним зовнішньополітичним пріоритетом України у сфері кібербезпеки є поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

ЛІТЕРАТУРА:

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. Офіційний веб-сайт Офісу Генерального прокурора України. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

2. Щодо кібератак на сайти державних органів. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/shodo-kiberatak-na-saiti-derzhavnikh-organiv

3. Щодо кібератаки на сайти військових структур та державних банків. Офіційний веб-сайт Кабінету Міністрів України. URL: https://www.kmu.gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-ta-derzhavnih-bankiv

4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Указ Президента України від 26.08.2021 № 447. URL: https://www.president.gov.ua/documents/4472021-40013

5. Про основні засади забезпечення кібербезпеки України.Закон України від 5 жовтня 2017 року № 2163-VIII. (Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403).

6. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України».Указ Президента України від 01.02.2022 № 37. URL: https://zakon.rada.gov.ua/laws/ show/37/2022#n5

7. Національна кібербезпека в умовах війни: основні досягнення, плани та перспективи. URL: https://cip.gov.ua/ua/news/nacionalna-kiberbezpeka-v-umovakh-viini-osnovni-dosyagnennya-plani-ta-perspektivi

8. Проєкт Стратегії кібербезпеки України (2021–2025 роки). URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf