АНОТАЦІЯ

Зінченко О.І. «Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону». – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 052 «Політологія». – Харківський національний університет імені В.Н. Каразіна, Харків, 2025.

Актуальність дисертаційної роботи передусім визначаємо динамічним розвитком інформаційних технологій і глобалізацією кіберпростору, що створює нові виклики для безпеки. Кібертероризм – це явище, яке набуло транснаціонального характеру, і масштабність його зростання є прямим наслідком зловживання відкритістю та доступністю глобальних інформаційних мереж. Сучасні виклики кібертероризму підривають не лише економічну стабільність, а й політичну систему держав, а його удари спрямовані на критичну інфраструктуру, урядові установи та, навіть, демократичні процеси.

Для проникнення в системи, викрадення конфіденційних даних, порушення роботи критично важливих служб і поширення страху кібертерористи використовують вразливості в програмному та апаратному забезпеченні, а також людській поведінці. Мотиви таких атак різноманітні – від ідеологічних і політичних цілей до фінансової вигоди. Атакуючи критично важливі об'єкти інфраструктури, зокрема електромережі, системи водопостачання, транспортні мережі, заклади охорони здоров'я, тощо, кібертерористи можуть викликати широкомасштабний хаос і підірвати довіру громадськості до урядових інституцій. Крім того, цілеспрямовані атаки на демократичні процеси, зокрема вибори, за допомогою дезінформаційних кампаній, хакерських атак і маніпуляцій з даними, становлять пряму загрозу легітимності влади і верховенству права.

У Європейському регіоні, де спостерігаємо високий рівень цифровізації державного управління та суспільного життя, ця загроза стає особливо критичною. Атаки на урядові органи, системи енергопостачання або охорони здоров’я здатні паралізувати життя держави та створити підґрунтя для політичної дестабілізації.

Відповідно, озброєння кіберпростору як державними, так і недержавними акторами може призвести до ескалації геополітичної напруженості та нової ери цифрових війн. Особливо важливо відзначити, що ефективні контртерористичні стратегії повинні враховувати прогалини в законодавстві, такі, як відсутність загальноприйнятого визначення кібертероризму і проблеми транскордонної юрисдикції. З політичного погляду існує потреба в більш тісній співпраці між країнами, а також між державним і приватним секторами для обміну розвідданими, передовим досвідом і технічними ресурсами. У соціальному плані підвищення обізнаності громадськості про кібербезпеку і розвиток культури цифрової стійкості є важливими для зменшення людської вразливості, якою часто користуються кібертерористи.

Отже, можемо зазначити, що актуальність цієї теми не обмежена проблемами національної безпеки окремих держав; вона стосується ширших глобальних викликів, пов'язаних насамперед із нестабільністю і вразливістю цифрового простору, які, зі свого боку, мають далекосяжні наслідки для політичних й економічних систем цілих регіонів та за їх межами.

Перший розділ дисертаційної роботи присвячений аналітичному розгляду теоретичного апарату таких термінологічних категорій, як «кібертероризм», «кібербезпека», «національна безпека держави».

У розділі також наголошено на необхідності захисту інформаційних мереж від кібертероризму, а першочерговим завданням вважаємо фіксування цього терміна на законодавчому рівні. Запропоновано, по-перше, модернізувати наявне в українському законодавстві визначення, а по-друге, з огляду на його актуальність і небезпеку цього явища, увести поняття

«кібертероризм» до правової системи на регіональному рівні. Окрім цього, через фрагментарність та відсутність єдиного термінологічного апарату на загальноєвропейському рівні вказано на важливості трансформації поняття «кібербезпека». Таким чином, проаналізовано наявні дослідження й досягнуті результати, указано на прогалини й дискусійні моменти, сформульовано нове розуміння поняття «кібертероризму» як політичного концепту. Зважаючи на уточнення визначення поняття «кібербезпека» та, відповідно, формулювання альтернативного підходу, надано рекомендації щодо вдосконалення національної політики України з кібербезпеки. Ідеться, зокрема, про запровадження нових політичних концепцій, таких, як «кіберсоціальна адаптація» та «кіберімунітет». Інноваційні підходи до кібербезпеки забезпечують комплексні гарантії національних інтересів у цифровому просторі. Для формування суспільного імунітету, здатного пом'якшити згубні наслідки кібертероризму, концепція «кібернетичного імунітету» передбачає одночасне застосування політичних і соціальних інструментів. Водночас «кіберсоціальна адаптація» стосується соціокультурних аспектів кібербезпеки, що визначає необхідність для суспільств розвиватися і адаптуватися до викликів, пов'язаних із цифровою епохою, в культурному і соціальному вимірах.

У дослідженні також акцентовано на важливості міждисциплінарної методології, гармонізації правових підходів та міжнародного співробітництва в боротьбі з кібертероризмом. Ключовими рекомендаціями є створення спеціалізованих національних підрозділів кіберполіції, модернізація наявних стратегій кібербезпеки та впровадження систем проактивного моніторингу критичної інфраструктури. Крім того, у дослідженні запропоновано запровадити посаду «кібер-омбудсмена», завданням якого є відстоювання державних інтересів, захист прав громадян та забезпечення свобод у цифровому просторі.

Другий розділ присвячено аналізу комплексної системи забезпечення кібербезпеки в державах європейського регіону, які мають високий рівень

захищеності від різного типу кібератак. Вивчення досвіду окремих країн регіону дозволяє визначити ключові моменти, які мають бути введені в систему захисту кіберпростору України, що допоможе протидіяти новим кіберзагрозам реалізовувати низку необхідних реформ, спрямованих на зміцнення правової, інституційної та стратегічної політичної систем.

Автор визначає, що чинна нормативно-правова база характеризується фрагментарністю та неефективністю, а це перешкоджає формуванню єдиної національної стратегії, здатної протистояти витонченій кібертерористичній діяльності. У своєму дослідженні автор пропонує за допомогою інтеграції принципів забезпечення кібербезпеки в більш послідовну та всеосяжну законодавчу структуру переглянути та гармонізувати застарілі правові норми. Насамперед, підкреслено на необхідності розширення національної стратегії кібербезпеки України з урахуванням сучасних викликів відповідно до оновлених міжнародних стандартів і геополітичних реалій. З метою посилення ролі в координації національної політики кіберзахисту також потребує реформування CERT-UA (урядова команда реагування на комп'ютерні надзвичайні події України). У таких критично важливих сферах, як охорона здоров'я, енергетика, державне управління та електронні комунікації, пропонуємо секторальний підхід, який для вирішення проблем забезпечення кібербезпеки передбачає створення спеціалізованих підгруп. Така реструктуризація має на меті підвищити ефективність та результативність зусиль України у сфері кібербезпеки, забезпечивши цілеспрямоване реагування на галузеві загрози й укріпивши загальну стійкість цифрової інфраструктури країни.

Крім того, з метою інтеграції кібертероризму в його оперативний мандат автор в своєму дослідженні акцентує на важливості трансформації Антитерористичного центру України. Зосереджений наразі на фізичних аспектах тероризму, центр у межах системи реагування повинен перетворитися на єдине відомство, здатне протидіяти як фізичним, так і кіберзагрозам. Така трансформація не лише посилить внутрішню безпеку

України, а й підвищить її роль у формуванні міжнародної політики безпеки. Використовуючи свій великий досвід у протидії гібридним загрозам, особливо з боку Росії, Україна може зробити унікальний внесок у глобальні зусилля з кібербезпеки. Цей стратегічний зсув відповідає ширшим цілям України, зокрема вступу до Європейського Союзу та НАТО, оскільки обидві організації надають кібербезпеці важливого значення у своєму порядку денному.

Відповідні реформи необхідні для переходу України від оборонної позиції до активної участі в глобальних ініціативах з кібербезпеки. Модернізувавши правову базу, реструктуризувавши ключові інституції та посиливши роль інтеграції протидії кібертероризму до стратегії безпеки, Україна може посилити свою стійкість до цифрових загроз. Такі зміни не лише зміцнять національну безпеку, але й позиціонуватимуть Україну як цінного партнера в міжнародних зусиллях із боротьби з кіберзагрозами, тим самим підтримуючи її інтеграцію в регіональні та міжнародні безпекові структури.

З метою забезпечення захисту в цифровому середовищі та підвищення обізнаності суспільства розроблена автором «Національна програма кіберосвіти» й доведена її необхідність. Ідея цього проєкту виникає на тлі «кадрового голоду» через війну. Брак працівників спостерігався і в сфері кіберзахисту, оскільки значний масив людей був мобілізований до лав ЗСУ, велика кількість населення також змушена була емігрувати. Програма розрахована на спеціалізовані напрямки професій, які необхідні для забезпечення функціонування критичних об’єктів держави, і матиме окремі плани, зорієнтовані для навчання медичних працівників, фінансистів та економістів, працівників енергетики, науковців, державних службовців та юристів. Кожен напрям матиме окремі варіанти підготовки та отримання знань, необхідних саме для діяльності окремих фахівців. З огляду на це вважаємо, що така програма дасть кожному професіоналу точні знання, необхідні для найбільш ефективної роботи в цифровому робочому середовищі.

У третьому розділі дослідницька увага зосереджена на тому, як повномасштабне вторгнення Росії у 2022 році змінило політичний ландшафт України та створило значні виклики безпеці європейських держав, зокрема й акцентовано на еволюцію загроз у кіберпросторі. Україна стала головною мішенню російських кібератак, які серйозно порушили роботу державних і приватних установ, критично важливих об'єктів інфраструктури та національних систем зв'язку. Ці кіберзагрози мають не лише прямі наслідки для України, але й створюють опосередковані ризики для європейської безпеки з урахуванням стратегічної ролі України як геополітичного буфера між Росією та Європою.

Отже, увага насамперед акцентована на політичному складнику вказаної проблеми. Конкретний вплив кібератак на критичну інфраструктуру України було розглянуто з особливим акцентом на двох ключових секторах: енергетичній інфраструктурі та системі електронної охорони здоров'я. Ці сектори визначені автором як життєво важливі для функціонування держави та особливо вразливі до кіберзагроз. Аналізуючи виклики в цих сферах та їхню вразливість, результати дослідження можуть стати внеском у посилення заходів кібербезпеки в Україні та, як наслідок, зміцнити загальну архітектуру безпеки в Європі.

У контексті ядерної інфраструктури дослідження підкреслює необхідність передових захисних заходів для пом’якшення ризиків кібератак, які можуть мати катастрофічні наслідки. Наголошено на важливості встановлення та закріплення концепції «ядерної кібербезпеки» в міжнародно-правовому полі, яка має велике стратегічне значення для України та Європи. Захист ядерних установок представлений як технічна та політична необхідність, що вимагає спільних зусиль держав, міжнародних організацій і наукового співтовариства для ефективного вирішення сучасних викликів безпеки. Аналізуючи поточний стан кібербезпеки електронної охорони здоров’я в Україні та порівнюючи його з практикою в окремих європейських країнах, визначаємо ключові вразливі місця та напрями для покращення.

Наголошено на важливості впровадження передового міжнародного досвіду та розроблення надійної законодавчої бази для посилення кібербезпеки в секторі охорони здоров’я.

Загалом визначено взаємопов’язаний характер викликів кібербезпеці в критично важливих секторах і вказано на потребу скоординованого багатобічного підходу для посилення стійкості України проти кіберзагроз. Вирішення цих проблем допоможе також зробити внесок у ширший дискурс про національну та регіональну безпеку в світі, що все більше цифровізується.

У роботі підкреслено, що в епоху цифровізації важливою є взаємопов'язаність національної та регіональної безпеки, а також доведена необхідність скоординованого підходу до розв’язання багатогранних викликів, пов'язаних із кібервійною.

У дисертаційному дослідженні запропоновано альтернативний підхід до визначення поняття «кібертероризм». Зважаючи на це, автором обґрунтована необхідність посутнього регулювання європейського законодавства щодо ефективної протидії актам кібертероризму. Спираючись на отримані в Україні уроки, автор наголошує на важливості встановлення європейських стандартів протидії кібертероризму, а також виявляє прогалини в нинішньому визначенні поняття «кібербезпека», необхідності реформування чинного українського та європейського законодавства з метою протидії новим викликам. Автор пропонує шляхи вдосконалення політики кібербезпеки України, одним із яких є створення посади «кібер-омбудсмена». Автор вводить нові соціально-політичні концепції, такі, як «кіберсоціальна адаптація» та «кіберімунітет», які є життєво важливими для зміцнення кібербезпеки. Крім того, у дослідженні акцентовано на необхідності уніфікованих правових підходів і посилення міжнародного співробітництва.

Звернена увага на спричинену війною та міграцією проблему кадрового голоду, зокрема брак експертів з кібербезпеки. З огляду на це запропоновано спеціалізовану кіберосвіту для різних професій «Національна програма підготовки фахівців з кібербезпеки». У тексті дисертаційної роботи

наголошено на необхідності реформування інституційних структур, що гарантують кібербезпеку України, посилення координації в таких секторах, як охорона здоров'я, енергетика, правоохоронні органи та електронні комунікації, детально обговорено важливість забезпечення кібербезпеки ядерної сфери та системи електронної охорони здоров'я.

Насамкінець для ефективної боротьби з кібертероризмом наголошуємо на необхідності регулювання та вдосконалення законодавства й міжнародної співпраці. У дисертації запропоновані рекомендації щодо вдосконалення політики України у сфері кібербезпеки, включно зі створенням нових інституцій та реформуванням наявних. Указано на важливості запровадження концептів «ядерної кібербезпеки» та «кібербезпеки eHealth», надано деталізовані пропозиції щодо реформування відповідних сфер у запропонованому порядку для України.

Ключові слова: *активні заходи, державна політика в сфері кібербезпеки, гібридна війна, зовнішня політика, кібертероризм, механізми регіонального управління, політична адаптація, політична інтеграція, політичні інститути, світовий порядок, суверенітет держави*.

ABSTRACT

Dissertation for the degree of Doctor of Philosophy in the speciality 052 – Political Science. V. N. Karazin Kharkiv National University, Kharkiv Ukraine, 2025.

The relevance of this dissertation is primarily determined by the dynamic development of information technology and cyberspace globalisation, which creates new security challenges. Cyberterrorism is a phenomenon that has become transnational, and the scale of its growth is a direct consequence of the abuse of the global information networks openness and accessibility. The current challenges of cyberterrorism undermine not only economic stability but also the political system of states, and its attacks target critical infrastructure, government institutions and even democratic processes.

Cyberterrorists exploit vulnerabilities in software, hardware and human behavior to infiltrate systems, steal confidential data, disrupt critical services and spread fear. The motives for such attacks vary from ideological and political goals to financial gain. By attacking critical infrastructure, such as power grids, water supply systems, transport networks, healthcare facilities, etc., cyberterrorists can cause widespread chaos and undermine public confidence in government institutions. In addition, targeted attacks on democratic processes, including elections, through disinformation campaigns, hacking and data manipulation, pose a direct threat to the legitimacy of government and the rule of law.

In the European region, where we observe a high level of digitalization of public administration and public life, this threat is particularly critical. Attacks on government agencies, energy supply or healthcare systems can paralyze the life of a state and create the basis for political destabilization.

Consequently, the weaponization of cyberspace by both state and non-state actors could escalate geopolitical tensions and usher in a new era of digital warfare. Notably, effective counterterrorism strategies have to address legislative gaps, including the absence of a universally accepted definition of cyberterrorism and challenges related to cross-border jurisdiction. Politically, closer international

cooperation – between states as well as public and private sectors – is essential to facilitate intelligence sharing, best practices, and technical resource allocation.

At the social level, raising public awareness of cybersecurity and digital resilience culture developing are important to reduce the human vulnerabilities that cyberterrorists often exploit.

Thus, we can note that the relevance of this topic is not limited to the individual states' national security problems, however it concerns broader global challenges related primarily to the digital space instability and vulnerability, which, in turn, have far – reaching consequences for the political and economic systems of entire regions and beyond.

The first chapter of the thesis is devoted to an analytical consideration of the theoretical apparatus of such terminological categories as «cyberterrorism», «cybersecurity», «state's national security». This chapter also emphasizes the necessity to protect information networks from cyberterattacks, and the primary task is to fix the term «cyberterrorism» by decree, moreover, some policy recommendations are given. Firstly, modernization of the existing cyberterrorism definition in Ukrainian legislation is put forward. Secondly, taking into account this phenomenon`s relevance and danger it`s come up with introducing the concept of «cyberterrorism» into the regional governance system. Besides, due to the fragmentarity and lack of a single European terminological apparatus, the author points the way to the importance of «cybersecurity» concept transforming. Thus, it is reviewed the existing research and the results achieved, points out the gaps and discussion points, and formulates a new insight into the «cyberterrorism» as a political concept. To improve the Ukrainian national cybersecurity policy, recommendations are provided in compliance with the clarified definition of «cybersecurity» and, accordingly, the formulation of an alternative approach. Particularly, this includes the introduction of new political concepts such as «cybersocial adaptation» and «cyberimmunity». Innovative approaches to cybersecurity provide comprehensive guarantees of national interests in the digital space. To build the community immunity capable of mitigating the harmful effects

of cyberterrorism, the concept of «cyberimmunity» involves the simultaneous usage of political and social tools. At the same time, «cybersocial adaptation» refers to the cybersecurity sociocultural dimensions, which determines the need for societies to develop and adapt to the challenges of the digital age in the cultural and social areas.

The research also emphasizes the importance of a multidimensional methodology, harmonization of legal approaches and international cooperation within combating cyberterrorism. The major recommendations include the dedicated national cyberpolice units establishing, existing cybersecurity strategies updating, and the introduction of proactive monitoring systems for critical infrastructure. In addition, the study proposes to introduce the position of a «cyberombudsman» whose task is to defend state interests, protect citizens' rights and freedoms in the digital space.

The second chapter is devoted to the analysis of the comprehensive cybersecurity system in the European region countries, which have a high protection level against full range of cyberattacks. The study of the individual countries experience allows us to identify the key issues that should be introduced into the of Ukrainian cyberspace protection system in, which will help counter new cyber threats and implement a number of necessary reforms aimed at strengthening the legal, institutional and strategic political systems.

The author identifies that the current legal framework is fragmented and inefficient, which hinders the formation of a unified national strategy capable of countering sophisticated cyber-terrorist activities. In his study, the author proposes to revise and harmonize outdated legal provisions by integrating cybersecurity principles into a more consistent and comprehensive legislative framework. First of all, the author emphasizes the need to expand Ukraine's national cybersecurity strategy to take into account current challenges in line with updated international standards and geopolitical realities. In order to strengthen its role in coordinating national cyber defense policy, CERT-UA (the government's Computer Emergency Response Team) also needs to be reformed. In such critical areas as healthcare, energy, public administration and electronic communications, we propose a sectoral

approach that involves the creation of specialized subgroups to address cybersecurity issues. This restructuring aims to increase the efficiency and effectiveness of Ukraine's cybersecurity efforts by ensuring a targeted response to sectoral threats and strengthening the overall resilience of the country's digital infrastructure.

In addition, in order to integrate cyberterrorism into its operational mandate, the author emphasizes the importance of transforming the Anti-Terrorist Centre of Ukraine. Currently focused on the physical aspects of terrorism, the Centre should be transformed into a single agency within the response system capable of countering both physical and cyber threats. Such a transformation would not only strengthen Ukraine's internal security, but also enhance its role in shaping international security policy. By leveraging its extensive experience in countering hybrid threats, especially from Russia, Ukraine can make a unique contribution to global cybersecurity efforts. This strategic shift is in line with Ukraine's broader goals, including accession to the European Union and NATO, as both organizations' place cybersecurity high on their agendas.

Relevant reforms are needed to move Ukraine from a defensive position to active participation in global cybersecurity initiatives. By modernising its legal framework, restructuring key institutions, and strengthening the role of integrating countering cyberterrorism into its security strategy, Ukraine can enhance its resilience to digital threats. Such changes will not only strengthen national security, but also position Ukraine as a valuable partner in international efforts to combat cyber threats, thereby supporting its integration into regional and international security structures.

In order to ensure protection in the digital environment and raise public awareness, the author developed the National Cyber Education Program and proved its necessity. The idea of this project emerged against the backdrop of a «staff shortage» due to the war. There was a shortage of employees in the field of cyber defense, as a significant number of people were mobilized into the Armed Forces, and a large number of people were also forced to emigrate. This program is designed

for specialised professions that are necessary to ensure the functioning of critical state facilities, and will have separate plans for training medical professionals, financiers and economists, energy workers, scientists, civil servants and lawyers. Each area will have separate options for training and obtaining the knowledge necessary for the activities of individual specialists. We believe that such a program will provide each professional with the precise knowledge necessary to work most effectively in the digital work environment.

The third section focuses on how Russia's full-scale invasion of Ukraine in 2022 changed the political landscape of Ukraine and created significant security challenges for European states, including the evolution of threats in cyberspace. Ukraine has become the main target of Russian cyberattacks, which have seriously disrupted the operation of public and private institutions, critical infrastructure and national communications systems. These cyber threats not only have direct consequences for Ukraine, but also pose indirect risks to European security, given Ukraine's strategic role as a geopolitical buffer between Russia and Europe.

Thus, attention is primarily focused on the political component of this problem. The specific impact of cyberattacks on Ukraine's critical infrastructure is examined with a particular focus on two key sectors: energy infrastructure and eHealth. The author identifies these sectors as vital to the functioning of the state and particularly vulnerable to cyber threats. By analyzing the challenges in these sectors and their vulnerabilities, the results of the study can contribute to strengthening cybersecurity measures in Ukraine and, as a result, strengthen the overall security architecture in Europe.

In the context of nuclear infrastructure, the study emphasizes the need for advanced protective measures to mitigate the risks of cyberattacks that could have catastrophic consequences. The importance of establishing and enshrining the concept of ‘nuclear cybersecurity’ in the international legal framework, which is of great strategic importance for Ukraine and Europe, is emphasized. The protection of nuclear facilities is presented as a technical and political necessity that requires joint efforts of states, international organizations and the scientific community to

effectively address current security challenges. By analyzing the current state of eHealth cybersecurity in Ukraine and comparing it with the practice in selected European countries, we identify key vulnerabilities and areas for improvement. The importance of implementing international best practices and developing a robust legislative framework to strengthen cybersecurity in the healthcare sector is emphasized.

Overall, the paper identifies the interconnected nature of cybersecurity challenges in critical sectors and points to the need for a coordinated multilateral approach to strengthen Ukraine's resilience against cyber threats. Addressing these challenges will also help contribute to the broader discourse on national and regional security in an increasingly digitalized world.

The paper emphasizes the importance of the interconnectedness of national and regional security in the digital age, and proves the need for a coordinated approach to addressing the multifaceted challenges posed by cyber warfare.

The dissertation study proposes an alternative approach to the definition of the concept of «cyberterrorism». In view of this, the author substantiates the need for existing regulation of European legislation on effective counteraction to acts of cyberterrorism. Based on the lessons learnt in Ukraine, the author emphasizes the importance of establishing European standards for countering cyberterrorism, and also identifies gaps in the current definition of the concept of ‘cybersecurity’ and the need to reform the current Ukrainian and European legislation in order to counter new challenges. The author suggests ways to improve Ukraine's cybersecurity policy, one of which is to create a ‘cyber ombudsman’. The author introduces new socio-political concepts, such as «cybersocial adaptation» and «cyber immunity», which are vital for strengthening cybersecurity. In addition, the study emphasizes the need for unified legal approaches and enhanced international cooperation.

Attention is drawn to the problem of staff shortages caused by war and migration, including the lack of cybersecurity experts. In view of this, the author proposes a specialized cyber education for various professions called the National Cybersecurity Training Program. The text of the thesis emphasizes the need to

reform the institutional structures that guarantee Ukraine's cybersecurity, strengthen coordination in sectors such as healthcare, energy, law enforcement and electronic communications, and discusses in detail the importance of ensuring cybersecurity in the nuclear sector and the eHealth system.

Finally, in order to effectively combat cyberterrorism, we prioritize the need to regulate and improve legislation and international cooperation. The thesis offers recommendations for improving Ukraine's cybersecurity policy, including the creation of new institutions and reform of existing ones. The importance of introducing the concepts of «nuclear cybersecurity» and «eHealth cybersecurity» is emphasized, and detailed proposals for reforming the relevant areas in the proposed order for Ukraine are provided.

Keywords: *active measures, cybersecurity state policy, cyberterrorism, foreign policy, hybrid warfare, mechanisms of regional governance, political adaptation, political institutions, political integration, state sovereignty, world order*.