Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна

Кваліфікаційна наукова
праця на правах рукопису

Зінченко Олександра Ігорівна

УДК 327.57-042.3: [351.86:004.056] (4) (043.5)

ДИСЕРТАЦІЯ
ПРОТИДІЯ КІБЕРТЕРОРИЗМУ ЯК ЗАГРОЗІ СУЧАСНІЙ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ДЕРЖАВ ЄВРОПЕЙСЬКОГО РЕГІОНУ

Спеціальність 052 – Політологія
Галузь знань 05 – Соціальні та поведінкові науки

Подається на здобуття ступеня доктор філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____ Зінченко О.І.

Науковий керівник:
Фісун Олександр Анатолійович, доктор політичних наук, професор

Харків – 2025

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, Україна, 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 «кіберомбудсмена», 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 «кіберомбудсмена». 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

O. Zinchenko « Countering Cyberterrorism as a Threat to the Modern National Security of the States of the European Region». – 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.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Публікації у наукових фахових виданнях України:

1. Зінченко, О. (2024). Політичні проблеми розвитку кібертероризму в міжнародному просторі. *Politicus*, 4, 154 – 160

2. Зінченко, О. (2024). Вплив політичної ситуації в Україні на проблеми кібербезпеки Європейського Регіону. *Politicus*, 5, 154 – 158

3. Зінченко, О. (2024) Європейські регіональні засоби протидії кібертероризму. *Регіональні студії*, 39, 94 – 100

Публікації у науково - періодичних видання України, що увійшли до наукометричних баз даних Scopus та/або Web of Science Core Collection:

4. Parfonova, I. & Zinchenko, O. (2024) Cybersecurity enhancement in the field of eHealth system development in Ukraine. *Medical Perspectives/Medičnì Perspektivi*, 29, 247-256. **(Scopus; Web of Science)**.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

5. Zinchenko, O. (2021) Development of cyberterrorism within COVID – 19. *The 5th International scientific and practical conference «International scientific innovations in human life": Proceedings of V International Scientific and Practical Conference»*, Manchester, 17–19 November 2021. С.682 – 687.

6. Zinchenko, O. (2021). Concepts and types of state's national security. *The 7th International scientific and practical conference «Modern scientific research: achievements, innovations and development prospects»*. December 19-21, 2021. С. 457 – 468.

7. Zinchenko, O. (2022). Cyberattacks as a Tool of Destructive Influence of Cyberterrorism. *International Journal of Science, Technology and Society*, 10(2), 23 – 26.

8. Зінченко, О. (2024). Кібертероризм в енергетичному секторі України та забезпечення кібербезпеки. *Науково-практична конференція «кібербезпека*

енергетики»: *Матеріали науково-практ. конф.,* м. Київ, 29 травня 2024 року. С. 52 – 55.

9. Зінченко, О. (2024). *Забезпечення конституційної складової кіберзахисту в Україні: актуальність та заходи. 28-річчя конституції України: досвід, воєнні випробування та повоєнний ренесанс*, м. Київ, 26 червня 2024 року;

10. Зінченко, О. (2024). Проблеми забезпечення кібербезпеки дистанційної освіти в Україні в умовах війни. *Інтеграція системи освіти України в європейський освітній простір*: *Зб. тез доп. VI Міжнар. науково-практ. конф.,* м. Київ, 25 жовтня 2024 року. С. 172 – 173.

11. Зінченко, О. (2024). Комплексний вплив кібертероризму на інформаційне суспільство. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення* (91): *матеріали Міжнародної наукової інтернет-конференції*, (м. Тернопіль, Україна, м. Ополе, Польща, 10-11 вересня 2024 року. С. 26 – 28.

12. Зінченко, О. (2024). Кібертероризм та проблеми кібербезпеки України в умовах воєнного стану. *Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки: матеріали Всеукраїнської наук.-практ. Конференції.* м. Київ, 27 вересня 2024 року. С. 98 – 100.

13. Зінченко, О. (2024). Кібербезпека як фактор успішної підготовки дисертації в умовах воєнного стану: виклики та рішення для України. *Підготовка дисертацій в умовах воєнного стану: актуальні питання та шляхи їх вирішення*, м. Рівне, 28 вересня 2024 року. С. 62 – 63.

14. Zinchenko, O. (2024). Cyberterrorism: History of Ukraine and current trends. Actual Issues of Modern Science. *Tuculart Edition, European Institute for Innovation Development.European Scientific e-Journal,* 33. 70 – 79.

15. Zinchenko, O.& Parfonova, I. (2024) Countering cyber threats in the context of digital educational technologies in the higher education system of Ukraine. *Academia Polonica*, 6, 230 – 238.

16. Zinchenko, O. (2025). Cybersecurity in international relations: Risks and prospects. *Eximia*, 14(1), 1 – 20.

17. Zinchenko, O. & Parfonova, I. (2025). Implementation of EU eHealth cybersecurity standards in Ukraine. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення : Матеріали науково-практичної інтернет-конференції, Тернопіль, Ополе,* 16–17 January 2025. С. 3 – 5.

18. Зінченко, О. (2025). Кібертероризм як новітній виклик безпеці в умовах глобалізації. *Сучасні суспільні комунікації: міжнародний досвід та українські реалії: Матеріали Міжнародної науково-практичної конференції.* ДЗ «ЛНУ імені Тараса Шевченка». 20 лютого 2025 року. С. 216 – 219.

19. Зінченко, О. (2025). Кібертероризм у російсько-українській війні як новий рівень агресії. *Russia-Ukraine War: Consequences for the World: Proceedings of the 5th International Scientific and Practical Internet Conference*, January 30 – 31, 2025. С. 102 – 104.

20. Зінченко О. Кібертероризм у сучасному політико-економічному вимірі: системний аналіз наслідків та механізмів протидії. Сучасні тенденції розвитку економіки, фінансів, обліку та права : Зб. тез доп. міжнар. науково-практ. конф., м. Ізмаїл, 23 трав. 2025 р. Ізмаїл, 2025. С. 24–25.

ЗМІСТ

ВСТУП

Актуальність теми. Характер сучасних загроз, що з'явилися в кіберпросторі, кардинально змінився внаслідок глобалізації інформаційних процесів, що поставило світову спільноту перед новими викликами, зокрема появою такого виду злочинності, як кібертероризм. Починаючи з кінця XX століття, коли світ вступив до цифрової ери, була здійснена низка відкритих і прихованих кібератак, однак тоді це були суто технічні операції, які переважно мали на меті корисливі мотиви. Утім уже з початку XXI століття звичайна кіберзлочинність перетворилася в «мережевого Левіафана», адже метою кібератак стали державні установи, критична інфраструктура, фінансові установи й навіть системи охорони здоров'я. Це спричинило надзвичайно руйнівні наслідки для мільйонів людей, завдаючи шкоди матеріальному чи інформаційному контенту, а страх і паніка водночас поглиблювали нестабільність.

У реаліях сьогодення, вважаємо, боротьба з кібертероризмом є однією з найважливіших проблем сучасності. Це стосується не лише технологій чи законодавства, а й базових засад, які визначають існування сучасних держав та суспільств. Масштаби кібертероризму зростають надзвичайно швидко. Ураховуючи залежність усіх секторів суспільного життя від інформаційних технологій, яка посилюється, така загроза стає тотальною. Таким чином, необхідність організованих систем протидії новітній загрозі постає передусім як на національному, так і на міжнародному рівнях.

Зважаючи на складний характер ситуації, держави мусять розробити всеохопні національні стратегії в кіберпросторі, які згодом мають бути інтегровані в міжнародні ініціативи. Оскільки явище є транскордонним і таким чином перебуває поза юрисдикцією однієї країни, національні зусилля мають бути доповнені постійними міжурядовими діалогами, які спричинять розроблення та вдосконалення спільної правової бази і єдиних стандартів боротьби з кібертероризмом.

Особливої актуальності набуває проблема забезпечення захищеності та стійкості до кібертерористичних атак об'єктів критичної інфраструктури, яка стає однією з головних цілей кібертерористів. Наслідки кібератак енергосистеми, транспорту чи медичних служб будуть катастрофічними для всього суспільства. Тож можемо стверджувати, що вказана на сьогодні тема є **актуальною**, адже питання щодо протидії кібертероризму потребує комплексного розв'язання, зокрема розроблення нових технологій безпеки, створення спеціальних підрозділів у структурах безпеки та розвиток ефективної міжнародної співпраці.

Мета і завдання дослідження. Відповідно до обраного *об'єкта* дослідження – кібертероризму як деструктивного політичного явища та *предмета* дослідження – протидії кібертероризму як загрозі сучасній національній безпеці держав європейського регіону, *мета* дисертаційної роботи полягає у вивченні виявів кібертероризму на сучасному етапі та визначенні механізмів протидії кібертероризму на регіональному рівні, а також орієнтирів для імплементації досвіду європейських держав Україною.

Для досягнення поставленої мети в роботі визначено такі **завдання**:

– виявити ступінь наукового розроблення цієї теми;

– розглянути підходи до розуміння понять «кібертероризм» та «кібербезпека»;

– сформулювати власні визначення понять «кібертероризм» та «кібербезпека»;

– з'ясувати засоби протидії кібертероризму держав Європи на регіональному рівні, визначити досягнення та недоліки, а також запропонувати власні методи покращення кібербезпеки в зазначеному регіоні;

– проаналізувати нормативно-правові, інституційні та політичні інструменти протидії кібертероризму в державах Європейського регіону;

– згідно з отриманими результатами визначити здобутки держав ЄС та порівняти їх з національними, виробивши рекомендації для покращення сучасного стану кібербезпеки в Україні;

– розглянути деструктивний вплив кібертероризму на критичну інфраструктуру України та інших європейських держав, розробити заходи протистояння та пониження руйнівної дії від такого роду кібератак в умовах війни з РФ та окреслити напрямки подальших досліджень у цій галузі.

Невід'ємним складником наукового дослідження кібертероризму є використання методів, які сприяють логічному аналізу й забезпечують обґрунтованість положень, що дає змогу глибше зрозуміти сутність цього явища та проаналізувати його вплив на сучасну систему безпеки. Під час вивчення цієї теми застосовано бібліографічний метод для оцінки ступеня розробленості проблеми та історичний метод для дослідження цього явища в динаміці. Аксіологічний та ціннісно-нормативний методи сприяли з'ясуванню значення явища кібертероризму для суспільства й держави та виявленню його впливу на найважливіші цінності. Метод нормативно-правового аналізу, а також термінологічний дозволили оперувати базовими та периферійними поняттями й стали неодмінним складником вивчення чинної правової бази європейських держав щодо кібербезпеки. Метод системного аналізу, аналізу і синтезу, а також порівняльний метод уможливили виконання різнобічного дослідження проблеми протидії кібертероризму та забезпечення кібербезпеки в державах європейського регіону, а також вироблення рекомендацій для України з імплементації та впровадження успішного європейського досвіду.

Теоретичну основу дослідження становлять праці таких вчених, як С.О.Гнатюк, Д.В. Дубов, О. Г. Корченко, Є. В. Паціра, С. В. Казмірчук, В. Л. Бурячок, М. А. Погорецький, В.В. Філінович, Д. Денінг, Г. Вайман, Марія Грасіела Паредес Пуенте де ла Вега, Сандей Олюдаре Огунлана, Венкатраман Шрідхаран, Бенджамін Лундстрьом, Б.Коллін, З. Хомбургер, О. Марченко, Ю. Лісовська, В. І. Андрєєв, В. О. Хорошко, В. С. Чередниченко, М. Є. Шелест, О. В. Олійник, О. В. Соснін, Л. Є. Шиманський, Ю. Р. Акчурін, А. В. Возженников, В. М. Фурашев, Є. О. Курій, С. Ф. Гончар, Г. А. Землянка, А. С. Карпенко, Е. А. Мамедова, А. В. Тарасюк, В. Б. Гавриляк, Є. В. Котух, Т. В. Станіславський, Л. А. Арсенович, О. О. Самойленко, Б. В. Бистрова, С. Р. Сунгурова, А. Д.

Младьонова, В. П. Таркін, С. А. Палій, М. В. Копійка, О. В. Фурсай Ю. В. Білявська, Я. І. Шестак, В. О. Голубєв, І. В. Діордіца, О. Г. Широкова-Мурараш та ін.

За всієї важливості наукових досліджень цих учених аналіз їхніх робіт дає змогу стверджувати, що окремі питання залишаються нез'ясованими, зокрема відсутнє єдине легальне визначення поняття «кібертероризм» у більшості країн Європи, не розроблений чіткий механізм протидії кібертероризму на регіональному й національному рівнях.

Наукова новизна полягає в тому, що дослідження є першим цілісним фундаментальним розглядом проблеми кібертероризму в політичному контексті, що ґрунтовно й системно аналізує феномен кібертероризму в політичному вимірі. Запропонована дисертаційна робота є важливим етапом у розвитку вітчизняної політичної науки, адже містить унікальні авторські поняття, концептуальні ідеї та новаторські висновки, які не лише становлять виняткову наукову новизну, а й суттєво змінюють парадигму вивчення кібертероризму, формуючи нові вектори для розвитку політичної науки.

Уперше:

– сформульовано та обґрунтовано визначення дефініції «кібертероризм» – як свідомого використання інформаційно-комунікаційних технологій для здійснення нападів на критичні об'єкти інфраструктури з метою досягнення політичних або ідеологічних цілей, наведення паніки серед населення чи підриву державної стабільності, суспільств і міжнародних структур через маніпуляцію інформаційними потоками, руйнацію цифрових інфраструктур або дестабілізацію стратегічних систем управління;

– розкрито сутність дефініції «кібербезпека», визначено її позитивні аспекти та вади, на основі з'ясованих прогалин сформульовано власне визначення поняття «кібербезпека» – як комплексний стратегічний процес гарантування безпеки національного суверенітету, політичної стабільності, критичної інфраструктури та забезпечення захисту інтересів прав та свобод громадян у кіберпросторі від деструктивного впливу будь-яких внутрішніх та

зовнішніх кіберзагроз із використанням багаторівневих політико-правових технічних та соціальних інструментів;

– розроблено міждисциплінарну методологію вивчення кібертероризму, продемонстровано необхідність гармонізації правових підходів та посилення міжнародного співробітництва у цій галузі. Деякі з рекомендацій передбачають створення національних підрозділів Кіберполіції, оновлення наявних стратегій кібербезпеки та активний моніторинг критичної інфраструктури;

– запропоновано створення посади «кіберомбудсмена» як уповноваженого представника держави, діяльність якого полягатиме в захисті суспільних інтересів, прав та свобод громадян у цифровому просторі;

– запропоновано інноваційні соціально-політичні концепції щодо підвищення рівня кібербезпеки в Україні: «кіберсоціальна адаптація» та формування «кіберімунітету» в суспільстві. Нові підходи до кібербезпеки передбачають інклюзивний захист як громадянських, так і національних інтересів у кіберпросторі. Змістом «кібернетичного імунітету» є застосування політичних і соціальних інструментів одночасно для формування «імунітету суспільства» проти згубних наслідків кібертероризму, «кіберсоціальна адаптація» стосується соціокультурного виміру кібербезпеки;

– сформульовано ідею нового Третього Додаткового Протоколу до Будапештської Конвенції про Кіберзлочинність 2001 року, уключаючи й феномен кібертероризму, його характеристики, криміналізацію та політичний інструментарій протидії («кіберімунітет для критичної інфраструктури», «політичний кіберкарантин», створення нових структур протидії задля забезпечення «політичного механізму кіберпосередництва»);

– як спеціальний механізм запропоновано розроблення нового підходу, спрямованого на вирішення проблеми – «кібертрибуналу» із урахуванням специфіки досліджуваного явища та вимоги сучасної практики для міжнародного суду у справах злочинів у кіберпросторі, а також

обґрунтовано пропозицію щодо розширення повноважень Міжнародного кримінального суду ООН та/або Міжнародного суду ООН у цій галузі;

– сформульовано «модель забезпечення кібербезпеки», яка містить чотири ключові компоненти: інтеграцію, адаптацію до небезпек, інновації, кіберосвіту. У перспективі ця формула може стати орієнтиром для майбутніх стратегій, оновлених політик кібербезпеки та напрямків для створення «щита» в кіберпросторі та формування опору сучасним цифровим викликам в Україні;

– запропоновано «Національну програму кіберосвіти в Україні», яка надасть кожному спеціалістові особливі знання, необхідні для максимальної продуктивності в цифровому робочому середовищі. Програма стосується галузей та професій, необхідних для функціонування життєво важливих державних об’єктів, і передбачає як окремі напрями підготовку медичних працівників, фінансистів та економістів, енергетиків, технічних працівників, юристів і т. ін. Кожен напрямок матиме окремі варіанти перепідготовки та отримання знань для ведення відповідної діяльності;

– висунуто пропозицію щодо новітньої розробки розгалуженої підземної системи управління АЕС із багатьма пунктами керування. Така система зможе здійснювати «повномасштабний» захист ядерних установок у кібернетичному вимірі та знизити ймовірність несанкціонованого вторгнення й певних катастрофічних наслідків. Рекомендовано також покласти регулювання такої діяльності на галузевий центр, створений при запропонованому реформуванні CERT – UA, який має працювати під робочою назвою CERT – NE;

– спираючись на представлену Концепцію, ми розробили термін «ядерна кібербезпека», зазначивши важливість його закріплення в міжнародній системі таким чином: «ядерна кібербезпека — це сукупність технічних, організаційних, правових та процедурних заходів, спрямованих на забезпечення захисту ядерних об’єктів, інформаційних систем та мереж управління від кібернетичних загроз і кібератак, з метою недопущення несанкціонованого втручання, яке може призвести до серйозних аварій, які

можуть нашкодити навколишньому середовищу, життю і здоров'ю людей, а також спричинити порушення міжнародної безпеки»;

– розроблено структуру та зміст поняття «кібербезпека eHealth» – це забезпечення організації своєчасними доступними та якісними медичними послугами під час використання кіберпростору, яке гарантується шляхом виконання особливих вимог, як-от: захищеність життєво важливої інформації та даних пацієнта (історії хвороб, результати аналізів, діагнози та плани лікування), належна робота медичних систем і обладнання, збереження безпеки та безперервності роботи у випадках надзвичайних ситуацій та дотримання правил, які містять необхідні методи захисту від зовнішніх і внутрішніх кіберзагроз;

– представлено «Вектор кіберстійкості eHealth» для України, який подає деталізований опис кожної дії, яку необхідно виконати Україні задля реформування і покращення української практики. Такий вектор розрахований на період 2026 – 2029 рр., що дає можливість у наступному 2030 році, після завершення вказаних дій, вивчити результати відповідної діяльності.

Удосконалено:

– нормативно-правові положення шляхом реформування таких Законів України, Указів та Постанов: «Про основні засади забезпечення кібербезпеки України», «Про національну безпеку України», «Про оборону України», «Про боротьбу з тероризмом», «Про затвердження Правил антитерористичної безпеки», «Про інформацію», «Про доступ до публічної інформації», «Про електронні комунікації», «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю», «Про захист персональних даних», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України», «Про правовий режим воєнного стану», «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», «Про вищу освіту» «Про освіту дорослих», «Про Національну програму

інформатизації», «Про критичну інфраструктуру», «Основи законодавства України про охорону здоров'я».

– положення регіональних документів, що стосуються кібербезпеки, таких, як «Будапештська Конвенція про кіберзлочинність 2001 року», «Боротьба з використанням Інтернету з терористичною метою», через внесення окремих ініціатив про включення поняття «кібертероризм», його опис та характеристику методик протидії йому до вказаних документів;

– функціональну взаємодію інституційних структур через унесення пропозицій щодо реформування CERT–UA у вигляді розмежування повноважень між підструктурами як галузевого розподілу критичної інфраструктури. Розширення компетенцій Антитерористичного Центру України через збільшення зони впливу, посилення фізичного захисту із використання кіберзахисту від терористичних атак. Удосконалення також стосується розроблення засобів протистояння відповідно до нової безпекової політики, яка б відображала новітній вектор, ураховуючи мультирівневість кіберзагроз.

Дістало подальшого розвитку

– у межах наявних підходів дослідження тематики кібертероризму відповідно до сформованих чотирьох етапів: 1960–1970 рр., 1980 – 1990 рр., 1990 – 2010 рр. і сучасний етап (з 2010 р.);

– виділення й порівняння рис кібертероризму та кіберзлочинності, пояснення основних відмінностей;

– учення щодо кібербезпеки, зокрема узагальнення сучасних напрацювань теоретичного забезпечення кібербезпеки. Розроблено концептуальні підходи до забезпечення сучасної кібербезпеки з урахуванням використання політичного інструментарію протидії багаторівневим загрозам у кіберпросторі;

– подальша деталізація типів кібертерористичних атак, які включають кібератаки на критичну інфраструктуру, загрозу суспільному

порядку, застосування соціальних мереж задля деструктивного психологічного впливу та дезінформації.

Практичне значення одержаних результатів. Дисертаційне дослідження може бути використане для вдосконалення національних та регіональних методик протидії кібертероризму. Розроблені положення та пропозиції за їхнього чіткого застосування, на нашу думку, сприятимуть підвищенню ефективності заходів державних органів у сфері забезпечення кібербезпеки у вигляді оптимізації інституційних механізмів, удосконаленні законодавства та впровадженні передових політичних рішень. Додатково отримані результати стануть корисними для міжурядової взаємодії для боротьби з кібертероризмом шляхом інтеграції міжнародних стандартів реагування на кіберзагрози та вдосконалення системи обміну інформацією між державами. Окремі положення роботи можуть бути використані в освітньому процесі та науково-дослідній роботі під час підготовки фахівців у галузі кібербезпеки, політики, міжнародних відносин і національної безпеки, а також у навчальних програмах для підвищення кваліфікації.

Структура та обсяг дисертації. Дисертація складається із анотації українською та англійською мовами, вступу, трьох основних розділів, висновків, списку використаних джерел, додатків. Загальний обсяг роботи складає 271 сторінки, з яких 203 сторінки припадає на основний текст. У дослідженні наявні 4 рисунки та 3 таблиці. Список використаних джерел містить 348 позицій і займає 38 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ КІБЕРТЕРОРИЗМУ

1.1. Підходи до визначення поняття «кібертероризм»

Порівнюючи погляди на головний суб'єкт і об'єкт безпеки в XX та XXI ст., можемо констатувати, що вони докорінно змінилися. Якщо раніше головними об'єктами захисту була територія та суверенітет, а захист від терористичних атак держави здійснювався шляхом створення та утримання силових структур, які вважалися головним гарантом безпеки, то з огляду на діджиталізацію терористичні удари додалися ще й у віртуальному просторі, а згодом з'явилося кардинально нове явище, яке отримало назву «кібертероризм», протистояти якому з року в рік стає все складніше, і запорукою успіху є невпинна модернізація засобів захисту та протидії.

Однак, попри значний розвиток інформаційних технологій, законодавчої сфери, політичних ідей та власне глобалізацію кіберпростору, єдиного й чітко визначеного підходу до трактування поняття «кібертероризм» на сьогодні не існує ні в науковій, ні в практичній сферах.

Тому, на нашу думку, важливим є дослідження еволюції визначення кібертероризму, яке охоплює не лише історичний аналіз змін у розумінні цього феномену, а й концептуальні підходи, які виникли в різні етапи розвитку цифрових технологій. Водночас вважаємо за необхідне розгляд ключових етапів трансформації поняття розпочати від перших теоретичних уявлень про нього у 80-х роках XX століття, коли проблема зламу інформаційних систем тільки починала набувати значення, до сучасних викликів, пов'язаних із використанням новітніх технологій. На сьогодні ж кібертероризм вже не стосується лише атак на інфраструктуру, адже включає різні форми дестабілізації через пропаганду, маніпуляцію інформацією та психологічний вплив на суспільство.

Доцільним також є зосередження уваги на аналізі міжнародних та національних підходів до визначення кібертероризму. Зокрема, висвітлимо підходи до визначення цього поняття, які використовують міжнародні організації, а також окремі держави. Такий аналіз спрямований на досягнення мети щодо створення новітніх механізмів, які б могли бути дієвими у протидії викликам кібертероризму. Особливу увагу звернемо на важливість змін у різного виду нормативно-правових актах, які регулюють суспільну політику в державах і дослідимо наявність розриву між науковими уявленнями та правовими нормами щодо розуміння реальних загроз, які виникають у цифрову епоху. Аналіз проводимо, спираючись на історичні приклади виявлених кібератак, спрямованих на критичну інфраструктуру та геополітичні системи, запропонувавши систематизацію знань про кібертероризм, та ідентифікуємо ключові недоліки наявних підходів до визначення і характеристики явища кібертероризму.

Насамперед наголосимо, що кібертероризм – це поняття, яке з моменту своєї появи залишається неоднозначним як у теоретичному, так і в практичному аспектах. Оскільки відбувся стрімкий розвиток цифрових технологій, терористичні дії отримали змогу розширити простір свого впливу, що суттєво ускладнило виявлення загроз та протидію таким протиправним діям.

На відміну від традиційного тероризму, який виявляється у фізичних атаках та безпосередньому насильстві, кібертероризм використовує такі засоби, як інформаційні системи та технології, що дозволяє йому бути «невловимим». Зважаючи на це, питання протидії кібертероризму в сучасному світі, де цифрова інфраструктура є частиною функціонування економіки, суспільства та держави загалом, є актуальним.

Визначення цього поняття, однак, досі залишається предметом дискусій, а це, на наш погляд, значно ускладнює виробленню шляхів протидії, адже неможливо протистояти явищу, яке належним чином не охарактеризовано. У межах наукових досліджень, у документах міжнародних організацій та державному законодавстві окремих країн запропоновано різні трактування, і це

ускладнює формування єдиної концепції. В одних документах кібертероризм пояснено виключно як атаки на критичну інфраструктуру, що спричиняють значні матеріальні збитки чи загрозу життю людей, в інших документах наголошено, що поняття включає також пропаганду, фінансування терористичних угруповань через інтернет або маніпуляцію інформацією в соціальних мережах із політичними чи ідеологічними цілями.

На нашу думку, відсутність уніфікованого підходу призводить до розриву між науковою теорією і позицією державних політиків. Важливе значення має й те, як на практиці відбувається боротьба з кіберзагрозами. Усе це спричиняє затримки в прийнятті рішень щодо реагування на атаки у кіберпросторі, а також у забезпеченні кібербезпеки держав загалом. Як бачимо, складність визначення кібертероризму пов'язана, насамперед, з його динамічністю.

Так, у 80-х роках XX століття, коли вперше почали використовувати цей термін, основна увага приділялась потенційній загрозі порушення інформаційних систем, але вже наприкінці 90-х років XX століття і на початку XXI із значним поширенням інтернету стало зрозуміло, що кіберпростір може використовуватися не лише для атак на інфраструктуру, а й для пропаганди, психологічного тиску та залякування населення.

Вважається, що події 11 вересня 2001 року [1; 2] стали переломним моментом у розумінні кібертероризму. З того моменту міжнародна спільнота почала активно обговорювати загрози, пов'язані з можливістю терористів використовувати цифрові технології для досягнення своїх цілей. З цим у подальші десятиліття увага вже зосередилася на складніших формах загроз, зокрема кібершпигунстві, використанні угруповань або кібератак, які здатні спричинити військові конфлікти.

Отже, можемо зробити висновок, що історія трансформації розуміння кібертероризму тісно пов'язана з розвитком технологій. Від ранніх теоретичних уявлень про небезпеку зламу систем ми перейшли до реальних кібератак, які змінюють геополітичну реальність. Прикладом можуть слугувати атаки на енергосистеми України у 2015 – 2016 роках [3], які продемонстрували, що

кібертероризм може мати не лише економічні наслідки, але й серйозно впливати на національну політику і від цього на міжнародну безпеку. Попри це, не всі держави готові визнати ці виклики, а спроби уніфікувати міжнародне законодавство, на наш погляд, залишаються обмеженими.

Зазначимо, що особливої уваги заслуговує проблема започаткування саме державного регулювання. Уряди окремих країн, зокрема США, активно впроваджують законодавчі акти, регулюючи протидію кіберзагрозам, однак на сьогодні в своєму законодавстві не дають прямої дефініції поняттю «кібертероризм», наслідком чого є відсутність розуміння різниці між кіберзлочинністю та кібертероризмом на законодавчому рівні.

Цю проблему можемо розглянути на прикладі «Patriot Act» у США від 2001 року. Цей документ визначає кібертероризм як дії, спрямовані на залякування або примушення уряду чи суспільства за допомогою кіберпростору, хоча прямої дефініції кібертероризму не надає [4]. Схожі законодавчі ініціативи також приймаються в Європейському Союзі через нормативно-правові акти, які прямо чи опосередковано стосуються кібербезпеки.

З огляду на це виникає закономірне питання: як в цьому випадку, ураховуючи динамічність появи новітніх загроз та стрімку еволюцію технологій, забезпечити чітке розуміння явища кібертероризму, щоб протидіяти йому. Вважаємо, насамперед потрібно прослідкувати історичну трансформацію поняття. Це є необхідним не лише для кращого розуміння цього явища, а й для виявлення прогалин у поточних підходах до його визначення, адже запорукою успішного контролювання кібертерористичних атак є формування системного підходу до розуміння природи, еволюції та механізмів протидії кібертероризму. Відповіді на ці виклики мають вирішальне значення для безпеки сучасного суспільства.

На сьогодні стан опрацювання проблеми кібертероризму свідчить про її відносно недавнє дослідження, яке активно розвивається у вітчизняній і зарубіжній науковій літературі. Умовно дослідження цієї теми можна поділити

на чотири етапи: 1960–1970 рр. – поява транзисторних обчислювальних систем, які спричинили перші дрібні кіберзлочини; 1980 – 1990 рр. – розробка перших операційних систем, арешти «віртуальних злочинців» і перші випадки створення комп'ютерних вірусів; 1990 – 2010 рр. – активізація кібератак, спрямованих на державні установи, утворення хакерських груп, шпіонські кібероперації; сучасний етап (з 2010 р.), який включає аналіз новітніх технологій, таких, як штучний інтелект і криптовалюти, та їхнє використання у кібертерористичних цілях.

Вагомий внесок у дослідження зробили українські вчені, зокрема, С.О. Гнатюк [5], О.Г. Корченко [6], Д.В. Дубов [7] , Є.В. Паціра [8], В.В.Філінович [9], С.В. Казмірчук [10], В.Л. Бурячок [11], М.А. Погорецький[12] та інші. Їх роботи зосереджені на аналізі українського досвіду протидії кіберзагрозам. Серед зарубіжних дослідників слід відзначити Д. Денінг [13], яка ще в 1990-х роках вивчала потенціал кібератак, Г. Ваймана, який вивчав реальність загрози кібертероризму ще у 2004 році [14].

На сьогодні не існує дисертаційних робіт українських дослідників, які б прямо досліджували указану тему, натомість у працях зарубіжних дослідників проблему кібертероризму розкрито через кілька ключових перспектив. Марія Грасіела Паредес Пуенте де ла Вега [15] та Сандей Олюдаре Огунлана [16] зосереджуються на правових і міжнародних аспектах. Пуенте де ла Вега в своєму дослідженні звертає увагу на виклики для міжнародного гуманітарного права, пов'язані з кібертероризмом. Вона підкреслює необхідність створення єдиного правового визначення кібертероризму та розроблення відповідних правових інструментів для боротьби з ним, акцентуючи на необхідності адаптації правової бази до нових загроз у кіберпросторі. Огунлана, в свою чергу, акцентує на важливості міжнародного співробітництва у протидії кібертероризму, особливо наголошуючи на необхідності обміну інформацією між країнами для виявлення загроз на ранніх етапах. Він акцентує на важливості координації зусиль та гармонізації законодавства між державами для ефективної боротьби з терористичними групами в кіберпросторі.

Венкатраман Шрідхаран [17] та Бенджамін Лундстрьом [18] зосереджують увагу у своїх працях на технічних аспектах кібербезпеки критичної інфраструктури, що також може наражатися на ризики кібертероризму.

Так, Лундстрьом наводить приклади реальних кібератак, які мали значний вплив на національні енергетичні системи. Він демонструє важливість інтеграції нових технологій для покращення безпеки.

Таким чином, дослідження Пуенте де ла Вега та Сандей Олюдаре Огунлана фокусуються на правових і міжнародних аспектах кібертероризму, по-перше, указуючи на необхідність реформування нормативної сфери та посилення міжнародної співпраці. По-друге, Сридхаран і Лундстрьом зосереджуються на технічних аспектах захисту критичної інфраструктури від кіберзагроз, наголошуючи на необхідності вдосконалення технологічних стандартів і засобів захисту. Однак цей аспект не є пріоритетним у нашому дослідженні, але й не може бути втрачений через прямий зв’язок із політичними інструментами протистояння.

У наведених працях фіксуємо значну схожість щодо розуміння різних аспектів кібертероризму. Усі дослідники погоджуються з необхідністю розроблення комплексного підходу до кібербезпеки, який поєднує правові, технічні та міжнародні заходи боротьби з кібертероризмом. Цей підхід має стати основою для забезпечення стійкості суспільства до сучасних загроз у кіберпросторі. Погоджуючись із такою пріоритетністю, вважаємо, що запропоновані нами ідеї зможуть бути не тільки значним поштовхом у протидії кібертероризму в Україні, а й будуть цікавими в європейському контексті.

Незважаючи на значний прогрес, нерозв’язаними залишаються ключові питання: відсутність загального визначення кібертероризму, обґрунтоване пояснення його складників, недостатній історичний аналіз цього явища, недослідженість використання новітніх технологій у кіберзагрозах, розрив між теорією та практикою. Ці проблеми ускладнюють правове регулювання й формування ефективних механізмів запобіганню кіберзагрозам. Саме на

розкриття цих аспектів і спрямоване наше дослідження, яке має на меті систематизувати знання про еволюцію поняття кібертероризму, дослідити зміни у розумінні цього явища з часом та виявити ключові підходи до його трактування в різних країнах.

Результати вивчених наукових праць свідчать про те, що переважно кібертероризм класифікують як специфічну форму тероризму. Однак, на нашу думку, є й різниця у тлумаченнях цих понять. Так, кібертероризм для досягнення цілей використовує інформаційні технології, а виник він унаслідок еволюційного розвитку тероризму в контексті цифрової ери.

Самостійно ж термін «кібертероризм», як ми вже зазначили, почав з'являтися в науковому обігу в середині 80-х років XX століття, коли швидкий розвиток комп'ютерних технологій та глобальних мереж поставив перед державами й суспільствами нові виклики в галузі безпеки. Першим, хто звернув увагу на можливість поєднання тероризму з інформаційними технологіями, був Б. Коллін, старший науковий співробітник Інституту безпеки та розвідки США. Він запропонував визначення кібертероризму як застосування комп'ютерних технологій і мереж для здійснення терористичних атак з метою завдання шкоди державам, організаціям або окремим особам, а ще й для поширення страху й паніки серед населення [19]. На думку американського вченого, кібертероризм є етапом еволюції традиційного тероризму, спричиненого бурхливим розвитком технологій і появою нових можливостей для здійснення насильства та маніпуляцій через віртуальний простір. Як бачимо, історично етапи становлення кібертероризму безпосередньо пов'язані з розвитком інформаційних технологій, тобто ці два процеси є взаємопов'язаними. На основі аналізу наукової літератури можемо стверджувати, що виокремлені періоди розвитку кібертероризму є доцільними, що певною мірою спрощує подальше вивчення цієї проблеми.

Отже, перший етап – це 1960 –1970 рр. – поява обчислювальних систем і первинні спроби несанкціонованого доступу до комп'ютерних мереж. У цей період розпочинається розвиток комп'ютерних систем, але самі атаки мають

поодинокий характер. Здебільшого їх здійснюють окремі хакери, які маніпулювали даними або викрадали інформацію з наукових і військових баз.

Наступний етап, з огляду на наш аналіз, починається з 1980 р., власне з першою появою самого терміна «кібертероризм». На той час кіберзагрози мали відносно обмежений характер, здебільшого вони полягали в хакерських атаках на окремі інформаційні системи або в зараженні комп'ютерів вірусами. Перші спроби об'єднати тероризм з цифровими технологіями були пов'язані з використанням комп'ютерних мереж для атаки на державні установи або великі корпорації для перехоплення або маніпулювання інформацією. Такі дії могли бути виконані як приватними особами, так і групами з ідеологічних або політичних мотивів.

Одним із перших історичних прикладів, що стосується вказаного часового проміжку, був випадок у 1989 році, коли група хакерів створила вірус, що мав на меті вплинути на електронні системи фінансових установ. Цей випадок не став надто відомим, проте став важливим сигналом для розуміння потенційної загрози від використання інформаційних технологій у цілях маніпулювання та дестабілізації [20].

Третій етап розвитку кібертероризму настає в 90-х роках XX століття і пов'язаний із значним розвитком інтернету та комп'ютерних мереж, адже рівень та складність кіберзагроз значно зростають. Тепер кібертероризм уже охоплює не лише прямі атаки на окремі системи, а й спроби дестабілізувати державні структури, зокрема через атаки на критичну інфраструктуру. Далі з'являються перші спроби впровадження цифрових технологій для здійснення пропаганди, психологічного тиску та створення паніки серед населення [21].

У перші десятиліття XXI століття, з розвитком технологій, розуміння кібертероризму суттєво змінилося. Кібертероризм більше не обмежувався лише атаками на окремі інформаційні системи або фінансові установи. Загрози стали складнішими, а методи – різноманітнішими.

Нарешті, етап сьогодення, або четвертий етап, який стартує від початку 2000-х років. Для цього часу характерне значне зростання кількості й масштабів

кібератак, багато з яких спрямовані на державні установи та критичну інфраструктуру.

Прикладом є 2007 рік, коли сталася одна з наймасштабніших атак на інфраструктуру Естонії. Слід відмітити, на сьогодні існує гіпотеза, що ці події зробило Естонію «піонером» у розвитку системи кібербезпеки. Тоді серія атак була використана для того, щоб паралізувати урядові сайти країни. Вважаємо, це був не просто перший вияв кібертероризму, як сьогодні часто стверджують, а «кібергібридна війна», оскільки кібертероризм використовувався для дестабілізації політичної ситуації в державі. Ця атака була пов'язана з політичним конфліктом між Росією та Естонією і засвідчує використання кібертероризму як інструменту для досягнення політичних цілей [22].

Ще одним показовим прикладом є атака на українську енергетичну систему в 2015 році, коли внаслідок кібератаки було паралізовано роботу декількох енергетичних компаній, що призвело до масових відключень електроенергії [23]. Цей приклад демонструє, що кібертероризм може бути використаний як інструмент гібридної війни для впливу на державні структури й забезпечення контролю над критично важливими секторами економіки.

Окрім вищенаведеного, можемо помітити, що в останні роки кібертероризм став важливим елементом глобальних інформаційних воєн, де різні країни використовують цифрові платформи для пропаганди, маніпуляції громадською думкою, а також для дискредитації політичного уряду окремої держави. Така стратегія, на нашу думку, не просто спричиняє економічні збитки, а може призводити до ескалації міжнародної напруги, створюючи нові ризики для безпеки на глобальному рівні.

Як бачимо, згідно з нашим аналізом, з розвитком інформаційних технологій змінювалося й розуміння кібертероризму: від первісних уявлень про окремі хакерські атаки й вірусні компанії, які виникли на межі 80-х і 90-х років XX століття, до сучасних складних форм, зокрема й кібернапади на критичну інфраструктуру й участь в інформаційних війнах. Кібертероризм перетворився на серйозну загрозу як для безпеки окремих громадян, так і для національної й

регіональної безпекових систем. Сучасні технології та політичні конфлікти дають можливість кібертероризму не лише дестабілізувати держави, а й створювати глобальні кризові ситуації через маніпулювання інформацією та атаки на критичні об’єкти інфраструктури.

Визначення кібертероризму залишається однією з найбільш дискусійних тем у наукових колах, оскільки на сьогодні немає єдиного підходу до його формулювання. Крім того, зважаючи на складну природу цього поняття, існує певна кількість його трактувань. Проаналізувавши дослідження, у яких подано визначення кібертероризму, уважаємо за потрібне виділити кілька.

Одним з основних елементів, на основі якого потрібно кваліфікувати кібертероризм, є об’єкт атаки. Здебільшого такого роду атаки спрямовані на інформаційні системи, комп’ютерні мережі, критичну інфраструктуру, що забезпечує функціонування економічних і соціальних аспектів сучасного суспільства. У своїх роботах дослідники, за нашими спостереженнями, звертають увагу на мету кібертероризму, якою є порушення нормальної роботи інформаційних і комунікаційних систем.

Важливо, однак, ураховувати, що основною метою кібертерористичних актів є не лише злам інформаційних систем, а й психологічний вплив на населення. Згідно з розумінням деяких дослідників такі атаки часто спрямовані на залякування громадян або ж на створення атмосфери страху й хаосу, а це в свою чергу, може призводити до соціальної дестабілізації або навіть політичних заворушень. Наприклад, атака на критичні інфраструктури, такі, як електричні мережі або системи водопостачання, може спричинити паніку серед населення і підштовхнути до політичної кризи.

Як елемент психологічного терору досліджує концепцію кібертероризму, яка поєднує кіберзлочинність із терористичними цілями, Чарвата [24]. Ми підтримуємо думку автора, що терористичні організації використовують Інтернет для вербування, радикалізації, пропаганди, збору коштів та управління. Інтернет дає їм значні переваги завдяки легкості використання, широкому охопленню та зростаючій залежності суспільств від електронних

платформ. Веб-сайти дозволяють терористам без обмежень поширювати свої меседжі, створюючи ілюзію легітимності. До 2007 року існувало понад 5500 таких сайтів. Крім того, Інтернет відкриває можливості для дезінформації, як це показав випадок з фальшивим веб-сайтом, який маніпулював інформацією для політичних цілей.

Зазначимо, що методи, які застосовують у кібертероризмі, відрізняються від традиційних терористичних атак, оскільки вони вимагають високої технічної підготовки й доступу до сучасних технологій.

До ключових методів належать:

– кібертерористичні атаки – дії, спрямовані на злам або перехоплення даних з інформаційних систем держави;

– вторгнення в мережі – атаки, які мають на меті отримати несанкціонований доступ до конфіденційної інформації або пошкодити мережеві системи;

– створення шкідливих програм – віруси та інші програмні засоби, що використовують для знищення або викрадення інформації [25].

Названі та інші методи активно розглядаються науковцями в дослідженнях. Одним зі значних внесків у вивчення методів кібертероризму став аналіз, проведений Р. А. Кларком, колишнім координатором боротьби з тероризмом в уряді США. У своїй роботі «Cyber war: The next threat to national security and what to do about it» у 2012 році [26] він детально описує, які методи можуть бути використані для знищення критичної інфраструктури, і зазначає, що це є характерною рисою кібертерористичних актів.

Унаслідок аналізу ми виявили існування різних підходів до визначення кібертероризму, що підтверджують й інші дослідження. Зокрема, у роботі Діордіци [27] та співавторів зазначено, що проблема відсутності єдиного міжнародного-правового регулювання кібертероризму, ускладнює ефективну боротьбу з цією загрозою через застосування країнами різних підходів до визначення цього явища, що, безперечно, має вплив на координацію дій на міжнародному рівні. Такий результат підтверджує переконливість зроблених

нами гіпотез та тверджень щодо необхідності всебічного дослідження вказаного поняття та активне впровадження методик протидії йому.

Аналіз наукової літератури уможливлює виділення кількох ключових рис, які характеризують кібертероризм як одне з найнебезпечніших явищ сучасності. Це особливості, які відрізняють його від традиційного тероризму, дозволяють оцінити масштаби загроз і розробити стратегії реагування.

Однією з основних рис кібертероризму є його технологічна природа. Наукові дослідження неодноразово звертають увагу на цей аспект. Так, у роботах дослідника Д. А. Льюїса у книзі «Rethinking Cybersecurity: Strategy, Mass Effect, and States» наголошено на тому, що без доступу до сучасних технологій, кібертерористичні атаки стають неможливими. Льюїс зазначає, що новітні комп'ютерні технології дозволяють здійснювати атаки із застосуванням високоточних інструментів, що може призводити до глобальних наслідків [28].

Наступною рисою є його транстериторіальність, тобто кібертерористи можуть розпочати наступальні дії з будь-якої частини Земної кулі. Це значним чином ускладнює їхнє виявлення та нейтралізацію.

Із цього випливає ще одна особливість – анонімність. Віртуальний простір дає змогу терористам приховувати свою ідентичність, використовуючи псевдоніми або такі інструменти, як VPN, чи, наприклад, анонімні браузери тощо. Це ускладнює встановлення особи тих, хто здійснює терористичний акт, і, відповідно, їх подальше переслідування. Питання анонімності в кіберпросторі детально розглядає у своїх дослідженнях Шмідт. Можливість анонімно здійснювати атаки, зауважує вчений, є серйозною проблемою для державних органів, оскільки відсутність фізичних слідів у кіберпросторі, ускладнює виявлення організаторів атак [29].

Нарешті, ключовою рисою кібертероризму є його здатність до масштабного впливу. Навіть одна локальна атака може мати глобальні наслідки через здатність впливати на інформаційну інфраструктуру, яка забезпечує роботу всіх інших критичних галузей, таких, як енергетика, охорона здоров'я, урядові служби тощо.

На сьогодні спостерігаємо спроби міжнародної спільноти розробити нормативно-правові акти для регулювання будь-яких видів кіберзлочинності. Одним із перших міжнародних документів стала Конвенція Ради Європи про кіберзлочинність [30]. Конвенція підписана 63 країнами, уключаючи Україну, та ратифікована більшістю з них. Цей документ містить положення щодо комп'ютерних злочинів, однак він не дає чіткого визначення кібертероризму і жодним чином не описує його. Вважаємо, було б слушним уключити термін «кібертероризм» до цієї Конвенції, особливо враховуючи серйозність наслідків його виявів у вигляді порушення суспільного порядку, основ конституційного складу, дестабілізації держав. З огляду на це, зауважимо, що кібертероризм не може бути ототожнений із рядовими кіберзлочинами, пов'язаними з навмисним утручанням в інформаційні системи, адже його масштаб і наслідки є значно серйознішими.

У світлі зазначеного проаналізуймо визначення поняття «кібертероризму» щодо його змісту та ознак у різних країнах (США, Франції, Великобританії та Німеччині) з метою виявлення спільних рис і розбіжностей, що впливають на ефективність міжнародної співпраці у протидії цьому явищу. Вибір цих країн зумовлений їхнім лідерством у сфері інформаційних технологій і кібербезпеки. Такий аналіз дозволить не лише глибше зрозуміти специфіку підходів до регулювання кібертероризму, але й сприятиме визначенню напрямів гармонізації законодавства, необхідних для посилення глобальної кібербезпеки.

Так, зокрема, США, як «інноваційний лідер», активно протистоять кіберзагрозам, що робить їхній досвід важливим для розуміння глобальних тенденцій. Наголосимо, що американська політика щодо кіберпростору має значний вплив на країни Європи. Це робить вивчення її досвіду актуальним для нашого дослідження. США активно працюють над удосконаленням законодавчої бази, підвищенням стандартів захисту прав та інтересів громадян і тим самим над створенням ефективних механізмів протидії кіберзлочинності.

Водночас у США переважає концепція саморегулювання Інтернету, тому спеціальне законодавство в цій сфері обмежене [31,32].

Франція після численних терористичних атак – одна з перших країн, яка впровадила Національну стратегію кібербезпеки для створення ефективної інфраструктури боротьби з кібертероризмом. Однак у Франції, як і в більшості країн, відсутня пряма дефініція кібертероризму. Тим часом вона опосередковано базується на широкому розумінні тероризму, яке включає не тільки фізичні акти насильства, але й кібернетичні, пов'язані з використанням технологій у терористичних цілях. Відповідно до французького Кримінального кодексу [33] акти, які використовують інформаційні системи для паніки або ураження критичної інфраструктури, можуть бути класифіковані як терористичні.

Німеччина також не регулює кібертероризм як такий. Утім є підстави посилатися на прямий зв'язок із цим явищем у межах боротьби з кіберзлочинністю і тероризмом через систему Законів про захист критичної інфраструктури [34]. Аналізуючи німецьке законодавство, доходимо до розуміння, що кібертероризм – це спроба здійснити атаку на критичні системи з метою загрози життєво важливим процесам у державі чи суспільстві. Німецький регламент спрямований на посилення кібербезпеки та накладення суворих санкцій на тих, хто намагався зламати захищені інформаційні системи з терористичними намірами.

У Великій Британії визначення кібертероризму обмежено Законом про тероризм (2000 р.) та його доповненнями. Тут кібертероризм можна вважати актом, за якого використання технологій для створення або загрози насильства має серйозні наслідки для національної безпеки. Тому можемо стверджувати, що конкретного визначення кібертероризму в британському законодавстві немає. Термін швидше є складовою частиною більш загального визначення тероризму [35].

Доцільно звернути увагу, що на сьогодні Україна є єдиною європейською державою, яка законодавчо закріпила термін «кібертероризм» у Законі «Про

основні засади забезпечення кібербезпеки України» від 05.10.2017, визначивши його таким чином: «кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням» [36]. У новій Стратегії кібербезпеки України від 2021 року [37] підкреслено, що кібертероризм є серйозною загрозою національній кібербезпеці України. Визначено перелік основних цілей кібертероризму на критичну інфраструктуру, як-от: атомна енергетика, транспорт та фінансовий сектор. З метою протидії кібертероризму у Стратегії передбачено створення загальнодержавної системи виявлення та реагування на кіберзагрози, що включає покращення нормативно-правової бази, упровадження аналітичних інструментів та забезпечення криміналістичної підтримки. Зважаючи на зазначене, кібертероризм у Стратегії визначений як ключова загроза, що вимагає скоординованих дій та розвитку інституційних можливостей для ефективного запобігання та нейтралізації. Додатково у 2024 році Кабінет Міністрів України затвердив Постанову «Про затвердження Правил антитерористичної безпеки» [38], де відображено системний підхід до забезпечення захисту об'єктів критичної інфраструктури, зокрема в аспекті кібертероризму. У Правилах закцентовано на необхідності протидії як фізичним, так і кібернетичним загрозам, що випливає з актуалізації глобальних ризиків, пов'язаних із зростанням кіберзлочинності. Ми вважаємо такий крок досить значущим, адже включення кібертероризму до загальних заходів антитерористичної безпеки свідчить про усвідомлення необхідності адаптації законодавства до нових викликів, спричинених цифровими технологіями, а також про інтеграцію міжнародних стандартів і підходів до національної політики безпеки України. Водночас залишається потреба в удосконаленні практичної реалізації цих заходів та покращенні взаємодії між державними органами, органами місцевого самоврядування та приватними суб’єктами для підвищення ефективності протидії кібертерористичним загрозам.

У результаті проведеного дослідження ми можемо зазначити, що, попри наявність законодавчих ініціатив у різних країнах, проблема визначення

кібертероризму залишається відкритою, адже потребує удосконалення кілька ключових аспектів:

– технічний, бо кібертероризм швидко змінюється разом з розвитком технологій, а тому державам необхідно постійно оновлювати методики протидії, які б ураховували стрімкий розвиток загроз;

– політичний, оскільки визначення кібертероризму може бути використане для політичного контролю, що викликає побоювання щодо порушення прав та свобод людини;

– правовий, адже багато держав не дають чіткого визначення кібертероризму, що створює труднощі для співпраці між країнами та ефективної боротьби з цим видом злочину.

На підставі вищевказаного констатуємо, що кібертероризм як складна й багатоаспектна проблема залишається темою для активних наукових і правових дискусій як на національному, так і на міжнародному рівнях. На сьогодні існують кілька концептів цієї теми, які ще не отримали повного розкриття або аналізу.

Незважаючи на те що термін опосередковано використовується у багатьох наукових працях та законодавчих ініціативах, чітке визначення кібертероризму, як ми зауважували вище, досі відсутнє. Як ми розуміємо, проблема полягає ще й у тому, що на міжнародному рівні існує кілька різних трактувань цього явища, а це заважає сформувати спільний правовий підхід.

Особливої уваги потребує питання захисту прав людини в контексті боротьби з кібертероризмом. Законодавство багатьох країн спрямоване на посилення контролю в цифровому середовищі для боротьби з кіберзлочинністю, однак це часто суперечить основним правам громадян, як наприклад, праву на приватність і свободу вираження поглядів. Збалансувати безпеку та захист прав людини в умовах стрімкої цифровізації є складним завданням, яке потребує ретельного аналізу. І тут важливим є розв’язання деяких проблем, з якими доводиться стикатися в процесі такого аналізу:

1. Відсутність уніфікованого визначення кібертероризму. Однією з ключових проблем є брак єдиного визначення кібертероризму на регіональному та міжнародному рівнях. Попри численні зусилля окремих країн і міжнародних організацій, досі не було розроблено узгодженого підходу до розуміння кібертероризму. Це призводить до труднощів у правовому регулюванні й координації міжнародних заходів протидії кібертероризму. Різні держави надають різні дефініції цього терміна, що ускладнює формування єдиних стандартів реагування. Тут є сенс узяти до уваги практику України у формуванні визначення «кібертероризму» та відповідної нормативно-правової бази щодо протидії цьому явищу через значний досвід у протистоянні. Незважаючи на недостатність врахування різних аспектів, Україна демонструє важливість і необхідність такого кроку.

Пропонуємо таке визначення кібертероризму, що значною б мірою усунуло прогалини в кваліфікації указаного явища, допомогло б уникнути дискусійних моментів щодо його розуміння: «кібертероризм – це свідоме використання інформаційно-комунікаційних технологій для здійснення нападів на критичні об’єкти інфраструктури з метою досягнення політичних або ідеологічних цілей, створення паніки серед населення чи підриву державної стабільності, суспільств і міжнародних структур через маніпуляцію інформаційними потоками, руйнацію цифрової інфраструктури або дестабілізацію стратегічних систем управління».

2. Нечітка межа між кіберзлочинністю та кібертероризмом. Ми вважаємо це значною законодавчою та політичною прогалинами, що ускладнює розроблення адекватних заходів і політик для боротьби з різними видами кіберзагроз. Кібертероризм як специфічну форму терористичної активності нерідко плутають із загальними кіберзлочинами, які мають інші цілі. Щоб усунути проблему нечіткої межі між кіберзлочинністю та кібертероризмом, ми вважаємо необхідним установити конкретні критерії для розмежування цих явищ.

Для реалізації цієї ідеї, по-перше, пропонуємо розробити чіткі правові дефініції кіберзлочинності та кібертероризму, що базуватимуться на ключових характеристиках, які їх відрізнятимуть. Кіберзлочинність зазвичай орієнтована на особисту вигоду, фінансові злочини або пошкодження інформаційних систем, у той час як кібертероризм має політичну, соціальну або ідеологічну мотивацію і спрямований на створення загрози національній безпеці, залякування населення чи підрив стабільності держави. Таким чином, головною відмінністю кібертероризму є його мотив і характер дій. По-друге, пропонуємо включити в законодавчі акти та міжнародні угоди спеціальні положення, які б дозволили класифікувати атаки на критичну інфраструктуру або інформаційні системи як кібертероризм. Завдяки цьому вдасться уникнути неправильної кваліфікації таких дій як звичайних кіберзлочинів і гарантувати належний рівень відповідальності для виконавців.

По-третє, необхідно вдосконалити методологію збору доказів і криміналістичних експертиз у випадках кібератак. Важливо, щоб правоохоронні органи мали чіткі інструкції щодо критеріїв розмежування кіберзлочинності і кібертероризму під час розслідувань. Особливу увагу слід приділити ідентифікації мотивів злочинців: якщо їхня діяльність спрямована на дестабілізацію суспільства чи викликання страху, така діяльність має розглядатися саме як кібертероризм.

Варто також звернути увагу на потребу забезпечення чіткої класифікації кібертероризму на міжнародному рівні, аби держави могли узгоджено діяти проти кібертерористів. Тож маємо підстави стверджувати, що такі кроки сприятимуть формуванню єдиної системи реагування та співпраці між країнами для нейтралізації кібертерористичних загроз, що є вкрай важливим у контексті їхнього транскордонного характеру. Таким чином, запровадження чітких критеріїв і створення узгодженої міжнародної правової бази дозволить установити основні відмінності між кіберзлочинністю та кібертероризмом і цим самим забезпечити ефективне протистояння цим загрозам у глобальному масштабі.

Недосконала правова база на сьогодні демонструє те, що регулювання кібертероризму залишається неповним і недостатньо узгодженим. Більшість держав не мають спеціальних правових норм, які б безпосередньо регулювали питання кібертероризму. Наявні законодавчі ініціативи зосереджуються на більш загальних питаннях кіберзлочинності, через це кібертероризм як окремий об'єкт правового регулювання не виділяється, що призводить до прогалин у боротьбі з ним.

3. Недостатність механізмів міжнародної співпраці є значною перешкодою у протидії кібертероризму. Наявні міжнародні угоди, зокрема Будапештська конвенція, мають обмежене застосування в частині кібертероризму. Це ускладнює координацію зусиль між державами особливо тоді, коли йдеться про транснаціональні кібертерористичні загрози.

4. Обмежене використання новітніх технологій, яке призводить до того, що використання кібертерористами новітніх технологій значно випереджає адаптацію захисту. Відсутність чіткої регуляторної та практичної технологічної бази у контексті протидії кібертероризму створює можливості для неконтрольованого використання цих інструментів у терористичних цілях.

5. Складність ідентифікації акторів кібертероризму, яка викликана транстериторіальним характером, а також можливістю забезпечення анонімності в кіберпросторі, робить виявлення виконавців таких кібератак майже неможливим, що є вагомим викликом для правоохоронних органів через унеможливлення ефективного притягнення їх до відповідальності.

6. Етичні та правові дилеми, які полягають у тому, що боротьба з кібертероризмом ставить держави перед необхідністю використовувати інструменти масового нагляду та обмеження приватності, що, своєю чергою, створює значні етичні і правові питання. Збалансування потреб національної безпеки із захистом прав людини є складним завданням, яке досі не отримало задовільного вирішення.

7. Проблема визначення мотивів та цілей кібертероризму – одна з найбільш серйозних прогалин, на наш погляд. На відміну від традиційного

тероризму, де мотиви та цілі є більш зрозумілими, кібертероризм може включати різноманітні мотиви, а саме: політичні, економічні, соціальні чи психологічні. Така різнобічність ускладнює не лише кваліфікацію, а й визначення ефективних механізмів протидії.

Отже, значні прогалини в розумінні кібертероризму потребують розроблення більш узгоджених і системних підходів, що охоплюють широке політико-правове поле. Лише гармонізація законодавчих і міжнародних ініціатив, посилення співпраці між державами та адаптація правових норм до сучасних технологічних реалій здатні забезпечити ефективну боротьбу з цією загрозою.

З огляду на це, перспективи подальших досліджень полягають у створенні більш ефективних інструментів для міжнародної співпраці та координації, розробці кращих стратегій реагування на кібертероризм і забезпеченні прав людини в цифровому середовищі. Проте, як вже було відзначено, для цього необхідно поєднати правові, політичні, технічні та етичні аспекти, що забезпечить не тільки ефективну боротьбу з кібертероризмом, але й захист основних прав громадян у глобальному кіберпросторі.

1.2. Проблеми тлумачення «кібербезпеки» у протидії кібертероризму та рекомендації щодо його вдосконалення

Із розвитком сучасних технологій питання кібербезпеки стають більш актуальними, оскільки кількість і масштаб різноманітних загроз зростає і ці проблеми мають глобальний вплив. Через те що кібербезпека держави – це частина її національної безпеки, вона є важливим атрибутом внутрішньої та міжнародної політики. Тому проблеми кібербезпеки у працях науковців продовжують викликати великий інтерес. Через це необхідним є акцентування уваги на сутності самого визначення та ідеї «державної національної безпеки», яка пояснюється через численні визначення її сутності. Важливо визнати, що розуміння поняття національної безпеки є похідним від історичної та

політичної еволюції держав, характеру їхніх політичних систем, специфіки міжнародної ситуації в той чи інший історичний період, цілей зовнішньої та внутрішньої політики тощо.

Сьогодні ідея національної безпеки виражається різними способами і характеризується різноманітністю визначень. Наше дослідження ґрунтується на визначенні, поданому в українському законодавстві. Тож «національна безпека України» [39] – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Вважаємо, що в межах нашого дослідження саме це визначення є влучним, адже виражає політичний аспект вразливості до кібертерористичних атак.

Досліджуючи погляди вчених на термін «кібербезпека», зауважимо, що останнім часом ним послуговуються все частіше. Проаналізуймо деякі визначення цієї категорії. Варто наголосити, що серед учених (як і у випадку з терміном «кібертероризм») немає одностайності в потрактуванні терміна «кібербезпека» і немає єдиного визначення на законодавчому рівні.

Учені, зокрема З. Хомбургер [40], зазначає, що кібербезпека повинна включати стратегії для боротьби з таким видом тероризму для зменшення ризиків, пов’язаних із використанням нових інформаційних та комп’ютерних технологій у таких актах насильства.

Як стан системи, де нейтралізуються загрози доступності, цілісності або конфіденційності даних, розглядає кібербезпеку, наприклад, О.Марченко [41]. Таке визначення, хоча й має певну раціональність, є надто загальним і не враховує специфіки об’єктів захисту чи необхідності адаптації до змінюваного середовища кіберзагроз. Це створює проблему як для практичної реалізації заходів, так і для формування єдиної концептуальної бази.

Інші автори, наприклад Ю. Лісовська [42, с.55], трактують кібербезпеку в контексті інформаційної безпеки, пов’язуючи її з використанням комп’ютерних систем та телекомунікаційних мереж. Це, зі свого боку, звужує сферу

кібербезпеки, нехтуючи її стратегічними, соціальними та економічними аспектами, що є критичними в сучасних умовах глобальної інтеграції.

Такі вітчизняні дослідники, як В. І. Андрєєв, В. О. Хорошко, В. С. Чередниченко, М. Є. Шелест, кібербезпеку розуміють як захищеність інформації та інфраструктури, яка її підтримує від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації та інфраструктури, що підтримує [43].

Зміст терміна кібербезпека, як зазначають О. В. Олійник, О. В. Соснін, Л. Є. Шиманський [44], створюється крізь призму загроз, тобто як комплекс системних превентивних заходів, що забезпечують захист життєво важливих інтересів особи, суспільства та країни від негативної інформації про економіку, політику (внутрішню та зовнішню), науку й техніку. Крім того, важливо також ураховувати самостійний і незалежний розвиток соціально-культурної та оборонної сфери, державного адміністративного устрою, елементів державного інформаційного простору, а також забезпечення інформаційного суверенітету України, захисту інформації й маніпулювання дезінформацією та її вплив на свідомість, підсвідомість і психіку кожної особистості та суспільства в цілому, здатність нації нейтралізувати або пом'якшувати наслідки внутрішніх і зовнішніх інформаційних загроз. Однією з ключових ідей, якій присвячені дисертаційні дослідження, є захищеність об'єктів критичної інфраструктури. Так, прикладом слугує робота Є.О.Курій [45], який розробив методологію підвищення захищеності критичних об'єктів за рахунок перехресного впровадження стандартів аудиту з кібербезпеки.

Такий підхід, на нашу думку, акцентує увагу на посиленні інтеграції різних стандартів з метою підвищення надійності та безпеки інфраструктури. А. В. Давидюк [46] у своїй роботі так само фокусує на методах і засобах підвищення рівня кібербезпеки об'єктів критичної інфраструктури, що є важливим для зменшення ризиків потенційних атак. С.Ф. Гончар [47] зосередився на розробленні методології оцінювання ризиків кібербезпеки

інформаційних систем критичної інфраструктури, що дозволяє ефективно виявляти й усувати вразливості, тим самим підвищуючи стійкість цих систем до кібератак.

Кібербезпека спеціалізованих систем є темою дисертації Г.А.Землянка [48], який досліджував методи та засоби забезпечення кібербезпеки багатофункційних флотів безпілотних апаратів в умовах комбінованих кібератак. Ця робота є важливою у світлі зростаючого використання безпілотних технологій у цивільному та військовому секторах. А. С. Карпенко [49] у своїй роботі розглянув забезпечення кібербезпеки глобально розподілених реплікованих систем зберігання даними з

контрольованою узгодженістю. Це дослідження спрямоване на захист розподілених систем зберігання даних, які використовують у сучасних хмарних сервісах, забезпечуючи при цьому їх узгодженість і надійність.

Окремо варто звернути увагу на аналіз нормативних аспектів. Так, адміністративно-правові аспекти кібербезпеки розглянуті, зокрема, у роботі Е.А. Мамедової [50], яка аналізує адміністративно-правові засади забезпечення кібербезпеки патрульної поліції в Україні. На нашу думку, це дослідження підкреслює важливість упровадження сучасних підходів до забезпечення безпеки в правоохоронних органах, ураховуючи цифрові загрози, що зростають. Л.Ю. Веселова [51] розглядає адміністративно-правове забезпечення кібербезпеки в умовах гібридної війни, що є надзвичайно актуальним для України в сучасних умовах. Крім того, А.В. Тарасюк [52] зосереджується на теоретико-правових основах забезпечення кібербезпеки України, пропонуючи загальний огляд законодавчих аспектів, які регулюють цю сферу.

У кількох роботах увагу приділено питанням кібербезпеки в державному управлінні. Так, наприклад, В.Б. Гавриляк [53] вивчав державні механізми провадження кібербезпеки в Україні, аналізуючи наявні засоби та їх ефективність на державному рівні. Є.В. Котух [54] розглядав теоретико-методологічні засади дотримання кібербезпеки в публічному секторі, що є

необхідним для впровадження системних підходів до управління кібербезпекою в державних установах. Т.В. Станіславський [55] аналізував забезпечення кібербезпеки в Україні через призму сучасних механізмів публічного управління, зосереджуючись на необхідності координації дій між різними державними інституціями.

На особливу увагу заслуговують дослідження, присвячені підготовці фахівців із кібербезпеки. Л.А. Арсенович [56] аналізував механізми формування та забезпечення функціонування системи підготовки фахівців із кібербезпеки органів державної влади. Автор підкреслює значення професійної підготовки кадрів для забезпечення ефективного управління кібербезпекою. О.О. Самойленко [57] у своїй дисертації розглядав теорію і методику підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища, пропонуючи інноваційні підходи до навчання в цій галузі. у своєму дослідженні Професійну підготовку бакалаврів із кібербезпеки в університетах США аналізувала Б. В. Бистрова [58], акцентуючи увагу на можливості використання міжнародного досвіду для вдосконалення вітчизняної освітньої системи.

Особливе місце в аналізі представлених робіт займає розгляд інформаційних війн і гібридних загроз. Дисертаційні дослідження таких авторів, як С.Р. Сунгурова [59], А.Д. Младьонова [60], В.П. Таркіна [61], присвячені вивченню інформаційних війн як складників гібридних конфліктів, зокрема в контексті війни в Україні. Ці дослідження розглядають інформаційно-психологічні й технічні засоби впливу та механізми їх нейтралізації. Аналіз інформаційних воєн як політичного інструменту, здатного впливати на суспільну думку та маніпулювати інформацією, підкреслює важливість розробки ефективних механізмів протидії. Зокрема О.В. Саган [62] та О.І. Жайворонок [63] розглядають явище інформаційного тероризму.

У роботах С.А. Палій [64], М.В. Копійки [65] та О.В. Фурсай [66] ідеться про міжнародні аспекти інформаційної безпеки. Вони аналізують роль інформаційних операцій у міжнародних відносинах, порівнюють українські та європейські підходи до інформаційної безпеки, а також розглядають політику

інформаційної безпеки окремих країн, зокрема Франції. Ці дослідження демонструють, що міжнародне співробітництво є ключовим елементом у боротьбі з кіберзагрозами, проте досі бракує глибокого аналізу ефективності наявнх альянсів і механізмів взаємодії.

Аналізуючи загальні результати, можемо виявити деякі важливі прогалини в дослідженні поняття «кібербезпеки». Незважаючи на те що більшість робіт зосереджені на адміністративних, технологічних та правових аспектах, політичний складник є недостатньо вивченим. Ще одним важливим недоліком у дослідженні цього питання є обмеженість міжнародної координації. Хоча в деяких статтях побіжно йдеться про міжнародний досвід, однак усебічний аналіз ефективності наявних міжнародних альянсів, таких, як НАТО і ЄС, у боротьбі з кіберзагрозами відсутній. Це свідчить про необхідність більш глибокого дослідження механізмів політичної координації та співпраці між державами для забезпечення колективної безпеки.

Третьою суттєвою проблемою, на наш погляд, є недостатня увага до участі громадськості та освіти. Деякі автори підкреслюють важливість цивільної освіти в галузі кібербезпеки, але лише поверхово розглядають питання розвитку такої кіберосвіти та активної участі суспільства в забезпеченні кібербезпеки. Ми погоджуємося з цим баченням авторів з огляду на важливість такої ланки, як поінформованість громадян у формулюванні загальної стратегії кібербезпеки.

Хоча в багатьох дослідженнях зосереджено увагу на інформаційній війні та гібридних загрозах, заходи щодо боротьби з ними не завжди вказані конкретно, часто досліджено поверхово. Крім цього, відсутні чіткі рекомендації щодо того, як ці заходи мають бути реалізовані на міждержавному рівні, що знижує їхню ефективність у протидії кібератакам. Отже, на наш погляд, слід більше уваги приділяти розробленню чітких стратегій протидії гібридним загрозам, які вимагатимуть міжурядової координації.

Можемо стверджувати, що розвиток кібербезпеки потребує збалансування юридичних, політичних і технічних міркувань і вимагає більшої

міжнародної співпраці та залучення громадянського суспільства. Тільки такий інтегрований підхід зможе дозволити сформулювати ефективні стратегії боротьби з поточними викликами та загрозами в цифровій сфері, захистити критичну інфраструктуру й підвищити кібербезпеку держави.

Аналіз наукових джерел засвідчує, що на думку вчених, кібербезпека – це насамперед стала і гарантована робота критично важливих інформаційних систем держави, порушення яких спричиняє нівелювання забезпечення державою всіх інших гарантій, безпеки її громадян та суспільства.

Порівнюючи ці визначення з положенням, закріпленим у законодавстві України, стає очевидною перевага українського формулювання. Закон України «Про основні засади забезпечення кібербезпеки» [36] визначає кібербезпеку як комплекс заходів, спрямованих на захист інформаційних систем, забезпечення їхньої цілісності, конфіденційності, доступності, а також стійкості до кіберзагроз. Цей підхід вирізняється більшою системністю, конкретикою та інтеграцією технічних і організаційних аспектів. Закон ураховує динамічність кіберзагроз і необхідність постійного оновлення заходів безпеки. Хоча і це визначення, з позиції нашого дослідження, не позбавлене певних недоліків.

По-перше, хоча українське законодавство чітко визначає параметри кібербезпеки, воно недостатньо охоплює соціально-економічні наслідки кібератак, які можуть мати критичний вплив на суспільство. Водночас деякі європейські визначення вказують на необхідності врахування економічних інтересів і стабільності цифрової економіки. Українська концепція ще не повністю інтегрує ці аспекти.

По-друге, український підхід, як бачимо, потребує вдосконалення в частині залучення приватного сектора до управління кіберризиками. Особливої ваги це набуває в контексті глобалізації кіберзагроз, коли великі транснаціональні корпорації мають більший вплив на цифрову безпеку, ніж деякі національні уряди.

Ще однією суттєвою прогалиною як у національних, так і в міжнародних визначеннях кібербезпеки є недостатня увага до культурних та міжнародних

відмінностей. Зокрема, Міжнародний телекомунікаційний союз (МСЕ) пропонує досить всеосяжне визначення кібербезпеки, яке включає стратегії, принципи та технології, спрямовані на захист кіберпростору [67]. Однак це визначення ігнорує положення про те, як культурні, правові та економічні особливості різних країн впливають на сприйняття безпеки. Наприклад, у країнах Європейського Союзу питання приватності має першочергове значення, натомість в авторитарних державах акцентовано на контролі інформаційного простору.

Окрім цього, значна частина поданих визначень кібербезпеки не враховує динамічного характеру кіберзагроз. Більшість підходів орієнтовані на статичні критерії конфіденційності, цілісності та доступності, але не розглядають механізмів адаптації до нових типів атак, таких, які використовують штучний інтелект чи технології квантових обчислень. У цьому контексті українське законодавство виглядає прогресивніше, адже передбачає регулярне оновлення заходів захисту, проте навіть тут не вистачає чітких інструкцій для адаптації політик кібербезпеки до інноваційних технологій.

Щодо практичної реалізації, то визначення часто сфокусовано на високорівневих принципах, таких, як конфіденційність та цілісність, але проігноровано конкретні механізми їхнього впровадження. Наприклад, Ю. В. Білявська та Я. І. Шестак [68] трактують кібербезпеку як систему захисту інформаційної складової, але не пропонують дієвих інструментів для досягнення такого захисту. Це призводить до того, що розуміння стосується переважно теоретичного рівня, а це особливо критично у випадках, коли необхідно швидко реагувати на реальні кіберзагрози.

Як складник національної та міжнародної безпеки аналізують кібербезпеку Д. В. Дубов та М. А. Ожеван [69]. Зокрема, вони досліджують формування провідними державами кіберстратегій, створення спеціалізованих структур, унесення до військової доктрини кіберкомпонента, оскільки кібербезпека, на їхню думку, має охоплювати воєнну, правову, політичну та етичну сфери.

Водночас через відсутність єдиної термінології та загальноприйнятих міжнародних норм країни по-різному трактують саме поняття кібербезпеки, що ускладнює глобальну взаємодію. Крім того, деякі аспекти практичної реалізації державної політики висвітлені дещо обмежено. Зокрема, потребують глибшого висвітлення питання щодо ролі приватного сектору, аналізу окремих кіберінцидентів та оцінки національного законодавства. Доцільним також видається більш детальний розгляд специфічних викликів, з якими стикається Україна в контексті розвитку кіберінфраструктури та вдосконалення нормативно-правової бази.

Порівнюючи ці аспекти, викладені в міжнародних джерелах й українському законодавстві, наголосимо, що в останньому чіткіше акцентовано на практичній реалізації заходів, що містять і конкретні вимоги до суб'єктів критичної інфраструктури. Це дозволяє досягти більшої ефективності в боротьбі з кіберзагрозами. Однак навіть тут, як ми вважаємо, існує певна прогалина у створенні механізмів оцінки ефективності впроваджених заходів. Брак чітких метрик ускладнює оцінку рівня кібербезпеки та визначення напрямів, які потребують покращення.

Важливим аспектом дослідження кібербезпеки є з'ясування ролі та відповідальності стейкхолдерів. У більшості міжнародних визначень ці аспекти залишаються «розмитими», тоді як у контексті українського законодавства, навпаки, чітко визначені обов'язки державних органів, підприємств та інших суб'єктів. На наш погляд, така ситуація, з одного боку, створює сприятливі умови для координації дій, але з іншого, вимагає вдосконалення у частині залучення громадянського суспільства та приватного сектору до управління кіберризиками.

У світлі аналізу є підстави стверджувати, що кібербезпека залишається багатогранним і складним явищем, яке вимагає більш інтегрованого підходу у визначенні. Відсутність єдиного підходу, недостатня увага до соціальних та економічних аспектів, недооцінка динамічності кіберзагроз, брак чітких механізмів реалізації, імовірно, є основними проблемами сучасних визначень

кібербезпеки. Українське законодавство пропонує чіткішу концепцію кібербезпеки, проте потребує вдосконалення в частині інтеграції міжнародного досвіду та адаптації до нових загроз.

Аналізуючи різні визначення, логічно також припустити, що кібербезпека є ключовим елементом національної безпеки і сприяє стабільній та захищеній роботі, зокрема й критично важливих інформаційних систем держави. У разі порушення їхнього функціонування можуть виникати серйозні загрози для гарантій безпеки громадян та суспільства. Тому найбільш вичерпним, на наш погляд, є визначення, яке підкреслює важливість кібербезпеки як частини національної безпеки та необхідність вжиття дієвих заходів для її реалізації.

Важливо, на нашу думку, також виявити схоже й відмінне в дефініціях описуваного поняття в окремих країнах та організаціях.

По-перше, маємо зазначити, що поняття «кібербезпека» посідає важливе місце в європейському правовому просторі, відображаючи загрози цифрової епохи та необхідність їхнього ефективного врегулювання. У нормативно-правових актах Європейського Союзу поняття кібербезпеки визначається як у формі прямої дефініції, так і в описово, залежно від мети та практичного значення окремого документа.

Так, у визначенні досліджуваного поняття, зафіксованому в Регламенті (ЄС) 2019/881 [70], який відомий як Закон «Про кібербезпеку», кібербезпека визначена як діяльність, необхідна для захисту мережевих та інформаційних систем, користувачів таких систем та інших осіб, які постраждали від кіберзагроз, а додатково вказано, що вона має охоплювати захист конфіденційності, цілісності та доступності даних, що передаються, обробляються або зберігаються в інформаційних системах. Таким чином, це визначення демонструє досить комплексний підхід до захисту, орієнтований не тільки на технічний бік, але і на безпеку користувачів і суспільства загалом. Однак, ураховуючи ситуацію, в якій опинилася Україна після повномасштабного вторгнення Росії, вважаємо, що на практиці доцільною була б рекомендація до оновлення змісту поняття відповідно до загроз, які

змінилися, адже цей прецедент вплинув не тільки на безпеку України, а й всього світу.

Описовий підхід до концепції кібербезпеки фіксуємо в Директиві 2016/1148, відомій як Директива NIS [71]. Вона не містить прямого визначення кібербезпеки, але детально описує її елементи та мету, прописуючи, що кібербезпека забезпечує високий ступінь безпеки мереж та інформаційних систем шляхом прийняття відповідних технічних та організаційних заходів. Тож, на перший погляд, Директива NIS дає чіткий опис, підкреслюючи важливість координації національних зусиль щодо забезпечення кібербезпеки та підвищення стійкості критичної інфраструктури в Європейському Союзі. Однак, як нам видається, цей підхід більшою мірою орієнтований на нормативні та управлінські аспекти кібербезпеки, ніж на конкретне визначення цього терміна.

З огляду на таку ситуацію, необхідно здійснити порівняльний аналіз теоретичного й практичного бачення питання на прикладі Центру Передового Досвіду Кіберзахисту (далі – CCDCOE), який співпрацює з європейськими країнами та НАТО з метою створення стандартів і проведення навчальних програм щодо кіберзахисту. Згідно з баченням CCDCOE [72], кібербезпеку слід розглядати як частину ширшої системи безпеки військових, і це вимагає тісної співпраці між військовими та цивільними структурами. Таким чином, методологія CCDCOE зосереджується на важливості кібербезпеки як частини сучасної системи захисту, яка акцентує на запобіганні кібератакам і розвитку стійкості у військовому контексті. Успішність такого підходу щодо розуміння кібербезпеки ми зможемо прослідкувати в наступних розділах, більш детально проаналізувавши роботу центру.

Ще один практичний підхід реалізовано Агентством Європейського Союзу з питань мережевої та інформаційної безпеки (далі – ENISA) [73], однак у своїй діяльності воно також покладається на описовий складник, підкреслюючи важливість співпраці між державним та приватним сектором для підвищення загального рівня кібербезпеки. Окрім того, ENISA акцентує увагу

на необхідності впровадження передових технологій і найкращих практик для забезпечення стійкості до новітніх загроз.

З огляду на сказане вище, логічно виникає питання: чи можна бути впевненим, що і в майбутньому за умови використання незмінного підходу успішним буде протистояння кіберзагрозам? Тому, на наше переконання, реформування методик протистояння кіберзагрозам має бути так само невпинним, як і зростання сучасних викликів до кібербезпеки.

На нашу думку, додатковим механізмом у цьому питанні може стати робота над європейською нормативно-правовою системою, зокрема реструктуризація та оновлення вже відомих актів і прийняття нових, більш спеціалізованих. Щодо Регламенту ЄС 2019/881 слід указати, що аналізоване визначення не включає всіх аспектів кібербезпеки, зокрема тих, що стосуються стратегічної координації та політики. Це може призвести до проблем з адаптацією заходів протидії до нових викликів, оскільки технічні та адміністративні підходи не становлять комплексної стратегії. Описовий підхід у Директиві NIS та Європейській стратегії кібербезпеки натомість демонструє більш гнучку позицію, але може бути недостатнім для створення універсальних механізмів і процедур кібербезпеки.

Ще однією прогалиною є відсутність уваги до людського фактору в питаннях забезпечення кібербезпеки. Більшість із досліджених нами описів стосуються технічних та адміністративних заходів, але вони не враховують важливості підвищення обізнаності користувачів та їхньої підготовки до протидії потенційним кібератакам. Крім того, у визначеннях не приділено необхідної уваги такому аспекту, як відновлення після кібератак, яке є важливим, адже відсутність чітко визначених механізмів може призвести не лише до вразливості під час наступних атак, а й ускладнити повернення систем до робочого стану.

Як наслідок стає зрозумілим, що для досягнення максимальної ефективності в забезпеченні кібербезпеки необхідно враховувати всі технічні,

політичні та військові її аспекти, дбаючи про тісний зв’язок усіх залучуваних структур.

Повертаючись до піднятої проблеми щодо відсутності єдиного уніфікованого визначення кібербезпеки в європейських організаціях, звертаємо увагу також на те, що різноманіття підходів до цієї проблеми зумовлено національними особливостями, правовими системами та рівнем технологічного розвитку кожної держави. Хоча основні принципи захисту інформаційних систем, забезпечення цілісності даних та боротьби з кіберзагрозами є спільним завданням, конкретні визначення та акценти можуть суттєво відрізнятися залежно від функцій та завдань кожної держави чи організації.

Отже, з метою глибшого розуміння поняття «кібербезпека» та відображення його трансформації у відповідь на зміни у характері загроз у кіберпросторі, було проведено дослідження підходів до кіберзахисту в низці європейських країн, а саме: Німеччині, Франції, Великій Британії та Нідерландах. Кожна з цих держав є лідером у сфері технологій і має розвинену інфраструктуру, що сприяє успіху в забезпеченні захищеного кіберпростору.

Німеччина та Франція, як економічні й політичні лідери Європи, активно розвивають комплексні стратегії для захисту від кіберзагроз, у тому числі й у критичній інфраструктурі, а Велика Британія з її історичним досвідом з питань кібербезпеки продовжує інвестувати в інновації для посилення захисту від кібертероризму. Нідерланди ж відомі своєю високою технологічною готовністю та участю в міжнародних ініціативах, що стосуються кібербезпеки. Ці країни демонструють різноманітність підходів і практик, що дозволяє отримати ширше уявлення про стан кібербезпеки в Європі.

Так, первинний аналіз матеріалів допоміг виявити, що у багатьох європейських країнах термін «кібербезпека» залишається багатозначним і не завжди має чітке визначення у національних законодавчих актах. Зазвичай аспекти кібербезпеки інтегровані у ширші правові межі, такі, як інформаційна безпека, захист критичної інфраструктури або управління ризиками, що

підкреслює багатогранність цього поняття та його тісний зв'язок із різними секторами національної безпеки.

У Німеччині, наприклад, Закон «Про ІТ–безпеку», що має назву «ІТ–Sicherheitsgesetz» [74], установлює жорсткі вимоги до захисту інформаційних систем, особливо тих, що належать до критичної інфраструктури, а саме: енергетичні мережі, транспорт чи охорона здоров'я. Хоча у цьому законі термін «кібербезпека» не визначений окремо, він розглядається як комплекс технічних та організаційних заходів, спрямованих на забезпечення цілісності, доступності та конфіденційності ІТ– систем. Такий підхід збігається з тим, що дає ENISA, адже базується на практичних аспектах управління кіберризиками через імплементацію сучасних технологій захисту. Однак слід ще раз наголосити на тому, що важливою залишається консолідація з політико-правовим напрямом з метою створення всеохопної методики кібербезпеки.

Франція, своєю чергою, Законом щодо військової програми 2019– 2025 років трактує кібербезпеку як «сукупність заходів, технологій і політик, спрямованих на захист національної цифрової інфраструктури, з особливим акцентом на безпеку військових комунікацій» [75]. Такий підхід виводить кібербезпеку Франції на стратегічний рівень і визначає її як важливий елемент національної оборони, тим самим виділяє кіберпростір як нову арену військових дій, наголошуючи на посиленій увазі до захисту об'єктів критичної інфраструктури.

Зауважимо також, що досвід Великої Британії вкрай важливий для України, оскільки на сьогодні ця країна виступає лідером в аспекті кібербезпеки, успішно відсікаючи майже всі загрози кіберпростору. Така наша позиція буде доведена далі через розгляд складників безпечного кіберпростору Британії. Так, наприклад Закон «Про кібербезпеку» 2018 року [76] пропонує розширене трактування кібербезпеки, зосереджуючись на захисті інформаційних систем та даних від несанкціонованого доступу, використання, розголошення, порушення, модифікації чи знищення. У цьому контексті кібербезпека охоплює широкий спектр заходів, спрямованих на забезпечення

захисту апаратного та програмного забезпечення, даних і мереж, що свідчить про цілісний підхід британського законодавства до цифрової безпеки. Особливістю британського підходу є баланс захисту персональних даних і водночас забезпеченні безперервності інформаційних процесів держави, що відповідає сучасним викликам щодо кібербезпеки.

У Нідерландах Закон «Про безпеку мережевих та інформаційних систем» [77] визначає кібербезпеку як ключовий елемент національної безпеки, зосереджуючись на захисті від несанкціонованого доступу, витоку даних та операційних збоїв у роботі інформаційно-комунікаційних технологій. Голландське законодавство зосереджує увагу на важливості впровадження заходів безпеки як у державному, так і в приватному секторах. Ця особливість, як бчимо, зближує його з британським. Однак підхід Нідерландів до кібербезпеки відзначається чітким розмежуванням різних типів загроз, таких, як кібервійна, шпигунство, терористичні дії в інтернет-просторі, хактивізм та кіберзлочинність. Нідерланди – єдина країна з досліджуваних нами, яка звертає на це значну увагу і визначає, що кожна з цих загроз має свої специфічні характеристики й потребує окремих стратегій реагування. Ми дотримуємось переконання, що такий підхід є досить всеохопним і необхідним для вивчення Україною, бо та стратегія, котру пропонують Нідерланди, дозволяє уникати плутанини в політичних дискусіях і сформувати національну стратегію кібербезпеки, яка справді працює.

Нарешті, скажемо Польський закон від 5 липня 2018 року «USTAWA z dnia 5 lipca 2018 r. o krajowymsystemiecyberbezpieczeństwa» [78], який визначає поняття кібербезпеки як стійкість інформаційних систем до дій, що порушують конфіденційність, цілісність, доступність і достовірність оброблених даних або супутніх послуг, пропонованих цими системами. На нашу думку, таке визначення є досить повним, адже охоплює питання організації та функцій національної системи кібербезпеки в Польщі, підкреслюючи її важливість для реалізації безпеки інформаційних систем. Уважаємо, що такий підхід до структуризації самого поняття є одним із ключових, оскільки він допомагає

з’ясувати, чому Польща на сьогодні є одним із європейських регіональних лідерів в організації кібербезпеки, про що йтиметься в наступних розділах.

Підбиваючи підсумок, зазначимо, що підходи до кібербезпеки в досліджуваних країнах демонструють спільні риси, такі, як акцент на критичній інфраструктурі, управлінні ризиками й консолідації роботи державного та приватного секторів в національну систему кібербезпеки. Водночас кожна з цих країн має свої унікальні особливості у правовому регулюванні кібербезпеки, що відображає національні пріоритети, рівень технологічного розвитку та характер кіберзагроз, з якими стикаються держави.

Важливим є те, що більшість європейських країн гармонізує свої національні законодавства відповідно до директив Європейського Союзу, зокрема Директиви NIS, упровадження якої сприяє створенню цілісного підходу до організації кібербезпеки. Проте кожна держава зберігає певну автономію у формулюванні національних законодавчих актів. Таку гнучкість пояснюємо особливістю адаптації заходів кібербезпеки до специфічних потреб кожної країни.

Разом із тим, попри зусилля з гармонізації, визначення кібербезпеки у законодавстві кожної з країн значно різняться. Деякі держави надають чіткі й конкретні визначення, установлюючи параметри та межі заходів кібербезпеки, а інші використовують неоднозначний підхід, інтегруючи аспекти кібербезпеки в ширші правові концепції, зокрема інформаційну безпеку або захист критичної інфраструктури, без прямого визначення терміна «кібербезпека».

Водночас динамічний характер кіберзагроз потребує від держав адаптивних законодавчих визначень, які б відповідали технологічним інноваціям і змінам у середовищі кіберзагроз. У цьому контексті багато європейських країн регулярно оновлює свої нормативно-правові акти з метою врахування нових викликів (далі ми з’ясовуватимемо, чи дозволяють уживані засоби забезпечувати державам їхню безпеку та ефективність методик у швидко змінюваних умовах кіберпростору).

Таким чином, законодавчі підходи до визначення кібербезпеки в Європі демонструють як тенденцію до уніфікації, так і різноманітність, зумовлену національними пріоритетами та правовими традиціями. Хоча базові принципи кібербезпеки (захист інформаційних систем, забезпечення цілісності, конфіденційності та доступності даних) є спільними для більшості країн, їх конкретизація та реалізація залишаються унікальними для кожної з них. Характер визначення терміна «кібербезпека» та його складників є відображенням багатовимірності, що поєднує юридичні, технічні й стратегічні компоненти та вимагає глибокого розуміння локальних підходів для забезпечення ефективного кіберзахисту.

У результаті аналізу було виявлено деякі прогалини, які не дають змоги повномірно розкрити концепт поняття кібербезпеки, що, своєю чергою, указує на кілька ключових аспектів, які потребують подальшого дослідження та чіткого визначення. Одним із основних напрямків є інтердисциплінарний підхід до кібербезпеки, оскільки вона охоплює широкий спектр дисциплін (від інформаційних технологій до права, економіки, соціальних наук і навіть медицини). Різні професіонали, що працюють у цих напрямах, можуть трактувати термін «кібербезпека» по-різному, а це створює певні перешкоди для формулювання єдиного та узгодженого визначення. Особливої актуальності це набуває в умовах глобалізації, коли кіберзагрози мають транснаціональний характер.

Отже, важливим для нашого дослідження є розроблення єдиної концепції кібербезпеки, яка б інтегрувала всі аспекти, не враховані до цього.

Ще одним питанням, що вимагає доопрацювання, є національні політики кібербезпеки, які охоплюють стратегії та підходи окремих країн до забезпечення цифрової безпеки. Різноманітність національних підходів до кібербезпеки, зокрема між країнами з різними рівнями економічного та технологічного розвитку, є основною перешкодою для глобальної координації в цьому напрямку. Відсутність єдиного бачення щодо того, як побудувати ефективну національну політику кібербезпеки, обмежує можливості для

співпраці між державами та міжнародними організаціями. Україна, зокрема, потребує узгодження власної національної стратегії в контексті міжнародних стандартів і загроз.

Ще один аспект, який потребує додаткового осмислення, – це кібербезпека як економічне «благо». Ураховуючи той факт, що сучасна економіка значною мірою залежить від технологій, питання інтеграції кібербезпеки в економічну стратегію держави стає надзвичайно актуальним. Однак на сьогодні не існує чіткого розуміння того, як кібербезпека може сприяти економічному розвитку та функціонуванню цифрових технологій.

Таким чином, приходимо до висновку що кібербезпека як політична й стратегічна концепція не обмежується захистом інформаційних систем і превентивними заходами проти кібератак. Навпаки, вона має бути фундаментальною частиною сучасної національної безпеки, настільки ж важливою, як оборонні можливості та дипломатичний складник. На нашу думку, сучасне розуміння кібербезпеки потребує вдосконалення та чіткого визначення, зокрема, це передбачає захист не лише технічних систем, а й соціальних, економічних і політичних компонентів. Крім того, удосконалення тлумачення терміна має значення для координації міжнародної, регіональної та державної співпраці. Нове визначення матиме потенціал для сприяння створенню освітніх програм, підготовки спеціалістів і росту кіберосвіченості населення.

Отже, запропонуємо визначення, яке згідно з нашим баченням охоплює сучасний стан проблем у кіберпросторі і новітніх викликів, спричинених трансформацією суспільства. Отже, відповідно до нашого підходу «кібербезпека – це комплексний стратегічний процес безпеки національного суверенітету, політичної стабільності, критичної інфраструктури та забезпечення захисту інтересів прав та свобод громадян у кіберпросторі від деструктивного впливу будь-яких внутрішніх та зовнішніх кіберзагроз із використанням багаторівневих політико-правових, технічних та соціальних інструментів».

Таке уточнення визначення терміна «кібербезпека» створює підґрунтя для ефективного впровадження практичних заходів на державному рівні. Розглядаючи політичні рекомендації для України, можемо виділити кілька кроків, які, на наш погляд, спрятимуть забезпеченню національної кібербезпеки та стійкості до сучасних загроз:

1. Україні необхідно розробити чітку системну стратегію кібербезпеки, яка б визначала пріоритети, роль уряду, приватного сектору та громадськості в забезпеченні цифрової безпеки. Така стратегія повинна бути інтегрована в загальну національну безпеку та враховувати як внутрішні, так і зовнішні загрози, зокрема агресію з боку інших держав у кіберпросторі.

Так, правильним кроком убачаємо 10 екстрених заходів, необхідних для реалізації системи кібербезпеки:

1) створення підрозділів кіберполіції, які б безпосередньо відповідали за кібербезпеку;

2) підготовка оновленої національної стратегії щодо роботи інформаційної та комунікаційної інфраструктур;

3) установлення показників, які визначають ефективність кібербезпеки;

4) забезпечення особливих умов конфіденційності в межах роботи служб, які забезпечують кібербезпеку України;

5) проведення міжвідомчого нормативно-правового аналізу для визначення пріоритетних питань в галузі кібербезпеки;

6) ініціювання національної інформаційно-просвітницької кампанії із сприяння забезпечення кібербезпеки;

7) розроблення єдиного міжнародного плану дій щодо забезпечення кібербезпеки і зміцнення регіонального та міжнародного партнерства;

8) підготовка технічного плану протидії актам кібертероризму;

9) вироблення основ для застосування новітніх технологій, які могли б забезпечити підвищення рівня кібербезпеки, надійності та стійкості роботи цифрової інфраструктури;

10) прийняття оновленого протоколу кібербезпеки, заснованому на стратегії управління.

Вищевказані заходи мають рекомендаційний характер до впровадження та удосконалення як в Україні, так і в інших державах, оскільки мережеві технології дають унікальну можливість застосування інноваційних технологій у «підривній» діяльності з метою політичного впливу, а збільшення масштабів соціальної небезпеки таких протиправних діянь в інформаційній сфері зумовлює необхідність підвищення рівня захищеності критично важливих об'єктів інфраструктури, а також важливим є посилення протидії загрозі поширення кіберзлочинності у будь-якому її вияві.

2. В українському законодавстві важливо стандартизувати терміни та концепти щодо кібербезпеки. Рекомендовано брати активну участь у міжнародних ініціативах з гармонізації забезпечення кібербезпеки. Це дозволить ефективніше співпрацювати з іншими державами та міжнародними організаціями задля забезпечення колективної кібербезпеки.

3. Необхідно розвивати міждисциплінарні підходи щодо підготовки кадрів, оскільки, як було наголошено, кібербезпека є не лише технічною проблемою, але й правовою, економічною та соціальною. Для цього важливо створювати програми навчання, які б ураховували комплексний підхід до цього напрямку та забезпечували підготовку фахівців, здатних працювати на перетині різних дисциплін. Крім того, Україні необхідно активно інвестувати в наукові дослідження щодо питань кібербезпеки.

4. Законодавчі ініціативи щодо кібербезпеки слід реформувати та постійно вдосконалювати, зокрема в українських нормативних актах слід уточнювати та оновлювати визначення термінів, пов'язаних із кіберзагрозами.

5. Необхідно створити національний механізм «кіберполітичного нагляду». Ідеться про політичний інструмент для забезпечення одночасно і контролю, і захисту прав громадян у кіберпросторі. Потрібно, щоб він виконував не лише функції нагляду, але й політичного представництва інтересів громадян в умовах цифрових викликів. Зокрема, це має стосуватися

формування державної кіберполітики, моніторингу дотримання стандартів кібербезпеки та впливу на ухвалення рішень з питань кіберзахисту, що безпосередньо стосуються прав і свобод громадянського суспільства. Функціонування такого механізму, вважаємо, слід налагодити через упровадження в Україні посади «кіберомбудсмена».

З огляду на постійне збільшення кількості кіберзагроз, уключаючи кібератаки на державні установи, критичну інфраструктуру та приватні компанії, а також зростання ролі цифрових технологій у повсякденному житті, запровадження такої посади могло б значно посилити національну кібербезпеку та довіру громадян до державних заходів у цьому напрямку. Першочерговим завданням кіберомбудсмена, як незалежного уповноваженого представника держави, має бути захист суспільних прав і свобод у цифровому просторі, моніторинг дотримання законодавства щодо кібербезпеки, а також функція посередника між державою, приватним сектором і власне громадськістю. Важливо, щоб кіберомбудсмен був уповноважений не лише розглядати скарги щодо порушення прав «всіх і кожного» у кіберпросторі, але й подавати пропозиції для вдосконалення національної кіберполітики та законодавства.

На наше переконання, професійне призначення кіберомбудсмена полягає у виконанні не лише правозахисних обов’язків, а й функції аналізу та попередження кіберзагроз. Наприклад, це може бути здійснення аудиту державних і приватних організацій щодо дотримання вимог кібербезпеки, виявлення вразливості та забезпечення підтримки в їх усуненні. Крім того, ця посадова особа повинна мати право брати участь у розробці законодавчих ініціатив та національних стратегій у галузі кібербезпеки, забезпечуючи належне врахування інтересів громадян.

На рівні міждержавної співпраці його завдання полягатиме в участі в міжнародних форумах і представництві України щодо питань, які стосуються суспільної політики в цифровому середовищі.

Узагальнюючи, зазначимо, що створення посади кіберомбудсмена свідчитиме про розвиток держави як демократичного механізму, здатного

реагувати на виклики цифрової епохи, сприятиме підвищенню прозорості та підзвітності державних структур, що є важливим для забезпечення довіри громадян до державної влади. Кіберомбудсмен зможе стати своєрідним «гарантом» того, що цифрові права громадян будуть захищені, а держава буде зобов'язана відповідати на запити громадськості та приватного сектора щодо питань забезпечення кібербезпеки. Це є важливим чинником у формуванні сильної кібердемократії, де громадяни відчувають себе захищеними й мають інструменти для відстоювання своїх прав.

6. Рекомендуємо впровадити таку концепцію, як «формування кіберімунітету суспільства», яка полягатиме в захисті громадян від впливу кібертерористичних наративів. Особливість концепції полягає у використанні політичних та соціальних інструментів для створення «імунітету суспільства» до руйнівного впливу кібертерористів.

Отже, «кіберімунітет» – це не лише технічний захист, а й навчання, роз’яснення, інформування, співпраця між державою та суспільством. Це як комплекс дій, які забезпечують кожному громадянину, організації та установі в Україні впевненість у захисті в ситуації кіберзагроз. Це наче «імунітет до хвороби», але колективний, коли всі разом навчаються бути більш захищеними у цифровому світі. Цей підхід поєднає соціально-політичні заходи з кібербезпекою, і основна увага має бути приділена формуванню стійкої громадської думки як елемента національної безпеки.

7. Доцільно започаткувати ще одну концепцію – «кіберсоціальну адаптацію». Це означатиме врахування соціальної та культурної специфіки забезпечення кібербезпеки, зробить запроваджувані заходи із посилення кібербезпеки більш ефективними та узгодженими з місцевими морально-правовими нормами, соціальними структурами та особистісними якостями, щоб їх можна було точно підлаштувати до певних соціальних умов та виробити імунітет до кібертероризму.

1.3. Методологічні основи дослідження проблеми протидії кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону

Згідно з проаналізованою нами інформацією доходимо висновку, що успіх кожної країни щодо захисту національних секторів інфраструктури значною мірою буде залежати від зусиль усієї світової спільноти, спрямованих на створення захищеного і безпечного кіберпростору. На жаль, виняткові технічні рішення та внутрішня політика держав не можуть забезпечити належний захист від кібертероризму через відсутність територіальних кордонів і можливість завдавати шкоди далеко за межами юрисдикції окремої держави.

Беручи до уваги сучасний розвиток кіберзагроз, їх високий рівень координації, глобальності та складності, можемо стверджувати, що необхідно всі узгоджені міжнародні зусилля спрямовувати для їхнього ефективного стримування. Визначене демонструє важливість широкого міжнародного співробітництва в галузі політики, уключаючи обмін інформацією про кіберзагрози, гармонізацію нормативно-правової бази, стандартизацію заходів реагування, спільні навчання і підготовку фахівців із кібербезпеки. Такого роду спільні дії міжнародного співтовариства, підкріплені політичною волею країн, зможуть забезпечити достатній рівень кіберстійкості і захисту від глобальних кіберзагроз.

А втім, відзначимо, що, незважаючи на вжиті у всьому світі заходи безпеки, загроза кібертероризму залишається, а в окремих інформаційно розвинених країнах постійно загострюється. Тому успішне вирішення цієї проблеми можливе лише за спільних зусиль держав із використанням при цьому різних принципів та методів попередження та протидії кібертероризму .

У ході дослідження даної проблеми розглянуті та застосовані такі методи аналізу: бібліографічний, історичний, термінологічний, метод нормативно-правового аналізу, ціннісно-нормативний, аксіологічний, метод аналізу і синтезу; системного аналізу, порівняльний.

Бібліографічний метод дозволив сформувати фундамент для подальших досліджень, оскільки допомагає систематизувати накопичені знання та побачити повну картину проблеми, визначає, які її аспекти вже вивчені, а які ще потребують висвітлення. Наприклад, у дослідженні кібертероризму ретельний аналіз літератури дає змогу визначити спочатку наявні методи боротьби з кіберзлочинністю, установити ефективність цих методів і нарешті потребу в їхньому вдосконаленні. Крім того, аналіз архівних матеріалів та історичних джерел дає змогу зрозуміти еволюцію кібертероризму, простежити зміни його форм і методів, що важливо для прогнозування майбутніх загроз і розроблення превентивних заходів.

Дослідження матеріалів, що стосуються електронних ЗМІ, є особливо актуальним у сучасну цифрову епоху, коли більшість джерел інформації можна отримати онлайн. Це полегшує доступ до найновіших наукових публікацій, звітів, результатів досліджень та інших ресурсів, які допомагають з'ясувати складну природу кібертероризму та його вплив на суспільство. Іншою важливою складовою бібліографічного методу є аналіз матеріалів, що висвітлюють правові аспекти протидії кібертероризму, зокрема міжнародні та національні нормативно-правові акти, положення та пропозиції щодо боротьби з кіберзагрозами.

Комплексний аналіз літератури допомагає з'ясувати прогалини, зрозуміти плюси та мінуси вже сформульованих концепцій, установлених фактів, зібрати накопичений досвід, щоб тим самим визначити обсяг теми. Цей метод дозволяє нам зосередитися на невідомих чи недостатньо вивчених аспектах проблеми, запропонувати нові рішення та створити концептуальну основу для подальших наукових досліджень. Згідно з темою нашої роботи це стосується визначення прогалин у національних стратегіях кібербезпеки, вивчення ефективності міжнародної координації щодо протидії кібертероризму та дослідження нових загроз, які ще не були належним чином вивчені.

Крім того, бібліографічний метод дає змогу оцінити підходи інших науковців до реалізації цієї теми, зрозуміти використовувані ними інструменти

та методи. Такий підхід допоможе нам вибрати найефективніший підхід до власного дослідження, дозволить уникнути повторення попередніх ідей і додасть новизни та вдосконалення загальнотеоретичної бази. Цей обширний аналіз допомагає створити основу для розробки нових методів, ідей і рішень проблеми кібертероризму.

Було опрацьовано 825 джерел, з яких відібрано 345. Вироблені критерії відбору допомогли вилучити непотрібну літературу, найголовніші з критеріїв такі:

– відсутність політичного контексту, тобто література, яка обговорювала виключно технічні чи юридичні аспекти кібертероризму без урахування політичного аспекту не вважалася підґрунтям дослідження. Для нашого дослідження було вкрай важливим зрозуміти політичні стратегії, вплив національної та міжнародної політики, через це технічні описи не становили інтересу;

– застарілість інформації, тобто література, що не враховує сучасних змін у характері кібертероризму та новітніх політичних підходів, не може адекватно відображати поточний стан проблеми. Це не стосувалося законодавчих актів, Конвенцій, Директив та історичних прикладів кібертерористичних атак;

– низька надійність джерел: література, опублікована в нерецензованих виданнях, праці авторів без визнаного досвіду у галузі кібербезпеки чи політики, була виключена з розгляду. Такі джерела не забезпечують високої якості інформації, а їх висновки можуть бути суб'єктивними або недостатньо обґрунтованими;

– мова публікацій стала не менш важливим критерієм відбору. Джерела російською мовою, зокрема статті, новини та документи, не використовуються у дослідженні через визнання країни – носія цієї мови агресором.

Наступним методом, використаним в ході дослідження цієї роботи, є історичний метод. Він необхідний з двох причин: по-перше, накопичений

історичною наукою досвід дослідження кібертероризму важливий для уточнення об'єкта та предмета роботи, а по-друге, такий матеріал значущий для аналізу еволюції кібертероризму як явища, що виникло і зазнало значних трансформацій на етапі розвитку інформаційних технологій. Таким чином, за допомогою історичного методу можна простежити, як кібертероризм змінювався з часом: від простих форм кіберзлочинності, таких, як злом веб-сайтів і поширення вірусів, до складних і організованих атак на об'єкти критичної інфраструктури.

Історичний метод також дозволяє виявити, як кібертероризм еволюціонував у відповідь на зміну політичних умов, технологічний розвиток і появу нових інструментів захисту від кіберзагроз і протидії їм. Зокрема, важливо дослідити характеристики атак у різні історичні періоди, щоб зрозуміти, як змінилися форми кібертероризму в контексті глобалізації та розширення міждержавних відносин. Такий підхід дає можливість глибше оцінити причини виникнення кібертероризму, його основні тенденції та виклики, з якими стикається міжнародне співтовариство в боротьбі з ним. Обраний метод уможливлює аналіз ключових прикладів з минулого, які мали вплив на формування сучасних підходів до протидії кібертероризму та загальному забезпеченню кібербезпеки. Спираючись на історичний досвід, можемо не лише зрозуміти, як кібертероризм так швидко трансформувався до рівня загрози, але й визначити найбільш вразливі періоди в розвитку критичної інфраструктури та детально вивчити, як різні держави та міжнародні організації реагували на кіберзагрози в різні історичні періоди.

Отже, застосування історичного методу в цьому дослідженні може допомогти точніше визначити природу та особливості кібертероризму, охарактеризувати його історичний розвиток, простежити зміни в його формах та цілях і, зрештою, краще зрозуміти, як же він впливає на сучасний світ. З огляду на це, на основі аналізу минулого досвіду та прогнозування майбутніх викликів можна буде визначити найбільш ефективні заходи протидії.

Наступним використовуватимемо термінологічний метод. Він дає можливість оперувати базовими та периферійними поняттями проблеми через аналіз наявних та закріплених у теорії суміжних понять. У межах нашого дослідження термінологічний метод передбачає вивчення багатогранності таких термінів, як «кібертероризм» та «кібербезпека», розробку та уточнення їхнього змісту та обсягу, місця в понятійному апараті, на якому базується дослідження, ураховуючи допоміжні пояснення таких визначень, як «тероризм», «кіберпростір», «національна безпека» та інші. Указаний метод допоможе систематизувати тексти нормативних актів та визначити їх як складників термінологічного апарату політологічної галузі. Це дозволяє охарактеризувати документ за ступенем розкриття термінів, їх повноту, точність, ступінь наукової розробки, адаптованість залучених понять до сучасного рівня розвитку проблеми. Додаткова структуризація тексту, зокрема, визначить необхідність та можливість політологічної інтерпретації інших термінів, які трапляються в тексті документів, розмежувати ідеї, закладені в документах, та подати власні уявлення про ступінь проблематики.

Термінологічний метод реалізується також через метод нормативно-правового аналізу, оскільки другий є невід'ємний складником вивчення чинної правової бази європейських держав щодо кібербезпеки та кібертероризму. Указаний метод полегшує аналіз законів, підзаконних актів та інших офіційних документів, які регулюють правові механізми суспільної взаємодії й містять політичні аспекти організації та функціонування системи державної влади та управління. Дослідження нормативних документів дає можливість зрозуміти, як законодавчий орган регулює питання забезпечення кібербезпеки та й власне заходи та плани, які застосовуються для захисту національних інтересів.

Реалізація цього методу дає можливість використовувати законодавчі акти нормативно-правової системи конкретної країни як надійний засіб документування, адже такі акти є прикладами зусиль державного апарату щодо протидії кібертероризму. Найяскравіше ці зусилля виявляються через криміналізацію нової злочинної діяльності, пов'язаної з використанням

інформаційних технологій. Оскільки створення технологій та їх широке впровадження у різні галузі людської діяльності призвело до появи нових видів злочинної поведінки, держави європейського регіону були змушені змінювати свої закони, уносячи зміни та доповнення, які полегшують більш ефективну відповідь на кіберзагрози.

Метод нормативно-правового аналізу сприяє розумінню того, як із часом розвивалися підходи до боротьби з кібертероризмом і які правові механізми застосовувалися для регулювання нових загроз у цифровому просторі. Наприклад, аналіз національних стратегій кібербезпеки полегшує визначення основних цілей політики кібербезпеки, серед яких визначається захист критичної інфраструктури, регулювання відповідальності за кіберзлочини, міждержавна співпраця та партнерство з міжнародними організаціями. Крім того, аналіз законодавчої бази дає змогу оцінити ступінь, до якого різні країни європейського регіону гармонізували своє законодавство щодо проблеми протидії кібертероризму. Це важливо, оскільки дозволяє визначити спільні та відмінні підходи до регулювання цієї проблеми, а врахування міжнародних угод, рекомендацій міжнародних організацій та національного законодавства полегшує оцінку ступеня успішності держав у колективних заходах безпеки.

Як результат, метод нормативно-правового аналізу дає можливість не лише створити правові основи боротьби з кібертероризмом, а й зрозуміти, як ці правові механізми функціонують у контексті політичної реальності, як вони впливають на організацію державної влади і які зміни необхідні для покращення реагування на сучасні загрози.

У вивченні кібертероризму велике значення має також ціннісно-нормативний метод. Він допомагає зрозуміти значення явища, вплив, який воно має на конкретні цінності та норми суспільства. За допомогою цього методу можна оцінити, наскільки кібертероризм порушує наявні соціальні правила, визначити ступінь загрози національній безпеці, громадському порядку та правам людини, оцінити вплив цього явища на соціальну стабільність і розвиток.

Ціннісно-нормативний метод також може полегшити ідентифікацію цінностей, на які негативно впливає кібертероризм, ідеться, наприклад, про стабільність, приватність і навіть свободу, тобто стимулює комплексний аналіз наслідків від кібертерористичних атак на різних рівнях (від особистого до національного). Наприклад, можна оцінити ступінь зменшення суспільної довіри до державних установ, або виміряти наслідки кібертерористичних атак на критичну інфраструктуру для громадян та держави.

Водночас указаний метод сприяє виробленню пропозицій і прогнозуванню майбутніх дій, бо дозволяє оцінити ефективність упроваджених заходів щодо дотримання нормативних вимог і необхідні додаткові дії для досягнення більшого рівня забезпечення кібербезпеки. Його використання допомагає порівняти кібертероризм з іншими суспільними викликами, визначити ступінь загрози для національної безпеки, громадського порядку та прав людини, а також оцінити, яким чином це явище впливає на суспільну стабільність та розвиток.

З огляду на зазначене, бачимо важливість ціннісно-нормативного методу в оцінці явища кібертероризму саме в контексті його впливу на суспільну політику та цінності, визначення найбільш ефективних шляхів досягнення бажаного рівня кібербезпеки не тільки для держави, а й для її громадян. Обраний метод сприяє кращому розумінню як загроз, так і засобів, пов’язаних з ними, що, своєю чергою, сприяє розробленню стратегій, які відповідають ціннісним орієнтаціям суспільства та сприяють стабільності й безпеці суспільства.

Аксіологічний метод дозволяє визначити кількісні характеристики вчинення кібератак конкретно на державні інфраструктури, які забезпечують головні потреби населення країн європейського регіону. Оскільки XXI ст. характеризується різким зростанням кібератак на системи життєдіяльності держав в усьому світі, відповідне зростання кількості спроб здійснити кібератаку може представляти нове покоління «терористів» та їх невдоволення урядами, приватними компаніями або іншими неурядовими групами. Унаслідок

цього кібертероризм стає ефективним способом тиску на владу, а його наслідки мають не менш небезпечний характер, аніж фізичні напади на критичну інфраструктуру. Подібні види атак, вироблені кібернетичним шляхом, можуть вивести з ладу такі критичні системи, як водо- й енергопостачання, ядерні реактори, транспортні вузли та інші стратегічні об'єкти.

Крім названих, важливим є використання в нашому дослідженні методу аналізу. Його використання пов’язане з розмежуванням понять «кібертероризм» та «кібербезпека», виокремлення складових елементів, тобто виділення ознак для вивчення їх як частини єдиного поняття. Цей метод використаний задля виявлення ознак, властивостей поняття з метою визначення їх схожих та відмінних рис.

Протилежний йому, але не менш важливий і використовуваний нами – це метод синтезу, який полягає у визначенні взаємозв'язків та об'єднанні різних елементів кібертероризму в єдине поняття.

З’ясувати, як розкриваються контрольні механізми попередження та протидії кібертероризму, ми зможемо за допомогою методу системного аналізу: визначено сильні та слабкі захисні методи європейських держав із Україною включно та розроблені можливі засоби покращення захисту критичної інфраструктури, а також регіональної та державної кібербезпеки загалом. Системний аналіз є підгрунтям для поєднання знань і досвіду фахівців щодо протидії кібертероризму під час знаходження рішень, труднощі яких не можуть бути подолані на основі суджень будь-якого окремого експерта.

Проблема полягає в тому, що кібертероризм – це складне як теоретичне, так і практичне питання, яке потребує термінового розв’язання чи хоча б контролювання ситуації. В основі названої проблеми – пояснення багатогранного феномену, який містить в собі велику кількість виявів, видів та детермінацій. Тому пошук найкращих рішень під час вибору стратегічних і тактичних варіантів протидії кібертероризму слід здійснювати з урахуванням системного аналізу. Реалізація таких проектів завжди пов'язана з елементами

невизначеності, що виникають у процесі розвитку як самих цих систем, так і систем допоміжних.

Останній метод, який ми застосуємо, – метод порівняння. Він допомагає пояснити і більш об'єктивно проаналізувати політичні процеси, які відбуваються під час вивчення явища кібертероризму та методів протидії йому. Наукове дослідження сприятиме використанню позитивного досвіду вироблених систем та методик протидії кібертероризму, накопичених у різних країнах європейського регіону, можливості їх використання стосовно специфіки організації кібербезпеки в Україні. Для виконання завдань цього дослідження використовуватимемо такий алгоритм:

1) розглянемо кожну досліджувану країну;
2) виокремимо ознаки, за якими можна їх порівняти;
3) порівняємо їх за всіма визначеними ознаками;
4) з’ясуємо спільне;
5) виявимо відмінності;
6) визначимо досягнення та недоліки.

Результатом порівняння стануть теоретичні узагальнення, виведені з урахуванням обробки емпіричного матеріалу як закономірностей, класифікацій, типологій та прогнозів. Головним завданням дослідження є вироблення підходів до формування політик безпеки, які містять у своєму складі підсистеми з різними функціями й умовами.

Отже, можемо стверджувати, що багато із обговорюваних вище методів покликані сформувати адекватні підходи до визначення політики безпеки в умовах протидії кібертероризму. Складність полягає не тільки в розробці конструктивних моделей, але й в пошуку теоретичних підходів до створення технологій та інструментальних засобів для реалізації окремих механізмів цих моделей. Робота на цих напрямках потребує залучення різних методів і спільної скоординованої роботи фахівців в області кібербезпеки.

Завершуючи аналіз методологічних засад дослідження проблеми «Протидії кібертероризму як сучасній загрозі національній безпеці держав Європейського регіону», можемо зробити певні висновки, наведені далі.

Протидія кібертероризму вимагає як внутрішніх, так і міжнародних зусиль. Причина в тому, що сучасні кіберзагрози не мають територіальних обмежень і можуть завдавати шкоди, що виходить за межі юрисдикції однієї країни. Це означає, що технічні рішення, які використовуються в одній державі, не є ефективними для забезпечення належного рівня кібербезпеки в іншій, натомість усі міжнародні суб'єкти повинні вжити узгоджених дій.

Сучасні кіберзагрози мають високий ступінь координації, глобальності та складності, що зумовлює необхідність співпраці між країнами щодо обміну інформацією, гармонізації законодавства та збільшення спеціалістів у сфері кібербезпеки. У цьому контексті політичне бажання держав співпрацювати та координувати дії має вирішальне значення для успіху. Незважаючи на застосовувані сьогодні механізми безпеки, кібертероризм продовжує залишатися значною загрозою, яка лише зростає. Це свідчить про необхідність постійного вдосконалення контрзаходів шляхом застосування різних підходів і методів, які охоплюють національний, регіональний та міжнародний рівні.

Методи, використані під час дослідження, уключаючи історичний, метод правового та нормативного аналізу, термінологічний, ціннісний та порівняльний, сприяють усебічному огляду накопичених знань щодо кібертероризму. Бібліографічний метод допоміг створити основу для додаткових досліджень шляхом широкого огляду наукової літератури, що призвело до виявлення вже наявних концепцій, задокументованих фактів та з'ясування прогалин, які потребують подальшого вивчення. Історичний метод допоміг в дослідженні еволюції кібертероризму, що дозволило нам спостерігати зміни в його формах і методах від простих випадків кіберзлочинності до складних атак на критичну інфраструктуру. Це посприяло розумінню механізмів розвитку кібертероризму та визначило майбутні виклики й загрози, що необхідні в розробленні ефективних стратегій їх запобігання.

Методом нормативно-правового аналізу виявлено структуру нормативно-правових актів різних країн щодо кібербезпеки та протидії кібертероризму, що дозволяє оцінити їх ефективність та потенціал для гармонізації на регіональному й міжнародному рівнях.

Ціннісно-нормативний та аксіологічний методи дозволили визначити значення явища кібертероризму для суспільства й держави, вплив, здійснюваний ним на найважливіші цінності – національну безпеку, стабільність, права, свободи і навіть життя громадян. Процедура аналізу та синтезу, а також метод системного аналізу полегшили структурний огляд кібертероризму, допомігши виявити різні складники у їх взаємозв'язках.

Унаслідок цього визначено, що для успішної протидії кібертероризму необхідним є комплексний міждисциплінарний підхід, який містить політичні, правові та технологічні компоненти. Це пояснюємо тим, що одним із головних недоліків на сьогодні є відсутність комплексного аналізу ефективності міжнародної співпраці. Розуміння та усвідомлення цих питань сприятиме як посиленню національної безпеки окремих держав, так і створенню єдиного міжнародного механізму боротьби з кібертероризмом. Зважаючи на наш підхід, цей спосіб є єдиним у забезпеченні достатнього рівня кібербезпеки як в окремих державах, так і в європейському регіоні загалом.

ВИСНОВКИ ДО РОЗДІЛУ І

Оскільки кібертероризм – уже реальність сьогодення, то вважаємо за необхідне закріпити на законодавчому рівні обов'язок державних і приватних структур здійснювати прийняття технічних заходів, які зможуть забезпечувати захист комп'ютерних мереж як одного з найбільш вразливих елементів сучасного суспільства. Варто додати, що вкрай необхідним є введення в нормативно-правову систему регіонального рівня поняття «кібертероризм» як актуального й небезпечного сьогодні явища. Проаналізувавши сутність цього поняття, ми дійшли висновку, що його потрібно вивчати саме через його складники. Згідно з українським законодавством національну безпеку у своїй сукупності формують воєнна, громадська, економічна, екологічна та інформаційна безпеки. Остання ж із переліку становить на сьогодні підґрунтя для формування інших.

Захист об'єктів критично важливої інфраструктури від деструктивних впливів у терористичних цілях ми вважаємо одним із актуальних завдань сучасності. Усвідомлюючи важливість його розв'язання, багато країн координує свою діяльність у цьому напрямку з урахуванням національних інтересів, а також економічних і технологічних можливостей. Хоча не можна не погодитись з тим, що надійний гарантований захист численних, потенційно вразливих для такого роду загроз критично значущих для держави об'єктів, можна забезпечити лише за умови існування налагодженої системи кібербезпеки національного масштабу, який буде впливати на регіональний і, як наслідок, на міжнародний. Дослідження для вирішення такого складного й важливого завдання ведуться в багатьох державах європейського регіону. Характер нових, стратегічно значущих загроз інформаційної безпеки, зокрема й кібертероризму, викликає необхідність посилити політику щодо безпеки інформаційних систем і мереж держав.

У ході проведених нами досліджень були розроблені і вдосконалені важливі інноваційні підходи до боротьби з кібертероризмом, які мають значний вплив на національну безпеку країн європейського регіону.

Таким чином, маємо такі підсумки:

1) уперше було проведено всебічний аналіз кібертероризму, його сутності, опис структури компонентів та обґрунтування його включення до європейської нормативної бази. Це дозволило нам сформулювати нове бачення кібертероризму, що вимагає професійних заходів на національному та регіональному рівнях. Були розроблені та вдосконалені підходи до створення єдиного концептуального бачення кібертероризму в контексті європейського регіону. Зважаючи на державний досвід України була запропонована основа для створення єдиного європейського стандарту боротьби з кібертероризмом. Такий підхід, на нашу думку, забезпечить цілісність та координацію зусиль різних держав у стримуванні та протидії кібертероризму;

2) визначено основні проблеми наукових підходів до з'ясування терміна «кібербезпека», а також недоліки у чинному законодавстві України. Установлено, що визначення терміна часто є занадто загальним або неповним, тому фіксуємо нагальну потребу вдосконалення визначення, що стосується соціально-економічних наслідків кіберзагроз і врахування потреби адаптації до новітніх проблем та викликів;

3) розроблено рекомендації для вдосконалення національної політики кібербезпеки, уключаючи створення посади «кіберомбудсмена», яка б забезпечувала моніторинг і захист прав громадян у цифровому середовищі;

4) запропоновані нові концепції, зокрема «кіберсоціальна адаптація» та «кіберімунітет» суспільства. Такі нові підходи зможуть забезпечити комплексний захист і громадянських, і національних інтересів у кіберпросторі;

5) була вдосконалена міждисциплінарна методологія вивчення кібертероризму, яка передбачає необхідність гармонізації правових підходів і поліпшення міжнародного співробітництва. Запропоновано створення національних підрозділів кіберполіції, оновлення стратегій кібербезпеки та

активний моніторинг критичної інфраструктури, зокрема окреслені напрями для подальших досліджень, уключаючи розвиток нових моделей протидії та гармонізацію кіберполітики.

РОЗДІЛ 2. МЕХАНІЗМИ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ ДЕРЖАВ ЄВРОПЕЙСЬКОГО РЕГІОНУ. ВНЕСОК УКРАЇНИ В ЄВРОПЕЙСЬКУ СИСТЕМУ КІБЕБЕЗПЕКИ ТА ШЛЯХИ ЇЇ РЕФОРМУВАННЯ

2.1. Європейські регіональні засоби протидії кібертероризму

У сучасних умовах інформаційного суспільства кіберпростір стає одночасно важливим ресурсом і вразливою сферою. Згідно із твердженням Джорджа Крістоу [79], колективна безпека кіберпростору стала одним із ключових пріоритетів політики Європейського Союзу, і з цим не можна не погодитись.

Проблема кібертероризму, як ми вже наголошували в попередньому розділі, є однією з найсерйозніших загроз для безпеки Європи в умовах швидкого розвитку цифрових технологій. Нагадаємо, що ми визначили кібертероризм як «свідоме використання інформаційно-комунікаційних технологій для здійснення нападів на критичні об’єкти інфраструктури з метою досягнення політичних або ідеологічних цілей, створення паніки серед населення чи підрив стабільності держави, суспільств і міжнародних структур через маніпуляцію інформаційними потоками, руйнацію цифрових інфраструктур або дестабілізацію стратегічних систем управління». Кібертероризм передбачає застосування інноваційних методів для здійснення терористичних атак, спрямованих на порушення функціонування критичної інфраструктури, поширення паніки та завдання економічних чи соціальних збитків.

Так, ми дійшли висновку, що різноманітність форм і методів, які застосовуються кібертерористами, змушує уряди країн та міжнародні організації активніше співпрацювати в пошуку ефективних механізмів протидії. У цьому контексті Європа демонструє потужний потенціал створення нормативно-правових, інституційних та технічних засобів боротьби з кібертероризмом. Зважаючи на викладене вище, убачаємо, що Європейський

Союз та його держави-члени зіштовхуються з необхідністю розроблення ефективних заходів для протидії цим загрозам.

На сьогодні важливими аспектами є створення єдиних правових норм, удосконалення співпраці між національними та міжнародними органами, а також розвиток технологій і механізмів для швидкого виявлення та реагування на кіберінциденти. Регіональні ініціативи, такі, як діяльність Європейського агентства з кібербезпеки (ENISA) та Центру кібербезпеки ЄС, відіграють важливу роль у координації зусиль і розвитку спільних стратегій для боротьби з кібертероризмом. Однак все одно їх спіткають численні виклики, зокрема, імовірно, через фрагментацію національних підходів, різний рівень готовності до кіберзагроз та недостатню інтеграцію кібербезпеки в загальну стратегію національної безпеки. Щоб підтвердити чи спростувати цю гіпотезу, важливо розглянути наявні на сьогодні європейські регіональні інструменти забезпечення кібербезпеки.

Один із них створений 23 листопада 2001 року: Рада Європи ухвалила Конвенцію про кіберзлочинність [30], яка визначала відповідальність за злочини, пов’язані з комп’ютерними системами та їхніми даними. Конвенція акцентувала увагу на важливості міжнародної співпраці між національними правоохоронними органами, особливо у випадках, коли злочинці та жертви перебувають у різних країнах, підкреслюючи необхідність боротьби із кіберзлочинами. Конвенція також установлювала зобов’язання для держав-учасниць щодо розвитку національного законодавства у ключових напрямках, наприклад: забезпечення конфіденційності та доступності комп’ютерних систем і даних, боротьба з порушенням авторських прав та використання комп’ютерного обладнання для злочинних цілей. Попри це, однак, її дії мали обмежений характер, створюючи серйозні загрози для громадської та національної безпеки. Імовірно, це одна із причин зростання кіберзлочинності в Європі.

Із розумінням цього у 2003 році до Конвенції про кіберзлочинність був прийнятий Перший Додатковий протокол [80], який мав на меті розширити

положення Конвенції у світлі зростання кількості расистської та ксенофобської пропаганди в кіберпросторі. У Протоколі йшлося про потребу чіткого правового інструмента для вирішення зазначених проблем шляхом криміналізації – розпалення ненависті за расовою, етнічною або національною належністю. Розглядаючи цей Протокол, маємо зазначити, що, з одного боку, цей крок зміцнює законодавчу базу для запобігання зловживання свободою слова від загрози громадському порядку, однак з іншого, – викликає певні суперечки щодо обмежень свободи слова в демократичних суспільствах.

Підписання Другого Додаткового протоколу відбулося в 2022 році [81] і вважається черговим кроком у розвитку міжнародного співробітництва у сфері кібербезпеки. Його мета – забезпечення більш ефективного способу отримання електронних доказів. Цифровізація суспільства спричинала збільшення кількості доказів, які зберігаються у формі електронних даних і часто перебувають в різних юрисдикціях. А коли правоохоронні органи потребують таких даних, вони стикаються з проблемами юридичних перешкод, пов'язаних з відмінностями в законодавстві в різних країнах. Другий Протокол якраз і спрямований на усунення цих бар'єрів, забезпечуючи швидший та ефективніший обмін даними між країнами. Уважаємо такий аспект важливим з точки зору підвищення своєчасності та ефективності розслідувань, але він також викликає питання щодо захисту прав людини і, зокрема, конфіденційності персональних даних.

Аналіз цих двох Додаткових Протоколів показує, що вони є важливою частиною розвитку міжнародної системи для боротьби з кіберзлочинністю, але вони також підкреслюють складність досягнення балансу між безпекою та свободою в сучасному інформаційному суспільстві. Перший Протокол спрямований на боротьбу з конкретними видами злочинів на ґрунті ненависті, натомість другий зосереджений на процедурних аспектах отримання доказів, необхідних для розслідування кіберзлочинів. Обидва Протоколи, на наш погляд, відображають різні, але взаємопов'язані аспекти кібербезпеки:

контроль вмісту інформаційних потоків і надання правових механізмів для ефективного переслідування кіберзлочинців.

Прикметно, що жоден Додатковий Протокол не містить положень, прямо пов'язаних із тлумаченням кібертероризму. Ми вважамо це значним недоглядом, оскільки, зважаючи на серйозність загрози кібертероризму для національної та міжнародної безпеки, це явище має бути різнобічно вивчене з метою ефективного йому протистояння, про що ми неодноразово зауважували й підкріплювали нашу позицію прикладами. Оскільки країни все більше покладаються на цифрову інфраструктуру, атаки, спрямовані на дестабілізацію таких систем, можуть мати катастрофічні наслідки. І це також є доказом правильності наших положень.

Відсутність чіткого міжнародно-правового механізму боротьби з кібертероризмом залишила прогалину в колективній безпеці, що не дозволяє ефективно координувати свої зусилля для боротьби. Кібертероризм, у нашому розумінні, потребує окремих законодавчих ініціатив, які б ураховували його конкретні особливості, уключаючи мотиви, масштаб впливу на суспільство та конкретні обставини, за яких організовуються такі атаки. Згідно з цим припускаємо, що недооцінювання загрози кібертероризму в межах Додаткового Протоколу до Будапештської конвенції ставить під сумнів цілісність підходу до забезпечення глобальної кібербезпеки та потребує подальших зусиль міжнародної спільноти щодо створення відповідних механізмів боротьби з кіберзагрозами.

Аналізуючи наявні інструменти боротьби з кіберзагрозами, відзначимо, що одним із перших практичних кроків у боротьбі з кібертероризмом і кіберзлочинністю стало створення 13 березня 2004 року Агентства з мережевої та інформаційної безпеки ЄС ENISA. Це агентство виконує постійний моніторинг мереж і вносить зміни до вже прийнятих правових актів, аби регулювати механізми протистояння та запобігати загрозам у сфері інформаційних технологій. ENISA, створене у 2004 році, до прийняття Cybersecurity Act, діяло як дорадчий орган, зосереджуючись переважно на

рекомендаціях та розробці стратегій кібербезпеки. Проте Регламент (ЄС) 2019/881 [70], який ми обговорювали вище, значно посилив повноваження агентства.

Основною метою ENISA нині є забезпечення безперебійного функціонування європейського регіону через надання консультацій, проведення оцінок ризиків і допомогу державам-членам. Щорічні зустрічі з політиками, ІТ-експертами та вченими допомагають удосконалити навички безпечного використання Інтернету та підготувати фахівців для протидії кібератакам різного масштабу [82, с. 120].

Визнаючи загрози, пов'язані з Інтернетом, Європейське співтовариство, зокрема ОБСЄ, ухвалило ще один документ, а саме: Рішення Ради міністрів №7/06 «Боротьба з використанням Інтернету з терористичною метою» [83]. Цей документ став важливим кроком у забезпеченні безпеки в Європі, окресливши напрями для посилення діяльності держав-учасниць у боротьбі з терористичними загрозами в Інтернеті. Він також підкреслив важливість захисту критично важливих інформаційних інфраструктур і закликав до приєднання європейських країн до Конвенцій Ради Європи, які сприяють боротьбі з кіберзлочинністю. Однак, на нашу думку, цей документ також має бути оновлений відповідно до сучасних загроз у кіберпросторі, зокрема доповнений положеннями про боротьбу з кібертероризмом, адже розширення меж боротьби за допомогою політичного інструментарію значно підсилить наявні механізми протиборства.

ОБСЄ [84] відіграє важливу роль у врегулюванні кібербезпеки, закладаючи основи для співпраці між країнами-учасницями та запобігаючи конфліктам у кіберпросторі. Заходи із зміцнення довіри спрямовані на зниження ризику кіберінцидентів, що важливо з огляду на загрози національній безпеці, які створює цифрова взаємозалежність країн. Підтримка національних стратегій кібербезпеки та міжнародна співпраця з ООН, ЄС і НАТО підкреслюють бажання ОБСЄ консолідувати міжнародні зусилля з протидії кіберзагрозам. З політичної точки зору така діяльність допомагає зміцнити

довіру між країнами, сформувати загальноєвропейську стратегію кібербезпеки та підвищити стійкість до можливих кібертерористичних атак, зміцнюючи таким чином стабільність всього регіону.

Украй важливим для європейської кібербезпеки став 2013 рік, коли країни ЄС ухвалили стратегію кібербезпеки, яка стала важливим кроком у зміцненні регіональної безпеки. Стратегія встановила «пріоритетну міжнародну політику у сфері кіберпростору для ЄС» у п’яти пріоритетах:

– забезпечення стійкості кіберпростору Європейського союзу;

– скорочення кількості кіберзлочинів;

– розвиток політики кібероборони, яка становить сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, здійснюваних у кіберпросторі та спрямованих на забезпечення захисту суверенітету й обороноздатності держави, запобігання виникненню збройного конфлікту й відсіч збройній агресії на основі спільної політики безпеки й оборони Європейського союзу;

– розвиток виробничо-технологічних ресурсів для забезпечення кібербезпеки;

– створення узгодженої всіма членами Євросоюзу міжнародної політики з кібербезпеки з іноземними партнерами для підвищення кооперації в цій галузі з третіми країнами.

– Згідно зі стратегією, фінансові, транспортні та енергетичні компанії повинні розробити і вжити заходів з протидії можливим кіберзагрозам. Як наслідок – понад 40 тис. європейських організацій зобов’язані звітувати про спроби кібератак, а найважливіші для економіки й інфраструктури підприємства повинні доводити надійність свого захисту. Стратегія стала першим всеохопним документом ЄС у цьому напрямку. Документ містить усі аспекти кіберпростору: внутрішній ринок, правосуддя, внутрішню та зовнішню політику [85].

У 2020 було прийнято рішення про оновлення Стратегії на період 2020 - 2030 рр. [86]. Нова Стратегія означала великий крок уперед у розвитку політики Європейського Союзу в умовах зростання кількості загроз у цифровому середовищі. З політичної точки зору, на нашу думку, цей документ є відображенням прагнення ЄС забезпечити свою стратегічну автономію та посилити вплив на глобальні стандарти кібербезпеки.

Порівняно зі Стратегією 2013 року, яка зосереджувалася на нормативній базі та координації зусиль держав-членів, нова Стратегія, на наш погляд, має більш прагматичний характер і орієнтована на конкретні дії, спрямовані на підвищення стійкості до кіберзагроз. Якщо раніше основний акцент стосувався правових основ кібербезпеки та міжнародного співробітництва, то оновлена Стратегія спрямована на розвиток внутрішніх спроможностей ЄС.

Стратегія 2020 року чітко акцентує увагу на зміцненні кіберстійкості критичних інфраструктур, це свідчить про зміну пріоритетів від реагування на загрози до їх попередження та створення інструментів, які можуть забезпечити довготривалу стійкість. На нашу думку, це є відповіддю на значну кількість кібератак на критичну інфраструктуру країн Європи, серед яких варто згадати, насамперед такі:

1) атака на телевізійний канал TV5Monde у 2015 році [87], яка була націлена на порушення інформаційного простору, створення паніки та поширення ідеологічних меседжів. Це є типовими ознаками кібертероризму, оскільки мета полягала в залякуванні населення та підриві довіри;

2) атаки на енергетичну інфраструктуру України 2015– 2016 рр. [88], про які ми згадували в попередньому розділі, що теж можна класифікувати як кібертероризм, оскільки вони мали на меті підрив критичної інфраструктури, що є життєво важливою для нормального функціонування суспільства, а також викликали масову паніку серед населення;

3) атака на німецький Бундестаг у 2015 році [89], спрямована на політичну дестабілізацію країни та підрив демократичних інститутів;

4) NotPetya – 2017 рік [90], метою було руйнування економічної інфраструктури, що завдало значних збитків і викликало серйозні збої у функціонуванні великих підприємств. Ми визначаємо таку атаку як кібертероризм через її деструктивний характер, спрямований на дестабілізацію економіки;

5) WannaCry у тому ж 2017 [91], кібератака на систему охорони здоров'я, яка була спрямована на дестабілізацію критично важливої інфраструктури, що становило загрозу життю та здоров'ю людей;

6) атака на британський парламент 2017 року [92, 93], що теж можна класифікувати як кібертероризм, адже вона мала політичний характер і була спрямована на викрадення даних з метою політичного тиску та шантажу, а її мета – залякування політиків і підрив довіри до демократичних інститутів;

7) DDoS-атаки на фінансові установи в Нідерландах у 2018 році [94], які мали на меті дестабілізацію фінансової системи країни та створення паніки серед населення. На нашу думку, це також можна класифікувати як кібертероризм, оскільки атака мала соціально-економічний вплив;

8) із 2018 по 2020 рр. масштабних атак зазнавали лікарні Чехії. Протягом трьох років постраждали легенева лікарня в Янові, лікарні у Брно та Бенешові, психіатричний госпіталь в Космоносах, а також лікарні Острави та Пардубицького, багато з кібератак були здійснені російськими вірусами [95, 96, 97];

9) протягом 2019 – 2020 рр. лікарні в Іспанії теж були вражені кібератаками [98], унаслідок яких було ускладнено догляд за пацієнтами, оскільки неможливо було отримати доступ до медичних записів, надсилати електронні листи, вводити дані або виконувати тести, що вимагають комп’ютерної фіксації;

10) атака на німецькі муніципалітети (2019 рік [99]) була спрямована на дестабілізацію місцевої влади та надання послуг громадянам. Зважаючи на масштаби атаки та її вплив на суспільство, вона може розглядатися як акт кібертероризму, метою якого було залякування та порушення стабільності.

11) у 2020 році хакери у Фінляндії викрали та оприлюднили конфіденційні нотатки психотерапевтичних сеансів десятків тисяч пацієнтів. Багато пацієнтів повідомили, що хакери шантажували їх електронною поштою [100].

Отже, як бачимо, з 2014 по 2020 роки збільшується кількість атак на критично важливі інфраструктури: під прицілом енергетика, охорона здоров'я, фінансові та державні установи. Ці атаки можна визнати актами кібертероризму, оскільки вони цілеспрямовано дестабілізують суспільство, створюють загрози життю людей та спричиняють паніку. Основними цілями цих атак є дестабілізація критично важливих систем, підрив довіри до державних інституцій і загроза національній безпеці. Це підкреслює необхідність зміцнення колективної кібербезпеки Європи, розширення співпраці між державами– членами ЄС і запровадження єдиної стратегії підвищення кіберстійкості та боротьби з кібертероризмом.

Це важливий політичний сигнал, оскільки він свідчить про готовність ЄС протистояти викликам, які виникають через глобальну конкуренцію в галузі високих технологій, і посилити власну позицію на міжнародній арені. У цьому сенсі стратегія має не лише безпековий, але й геополітичний вимір, адже розвиток технологій та інфраструктури є ключовим фактором збереження політичного впливу у глобальному масштабі.

Що стосується практичного впровадження заходів кібербезпеки, то відзначимо також, що в рік прийняття першої Стратегії було створено Європейський центр боротьби з кіберзлочинністю (ЕС3) [101], який став ключовим інститутом у цій сфері. Центр заснований на базі Європолу, активно підтримує держави-члени в розслідуванні кіберзлочинів, здійснюючи оперативну та аналітичну підтримку. З моменту свого створення ЕС3 брав участь у численних операціях, пов'язаних із арештом кіберзлочинних організацій. Для розв'язання найзначніших міжнародних інцидентів ЕС3 співпрацює з групою кіберрозвідки CIT, яка забезпечує збір і аналіз інформації про кіберзлочинність з різних джерел, а Об'єднана цільова група боротьби з

кіберзлочинністю J-CAT підтримує практичне спрямування наведених структур. Діяльність вище наведених організацій також свідчить про активну позицію ЄС у протидії кіберзлочинності та забезпеченні безпеки своїх громадян [102].

Важливо підкреслити, що питання кібербезпеки в Європейському Союзі регулюються ще одним документом – Директивою №2016/1148, ухваленою 6 липня 2016 року, яка встановлює заходи захисту мереж та інформаційних систем у критичних секторах (банківській справі, енергетиці, транспорті та охороні здоров'я). Директива зобов'язує держави-члени розробити національні стратегії кібербезпеки, створити контрольні органи та мережі реагування на інциденти [71].

Прийняття [103] Директиви про мережеву та інформаційну безпеку NIS2 у 2022 році є важливим кроком у зміцненні кібербезпеки ЄС. Метою NIS2 виступає посилення захисту критичної інфраструктури та мережевих систем ЄС, адаптація до нових викликів і загроз, що виникають у сучасному цифровому середовищі.

Директива NIS2 значно розширює сферу застосування порівняно з першою Директивою NIS і охоплює не лише традиційні ключові сектори, такі, як енергетика, транспорт і фінанси, але й нові – цифрові послуги, водопостачання, виробництво продуктів харчування та сектор інформаційних технологій. Такий підхід, на наш погляд, демонструє політичну готовність ЄС у питаннях кібербезпеки та визнання нової реальності: кіберзагрози стають глобальними та охоплюють не лише державний, а й приватний сектори.

Із політичної точки зору NIS2 є інструментом забезпечення стратегічного зміцнення колективної безпеки ЄС. Такий підхід є важливим, оскільки сучасні кіберзагрози не знають кордонів, а створення єдиної європейської мережі обміну інформацією та створення спільного середовища безпеки, в якому кожна держава-член відіграє свою роль у забезпеченні загальної стійкості, є вкрай нагальним.

Директива також наголошує на важливості зобов'язань компаній повідомляти про кіберінциденти. Це не тільки допомагає швидко реагувати на загрози, але й сформувати загальну картину європейської кібербезпеки. Цей проактивний підхід допомагає уникнути фрагментації та дозволяє швидше мобілізувати ресурси для реагування на великі інциденти.

Важливим елементом також є Європейська схема сертифікації кібербезпеки на основі загальних критеріїв EUCC [104]. Вона визначає правила і стандарти для оцінки ефективності кіберзахисту. А це своєю чергою сприяє зміцненню довіри громадян країн Європейського союзу до цифрових продуктів і послуг, необхідних для функціонування Єдиного цифрового ринку. Однак, на нашу думку, добровільний характер такої сертифікації та знов-таки різні підходи держав-членів створюють виклики, які потребують політичної волі для їх подолання.

Загалом EUCC є важливим кроком до зміцнення кібербезпеки, єдності та довіри в ЄС, а значить, відповідає стратегічним цілям щодо захисту кіберпростору.

Ще одним сертифікаційним елементом є Загальний регламент захисту даних GDPR. Це регламент ЄС, який регулює оброблення персональних даних [105]. Його мета полягає в тому, щоб забезпечити захист особистих даних громадян ЄС, надати їм контроль над своїми даними та гармонізувати нормативні підходи держав-членів. GDPR є обов'язковим для всіх країн ЄС і Європейської економічної зони (ЄЕЗ) і головне – має екстериторіальну дію. Такий підхід, на нашу думку, демонструє прагнення ЄС розширити свій вплив на глобальне цифрове регулювання та встановити стандарти, яких міжнародні компанії повинні дотримуватися. І на сьогодні це є політично важливо, оскільки таким чином ЄС фактично встановлює межі глобального регулювання захисту даних.

Україна, рухаючись до євроінтеграції, також адаптує своє законодавство до вимог GDPR [106]. Це важливий політичний крок для України, оскільки наближення до європейських стандартів захисту даних є частиною ширшої

стратегії інтеграції з ЄС. Імплементація положень GDPR в Україні не лише підвищує рівень захисту громадян, а й зміцнює її позиції в переговорах з європейськими партнерами, демонструючи готовність відповідати високим вимогам і гармонізувати українське правове поле з європейськими нормами. Це є позитивним кроком, що зміцнює політичну стабільність і довіру до України як надійного партнера в час, коли цифрові права та безпека стають все більш важливими в міжнародних відносинах.

Європейська комісія із захисту даних EDPB [107] відіграє важливу наглядову роль у координації дій органів із захисту даних у кожній країні ЄС для забезпечення послідовного застосування GDPR. Однак, на нашу думку, EDPB виконує не лише технічну, а й важливу політичну функцію, оскільки її діяльність спрямована на уніфікацію стандартів захисту даних у різних країнах, тому консолідація ЄС як єдиного регулювального простору, є важливим кроком. У сучасних умовах, коли країни-члени мають власні пріоритети та політичні розбіжності, діяльність ЄДПБ може підтримувати баланс між національними суверенітетом та загальноєвропейськими інтересами. Тож з позиції нашого аналізу функція EDPB як арбітра між органами із захисту даних кожної країни має особливу політичну вагу, оскільки сприяє запобіганню суперечок між державами-членами і забезпечує цілісність європейської системи.

Отже, як бачимо, на сьогодні в Європейському Союзі значно зросла політична активність щодо посилення кібербезпеки у відповідь на загрози в цифровій сфері, що постійно зростають. Європейська Комісія разом із іншими європейськими інституціями намагається активно розбудовувати нову інфраструктуру кіберзахисту, зокрема різні механізми співпраці, запобігання та раннє виявлення загроз. Цей процес можна розглядати як важливий політичний проєкт, спрямований не лише на підвищення технічних стандартів, але й на зміцнення суверенітету та єдності ЄС перед обличчям нових викликів.

У цьому контексті створення національних CSIRT, Computer Security Incident Response Teams, спільно з CERT-EU є важливим кроком на шляху

впровадження загальноєвропейського підходу до забезпечення кібербезпеки. Ці структури сприяють швидкому реагуванню на кібератаки та дозволяють координувати зусилля між державами-членами. Їхня діяльність відображає нову політичну реальність, у якій безпека в цифровому просторі стала пріоритетом на найвищих рівнях прийняття рішень ЄС.

Ці групи займаються не лише технічними аспектами кіберзахисту, а й допомагають підвищити рівень взаємної довіри між країнами ЄС, оскільки координація у сфері кібербезпеки передбачає обмін конфіденційною інформацією та спільне розуміння загроз. Це також є політичним показником зміцнення внутрішньої солідарності ЄС та колективної здатності держав реагувати на зовнішні виклики, які можуть мати дестабілізуючий вплив на весь регіон.

Ще одним важливим компонентом Європейської платформи кібербезпеки є Європейська організація з кібербезпеки ECSO – приватний партнер Європейської Комісії. ECSO відіграє ключову роль у розвитку державно-приватного партнерства з кібербезпеки. Ми розглядаємо інтеграцію приватного сектору в політику безпеки ЄС як стратегічно виважене рішення, оскільки більшість критичної інфраструктури перебуває у приватній власності. Це може означати, що політика кібербезпеки має враховувати інтереси приватних компаній, залучення яких може забезпечити більш адаптивні та ефективні механізми захисту. Важливість співпраці ЄС з ECSO полягає в тому, що таке державно-приватне партнерство демонструє здатність ЄС реагувати на виклики часу шляхом мобілізації державних і приватних ресурсів, а також сприяє формуванню нових політичних відносин між національними урядами, європейськими інституціями та приватними зацікавленими сторонами, що веде до кращої стійкості в кіберпросторі ЄС. Важливий політичний вимір ECSO полягає в тому, що для реалізації спільних стратегій із покращення кібербезпеки організація об’єднує різні зацікавлені сторони з усього ЄС, уключаючи підприємства, академічні установи та уряди. Ця співпраця не тільки допомагає покращити кіберзахист, але й сприяє зміцненню політичної

солідарності та створенню єдиного простору для взаємодії та прийняття рішень щодо цифрової безпеки. Однак слід зазначити, що, на нашу думку, такі амбіції не позбавлені проблем саме того, що будь-яка взаємодія між державним і приватним секторами вимагає політичного компромісу, особливо щодо управління інформаційною безпекою та розподілу відповідальності за захист критичної інфраструктури. Крім того, різноманітність правових і технічних систем між державами також ускладнює координацію та створює перешкоди для ефективного обміну інформацією. У цьому контексті ЄС стикається з проблемою скоординованого підходу, який вимагає величезної політичної волі та співпраці.

Таким чином, посилення кібербезпеки в ЄС є складним і багатогранним процесом, що містить технічні, політичні та економічні компоненти. Інвестиції в запобігання, раннє попередження та координацію дій мають не лише суто безпековий вимір, але також є механізмами зміцнення європейської солідарності та демонстрації об'єднаності зусиль перед обличчям нових загроз. Залучаючи такі інституції, як ECSO, і співпрацюючи в межах CSIRT і CERT-EU, ЄС підкреслює свою здатність розробляти інноваційні підходи для забезпечення колективної кібербезпеки, що є ключовим елементом підтримки стабільності та безпеки в усьому регіоні.

На відміну від ЄС протидія кіберзагрозам у НАТО визначається поняттями «кібероборона» та «кіберзахист», у яких, як і в ЄС, наголошено на напрямі захисту безпеки й включено до переліку основних цілей колективної оборони, а не внутрішньої безпеки.

Сучасні кібератаки спонукають Північноатлантичний альянс постійно розширювати свої методи протидії кіберзагрозам. НАТО активно співпрацює з країнами-партнерами для захисту власних мереж і зміцнення можливостей протистояти кіберзагрозам. Співпраця між ЄС та НАТО базується не лише на тому, що 22 країни є членами обох організацій, а й на спільному прагненні заповнити прогалини в безпекових можливостях, особливо в кіберсфері.

Ключовою віхою у співпраці ЄС та НАТО стало створення у 2013 році Центру кіберзахисту НАТО при Європейському оборонному агентстві, що сприяло обміну інформацією та спільним тренуванням. Спільні навчання, зокрема Cyber Coalition та Cyber Europe, стали платформою для розвитку спільних заходів у кіберборотьбі [72].

Зауважимо, що актуальні виклики, пов’язані з російською агресією проти України, стимулюють поглиблення співпраці між ЄС та НАТО. У 2016 році було підписано технічну угоду між ЄС та НАТО про співпрацю в галузі кіберзахисту, що налагодило практичну взаємодію між CERT– EU та NCIRC [108].

Окрім цього, існує Hybrid CoE як міжнародна мережа, яка займається системним підходом до боротьби з гібридними загрозами [109]. Вона об'єднує 36 країн-членів, зокрема країни ЄС і НАТО, а її місія полягає в покращенні безпеки шляхом надання досвіду та навчання для протидії гібридним загрозам.

На нашу думку, такі центри передового досвіду стали важливими механізмами політичної інтеграції а галузі безпеки. Спільні тренінги, які проводять центри, дозволяють країнам виробити спільне розуміння викликів і шляхів їх подолання. Такий центр, як наприклад Hybrid CoE, є своєрідним «містком» між європейськими та трансатлантичними структурами, забезпечуючи синергію у протидії гібридним загрозам. Hybrid CoE залучає державні установи, приватний сектор і наукові кола для формування комплексного підходу до протидії гібридним загрозам, а також підтримує дослідницькі та навчальні програми для підвищення готовності держав до боротьби з гібридними загрозами. Ми вважаємо, що така практична підготовка – це не лише механізм обміну досвідом та навчання, але й інструмент формування спільних політичних підходів до забезпечення стійкості та стримування. У сучасних умовах, коли гібридні загрози стають дедалі більш поширеними, роль Hybrid CoE полягає в забезпеченні не тільки фізичної, але й політичної безпеки демократичних держав, захисту їх від підривної діяльності та стійкості до зовнішніх впливів.

Досить вагомим для забезпечення кібербезпеки став Талліннський механізм [110,111,112], заснований у 2023 році. Він покликаний зміцнити кібербезпеку України від постійних гібридних атак з боку Росії. Механізм об'єднує кілька великих країн-партнерів, зокрема Україну, Канаду, Данію, Естонію, Францію, Німеччину, Нідерланди, Польщу, Швецію, Велику Британію та США. Його метою є координація міжнародної підтримки шляхом розвитку технічних знань і людських можливостей для забезпечення швидкого реагування на кібератаки та підвищення кіберстійкості України. Головною передумовою для створення Талліннського механізму стало посилення кібератак на Україну та збільшення втрат, яких зазнає її критична інфраструктура, державні установи, фінансовий та інформаційний сектори.

Талліннський механізм має стратегічне значення не лише для України, а й для Європи загалом. Спрямовані на українську інфраструктуру кібератаки часто впливають на інші країни, знов-таки підкреслюючи транснаціональний характер сучасних кіберзагроз. Міжнародна платформа, створена в межах цього механізму, є ефективним інструментом для об'єднання країн у їх зусиллях щодо забезпечення безпеки мережі. Водночас механізм є частиною спільного реагування на загрози, що допомагає встановити нові стандарти. Варто зазначити, що ефективність Талліннського механізму багато в чому буде залежати від зусиль усіх залучених сторін. Україна має продовжувати адаптацію власної інфраструктури до сучасних викликів та підготовки нових спеціалістів. У цьому контексті міжнародне співтовариство, на наш погляд, має підтримувати Україну як важливого партнера у боротьбі з кіберзагрозами та продовжувати діяти солідарно. Лише комплексні зусилля, інноваційні підходи та стратегічне планування зможуть забезпечити довгострокову стійкість кіберпростору, що є основою стабільності в Україні та європейському регіоні загалом.

Нарешті, не можна не згадати про аспект криміналізації кіберзлочинності, адже це є значним показником ефективності всіх заходів, які вживаються. За покарання кіберзлочинців відповідає EJCN [113] – створена у 2016 році

Європейська судова мережа з питань кіберзлочинності. Ця організація є важливим компонентом, який не лише формує правову базу для боротьби з кіберзлочинністю, а й слугує інструментом для зміцнення політичної інтеграції країн ЄС у зазначеномунапрямку. EJCN тісно співпрацює з Євроюстом [114,115], який у свою чергу здійснює і координацію дій правоохоронних органів різних держав з питань розслідування кіберзлочинів, допомагає в проведенні розслідувань за запитом відповідного органу публічної влади держав, надає правоохоронним органам цих країн інформацію про проведені розслідування щодо кіберзлочинців. Така співпраця, на нашу думку, не лише сприяє покращенню судової координації, але й сприяє розробленню спільного політичного підходу до питань кіберпростору. Знов- таки, така взаємодія символізує бажання ЄС зміцнити єдність і захистити свої інтереси перед обличчям кіберзагроз, які можуть дестабілізувати Союз.

Забезпечення координації між судовими системами різних країн ЄС також підкреслює той факт, що питання кібербезпеки вже давно є пріоритетними на найвищих рівнях прийняття рішень та демонструє, що кіберзлочинність є не лише кримінальною проблемою, а й загрозою національній безпеці та політичній стабільності держав. Зусилля EJCN та Євроюсту в цьому напрямку сприяють розробці спільної політики безпеки, яка включає координацію дій, обмін інформацією та розробку спільних підходів, спрямованих на протидію кіберзагрозам. Політична важливість цих структур полягає також в їхньому внеску в консолідацію європейської політичної культури у сфері кібербезпеки. Це особливо важливо в умовах збільшення кількості гібридних атак, коли кіберзагрози стають невід'ємною частиною інструментарію політичного впливу на країни. Солідарність, яку демонструють держави як в межах EJCN, так і за підтримки Євроюсту, стає ключовим фактором у підтримці європейської єдності перед обличчям зовнішніх і внутрішніх викликів.

Звичайно, інтеграція кібербезпеки пов'язана з багатьма проблемами, зокрема, різними рівнями технічної готовності, національними пріоритетами та

суверенними підходами держав, що може уповільнювати процес координації. Однак існування та ефективна діяльність EJCN та Євроюсту демонструє політичну волю подолати ці перешкоди та сформувати спільний фронт проти кіберзлочинності. Ці інституції демонструють готовність Європи відігравати активну роль у формуванні міжнародного порядку в цифровій сфері, де закон, порядок і співпраця стають інструментами для забезпечення національних інтересів країн і колективної безпеки всього європейського простору.

Отже, проаналізувавши європейські регіональні засоби протидії кібертероризму, маємо зазначити, що комплексно вони формують багаторівневу систему, яка поєднує правові, технічні та організаційні механізми захисту. ЄС перебуває на роздоріжжі інституційних викликів і загроз, що виникають через активізацію кібертерористичної діяльності, яка кидає виклик традиційним основам національної безпеки та стабільності.

З огляду на це, ми вважаємо за необхідне сформулювати Третій Додатковий протокол до Будапештської конвенції, спрямований саме на протидію кібертероризму. Такого роду рішення спричинене активним поширенням кібертерористичних атак на енергетичні мережі, транспортні системи, фінансові установи й державні служби з метою дестабілізації критичної національної інфраструктури та створення загрози національній і міжнародній безпеці, що й було підкреслено у сформульованому нами визначенні. Такі атаки, як збій в електромережах чи транспорті, атаки на фінансові установи та систему охорони здоров'я, спроби дестабілізації уряду тощо можуть мати катастрофічні наслідки, а це ще раз підкреслює необхідність кращої координації між країнами для реагування на загрози кібертероризму.

Третій Додатковий Протокол має містити конкретні інструменти для боротьби з кібертероризмом. Одним із таких інструментів могло б стати створення «кібертрибуналу» – міжнародного суду з питань кіберзлочинності, який би діяв дистанційно та давав можливість реагувати на кіберінциденти в реальному часі, або задля досягнення цієї мети розширити повноваження

Міжнародного суду ООН та/або Міжнародного Кримінального Суду (на це, як нам видається, існує декілька причин).

Переконливим аргументом щодо того, чому кіберзлочинність має бути передано під юрисдикцію Міжнародного Суду ООН, є відсутність ефективного механізму міжнародної відповідальності. Транснаціональний характер більшості кібератак ускладнює розслідування на національному рівні та ставить під сумнів здатність держав ефективно переслідувати злочинців, особливо якщо є підозри, що їхня діяльність пов'язана з державними органами в інших країнах. Міжнародний суд ООН може слугувати платформою для обговорення та вирішення таких суперечок, а також інструментом для підвищення рівня співпраці та довіри між державами з питань кібербезпеки.

Крім того, перенесення кіберзлочинності під юрисдикцію Міжнародного Суду ООН допоможе створити єдиний міжнародно-правовий підхід до цієї проблеми. Наразі існують значні відмінності в тому, як національні закони тлумачать і переслідують кіберзлочинність, створюючи правові прогалини та можливості для кіберзлочинців використовувати «лазівки» в юрисдикції, щоб уникнути відповідальності. Міжнародний Суд ООН міг би сприяти гармонізації підходів до визначення кіберзлочинності та розробці загальноприйнятих стандартів, що зменшило б правову невизначеність та підвищило ефективність глобальної боротьби з кіберзлочинністю.

Ще одним важливим аспектом є необхідність запобігання ескалації конфліктів між державами через кіберзлочинність. Кібератаки можуть бути використані як інструменти провокації, спрямовані на дестабілізацію міжнародних справ і створення умов для відкритого конфлікту. Як установа з міжнародною легітимністю, Міжнародний Суд Організації Об'єднаних Націй може виступати посередником у таких конфліктах, виявляти винних у кібератаках і запобігати подальшій ескалації конфліктів.

Варто також зазначити, що залучення Міжнародного Суду ООН до розгляду кіберзлочинності, на нашу думку, сприятиме більшій прозорості державних відносин у сфері кібербезпеки. Сьогодні держави часто вдаються до

«таємних дій» в кіберпросторі, ускладнюючи доведення своєї відповідальності та створюючи атмосферу недовіри. Існування міжнародних судових механізмів дозволило б країнам відстоювати власні інтереси на міжнародному рівні, а не «тіньовими» засобами досягати цілей.

Таким чином, важливим кроком у створенні ефективної міжнародної системи боротьби з кіберзагрозами вважаємо перенесення кіберзлочинності в юрисдикцію Міжнародного суду ООН. Це змогло б забезпечити вирішення суперечок у сфері кібербезпеки, сформувати єдиний правовий підхід щодо реагування на кіберзлочини та запобігти ескалації конфліктів через кіберінциденти. Ураховуючи масштаби сучасних кіберзагроз, міжнародне співтовариство має діяти разом і використовувати всі доступні інструменти для забезпечення безпеки, миру та стабільності.

Уважаємо також за доцільне в межах запропонованого Третього протоколу ввести такий важливий компонент, як «Конвенцію про взаємні кіберзобов'язання», тобто міжнародний договір, у якому б країни-учасниці зобов'язалися швидко активувати спільні заходи кіберзахисту в разі кібертерористичної атаки на одну із сторін. Така угода слугувала б аналогією «колективної оборони» в кіберпросторі, що значно підвищило б ефективність скоординованої відповіді на атаки. Влучим додатковим інструментом має стати «політичний тригер міжнародного реагування», який автоматично запускає серію політичних заходів або запровадження тимчасових міжнародних правил для посилення безпеки, коли кіберзагрози досягають певного рівня (наприклад, великомасштабна кібератака). Такий механізм забезпечив би швидкість і ефективність прийняття рішень, необхідних для реагування на загрози.

Доцільно було б також, на наш погляд, започаткувати «політичний механізм кіберпосередництва» у вигляді створення органу-посередника в кіберпросторі, який діятиме як нейтральна сторона для вирішення конфліктів між країнами у випадках підозри в кібератаках або підтримці кібертероризму. Це з високою мірою вірогідності допомогло б запобігти ескалації конфліктів і сприяло б мирному вирішенню суперечок у кіберпросторі.

До важливих заходів також необхідно було б додати так званий «кіберімунітет для критичної інфраструктури». За своїми ознаками він схожий із тим кіберімунітетом, про який ішлося в попередньому розділі, тільки вже для технологічних об'єктів, однак відмінність між ними в тому, що ця концепція має базуватися на угодах про недоторканність певних цифрових ресурсів, подібно до дипломатичного імунітету, але в кіберпросторі. Прогнозуємо, що такий крок підвищить рівень захисту критично важливих систем і забезпечить їх тривалу недоторканність.

Ще один напрямок, який потребує уважного розгляду, – це концепція «мережевого нейтралітету», яка б передбачала створення зони нейтралітету, подібної до демілітаризованої, де всі країни погоджуються не проводити жодної кіберактивності, яка могла б бути сприйнята як загроза чи агресія, що теж з високою вірогідністю підвищить рівень довіри та безпеки в міжнародних відносинах.

Пропонуємо також започаткувати «політичний кіберкарантин». Оскільки розвиток кіберзагроз можна порівняти з пандемією вірусу [116], це дозволило б визначати країни чи регіони, які активно підтримують кібертероризм, «карантинними зонами», які автоматично відключаються від ресурсів глобальної мережі на обмежений період часу, щоб нейтралізувати загрозу та запобігти її подальшому поширенню.

Отже, формулювання Третього Додаткового протоколу до Будапештської конвенції, спеціально спрямованого проти кібертероризму, є необхідним кроком для забезпечення міжнародної безпеки в епоху цифрових технологій. Протокол має поєднувати низку інноваційних механізмів, спрямованих на підвищення ефективності боротьби з кібертерористичними загрозами, забезпечення швидкого реагування та зміцнення міжнародної солідарності. На сьогодні, переконані, належний рівень кібербезпеки та захисту від терористичних загроз у цифровому просторі можна забезпечити лише за умови чіткої координації та готовності до співпраці на глобальному рівні.

Зважаючи на наш аналіз, можемо зробити висновок, що реальний успіх у боротьбі з кібертероризмом можливий лише за умови досягнення політичної консолідації в цій сфері на міжнародному рівні, і це є 100% доказом тієї гіпотези, яку ми сформулювали на початку. Кібертероризм як нова загроза вимагає адаптивних стратегій, заснованих на інноваційних механізмах колективного захисту, кіберпосередництві та міжнародних інструментах реагування та захисту. Це означає, що кіберпростір має бути переосмислений як політичний вимір суверенітету та безпеки, причому кожна країна має виступати не лише суб'єктом, а й відповідальним у всій системі оборони.

Саме тому формування нової політико-правової системи в галузі кібербезпеки, у тому числі боротьби з кібертероризмом, є необхідним кроком для збереження миру та стабільності в епоху цифрових технологій. Це не просто технічний аспект безпеки, а виклик, який має прямий вплив на національний суверенітет, стабільність політичних режимів і довіру громадян до здатності урядів забезпечити безпеку в новому середовищі.

2.2. Нормативно-правові та інституційні інструменти протидії кібертероризму в державах європейського регіону

Динамічний характер кіберзагроз вимагає постійного вдосконалення засобів захисту. Нові типи атак ставлять нові виклики перед системою кібербезпеки. Тому європейські країни для розробки нових засобів захисту змушені постійно оновлювати свої стратегії, залучати до співпраці приватний сектор, інноваційні компанії та академічні установи.

На державному рівні ця система ґрунтується на гармонізації законодавства європейських країн, створенні єдиних стандартів криміналізації кіберзлочинів і встановленні механізмів міжнародної правової допомоги.

Як ми вже неодноразово зауважували, у сучасному світі кібербезпека є критично важливою для забезпечення національної безпеки, захисту

економічних інтересів та приватного життя громадян, тож спонукає країни до розробки ефективних стратегій захисту своїх кіберінфраструктур.

Для цього ми проведемо порівняльний аналіз стану забезпечення кібербезпеки в таких країнах, як Данія, Естонія, Франція, Німеччина, Нідерланди, Польща, Швеція та Велика Британія.

По-перше, ці країни мають різний рівень розвитку кібербезпеки, тому цікавим буде порівняння їх стратегій, інвестицій та досягнень. По-друге, вони демонструють різні підходи до забезпечення кібербезпеки, що відображає їхні політичні, економічні та соціальні контексти. По-третє, в умовах ризиків, що постійно зростають, зокрема й кібертероризму та організованої кіберзлочинності, і з якими стикається Європа, аналіз цих країн також дасть змогу виявити найкращі практики та можливості для співпраці між державами. Країни, які ми обрали для аналізу, активно беруть участь у міжнародних ініціативах та програмах, що сприяє обміну знаннями й ресурсами у щодо кібербезпеки, а також є партнерами України в Талліннському Механізмі.

Таким чином, вибір Данії, Естонії, Франції, Німеччини, Нідерландів, Польщі, Швеції та Великої Британії для аналізу щодо кібербезпеки є обґрунтованим і сприятиме глибшому розумінню різноманітності підходів, які ці країни застосовують у відповідь на сучасні виклики кіберзахисту.

Зазначимо, що, розглядаючи різні аспекти кібербезпеки цих країн, важливо врахувати кілька чинників, зокрема, рівень розвитку кіберінфраструктури, законодавчі ініціативи, інвестиції у технології та підготовку фахівців. У цьому контексті доцільно почати з Естонії, яка відзначається своєю інноваційною політикою в галузі кібербезпеки.

Незважаючи на те що Естонія невелика за розміром країна, вона одна з найбільш технологічно розвинених держав, яка стала глобальною моделлю боротьби з кібертероризмом. Однак така трансформація не відбулася відразу, а виникла після вже згадуваних нами серій кібератак у 2007 році, спрямованих на критичну інфраструктуру країни. Відтоді Естонія реалізувала багатогранну стратегію, яка поєднує технологічні інновації, міжнародну співпрацю та

активну позицію щодо освіти та законодавства з кібербезпеки, вона стала однією з перших країн, яка у 2008 році ухвалила національну Стратегію кібербезпеки [117]. Ця стратегія акцентує на важливості державно-приватного партнерства, сприяючи співпраці між урядом та різними галузями промисловості. Основною метою стратегії стало не лише підвищення потенціалу кібербезпеки, але й покращення обізнаності населення про кіберзагрози, що, своєю чергою, зміцнює довіру до цифрового середовища. Перша Стратегія передбачала комплексний підхід до захисту інформаційних систем, які є критично важливими для функціонування держави й бізнесу. Серед ключових аспектів – створення системи контролю у сфері кібербезпеки, зміцнення міжнародного співробітництва, удосконалення методів боротьби з кібертероризмом, а також розроблення нової законодавчої бази.

Для підтримки реалізації цієї стратегії Естонія значно вдосконалила законодавство, зокрема зосередила увагу на захисті критичної інформаційної інфраструктури, а також інвестувала в безпечні електронні послуги, що гарантує надійність її цифрової інфраструктури.

Серед основних тенденцій розвитку можна виділити також створення Об'єднаного Центру передових технологій з кібероборони НАТО (CCDCOE) у 2008 році [118]. Цей центр, розташований у Таллінні, став важливим майданчиком для міжнародної співпраці в галузі кіберзахисту. Він здійснює навчання, такі, як «Locked Shields» [119], і розробляє стандарти для країн – членів НАТО, що допомагає впроваджувати ефективні стратегії кібербезпеки. Україна стала учасником CCDCOE лише у 2023 році, що підкреслює важливість цього центру для регіональної безпеки [120,121].

У 2009 році Уряд Естонії заснував Кіберраду [122], яка стала ключовим консультативним органом для координації дій на державному рівні. Кіберрада об'єднала різні установи та відомства, забезпечивши стратегічну координацію, вироблення політичних рішень та контроль за виконанням завдань Стратегії кібербезпеки.

Ще одним важливим етапом стало створення у 2010 році Державного агентства інформаційних систем RIA [123], яке отримало статус центрального органу з розширеними повноваженнями. RIA відповідає за моніторинг кібербезпеки, управління ризиками, захист критичної інформаційної інфраструктури та реагування на інциденти. Крім того, агентство здійснює контроль за розробленням і впровадження технічних стандартів та інструкцій щодо захисту інформаційних систем, а також заохочення використання методів шифрування та безпечного зв'язку для захисту даних і зв'язку.

Тож, як бачимо, до 2013 року Естонія досягла значного прогресу в зміцненні своєї кібербезпеки, зосередивши увагу на міжнародній співпраці для боротьби з глобальними кіберзагрозами. Той факт, що протягом цього часу на Естонію не було зафіксовано значних кібератак, може свідчити про надуспішність проведеної країною роботи.

У 2014 році Естонія оновила Національну стратегію кібербезпеки, де головним принципом стала інтеграція кібербезпеки в загальну національну безпеку. На наш погляд, такий крок може бути пов'язаний із двома причинами, а саме: із прийняттям Стратегії кібербезпеки ЄС у 2013, а також з анексією Криму, яка супроводжувалася серією кібератак на Україну [124]. А оскільки Естонія вже відчувала на собі небезпеку російських кібернападів, очевидним стало швидке оновлення системи кібербезпеки із урахуванням нових викликів. Це окреслило важливість захисту особистих даних та прав громадян, а також дотримання принципу пропорційності у заходах безпеки.

Ураховуючи вищезазначене, Національна стратегія кібербезпеки Естонії 2014 року підкреслила необхідність узаємодії між державним, приватним і громадським секторами, що зміцнює кіберзахист і підвищує стійкість до загроз. Вона також зосередилася на індивідуальній відповідальності користувачів, наголошуючи на їх внеску в загальну безпеку цифрового простору. Пріоритетом є запобігання загрозам та ефективне реагування на кіберінциденти, а також розвиток науково-дослідної діяльності та інновацій, які забезпечують міжнародну конкурентоспроможність країни [125].

Зазначимо, що не тільки однією Стратегією гарантовано кібербезпеку Естонії. Існує розгалужена нормативно – правова база, яка містить кілька ключових законів, які підтримують цю стратегію:

– Закон «Про кібербезпеку» від 2018 року [126], який оновлює вимоги до інформаційних систем та створює правові межі для реагування на кіберінциденти. А задля успішного подолання кіберзагроз указаний Закон установлює ролі державних установ і організацій;

– Закон «Про захист персональних даних» від того ж 2018 [127] регулює обробку персональних даних, забезпечуючи права громадян на доступ і коригування своїх даних. Окрім того, він установлює суворі вимоги до організацій, які оброблюють дані для захисту від несанкціонованого доступу;

– Закон «Про цифровий підпис» [128], тоді Естонія стала однією з перших країн, яка впровадила такий закон у 2000 році, що дозволяє громадянам безпечно підписувати документи онлайн і взаємодіяти з урядом через цифрові платформи. Варто відзначити, що Україна теж прийняла Закон «Про електронний цифровий підпис» [129] через 3 роки після Естонії, однак він, на відміну від естонського, утратив свою чинність і був замінений Законом України «Про електронну ідентифікацію та електронні довірчі послуги» [130], який уже містив більш ширший спектр інформаційного впливу та спирався на новітні технології;

– Естонський закон «Про публічну інформацію» [131] також містить положення щодо захисту інформаційних систем, які гарантують доступ до публічної інформації, він спрямований на забезпечення прозорості в державному управлінні.

У 2019 році Стратегію Кібербезпеки Естонії було оновлено на період до 2022 року [132]. Вона визначила довгострокове бачення, цілі, пріоритетні напрями дій, ролі та завдання для цього напрямку. Згідно з положеннями Стратегія базується на досвіді, отриманому протягом двох попередніх періодів і вимагає гарантії скоординованості дій усіх установ, що здатні забезпечувати та підтримувати високий рівень кібербезпеки Естонії. Серед них державний

сектор (як цивільний, так і оборонний), постачальники інформативних послуг, підприємці різних галузей та наукові працівники. Метою цього документа стало узгодження та створення умов для здійснення всебічної, систематичної та всеосяжної галузевої політики.

Згідно з аналізом матеріалів щодо стратегій кібербезпеки можна встановити конкретні покращення, зроблені Естонією на кожному етапі. Так, стратегія 2008 року акцентує на трьох компонентах: зміцненні законодавчої бази, розвитку електронних послуг та розвитку партнерства. Протягом шести років Естонія працювала над удосконаленням своєї правової бази, установлюючи комплексні закони та правила з кібербезпеки для захисту критично важливої інформаційної інфраструктури. Окрім того, були зроблені великі інвестиції в розроблення безпечних електронних послуг, які забезпечать надійність і безпеку своєї цифрової інфраструктури. Найголовнішим кроком можна назвати той факт, що країна зосередилася на розвитку міцнішого державно-приватного партнерства, сприяючи спільному підходу до кібербезпеки, який використовує досвід як уряду, так і організацій приватного сектору.

Зауважимо, що програма кібербезпеки Естонії на 2021–2024 роки націлена на забезпечення стійкості та безпеки цифрової інфраструктури країни перед кіберзагрозами. Основною метою є перетворення Естонії на найкліматичнішу цифрову державу, що забезпечує надійне функціонування критичних інфраструктур. Програма містить стратегії для підвищення кіберстійкості через удосконалення інфраструктури, упровадження стандартів безпеки, активну міжнародну співпрацю та розвиток кваліфікованих фахівців у галузі кібербезпеки.

Ключовими напрямами програми є захищеність нових цифрових послуг і розвиток системи моніторингу кіберінцидентів. Однак існують виклики (відсутність єдиної координації між секторами, нестача кваліфікованих спеціалістів), які часто стосуються й приватного сектору. Програма також

наголошує на важливості підвищення обізнаності громадян щодо кіберзагроз [133].

Кіберзагрози 2023 року виявилися складними, зокрема атаки програм–вимагачів, що торкнулися різних секторів – від охорони здоров'я до виробництва. Багато атак були політично мотивованими й пов'язаними з підтримкою України та санкціями проти Росії. У відповідь Естонія посилила захист своїх кіберінфраструктур через проактивні ініціативи, що виявилися критично важливими для запобігання кібератакам [134].

Уже 5 Стратегія Естонії на 2024–2030 рр. [135] формує концептуальну основу для забезпечення стійкості країни в умовах швидкої діджиталізації. Документ акцентує на інтеграції кібербезпеки в усі аспекти державного управління й економіки, аналізує глобальні технологічні та політичні тренди, оцінює ризики та визначає заходи для їх мінімізації. Зокрема, у документі вказано на загрози, пов'язані з новітніми технологіями, такими, як штучний інтелект, а також політично мотивовані атаки. Особлива увага в Стратегії приділена впливу російської агресії на Україну, зокрема масштабним гібридним атакам на критичну інфраструктуру. Естонія, маючи значний досвід у кібербезпеці, підтримує Україну, надаючи ресурси для зміцнення її кіберпростору. Країна має надійну правову базу, зокрема Закон «Про кібербезпеку», який забезпечує правову основу для управління та реагування на кіберінциденти.

Отже, бачимо, що пріоритети Естонії в галузі кіберзахисту стосуються не тільки захисту критичної інфраструктури, а й забезпечують упровадження освітніх програм та підвищення обізнаності громадян у сфері кібергігієни, що підкреслює безсумнівне «лідерство» країни в питаннях комплексного підходу до організації стратегії кібербезпеки. Естонія активно розробляє навчальні платформи та залучає молодь до ініціатив з цифрової безпеки.

Варто вказати також про вже згадуваний нами Центр Кіберзахисту НАТО, відкритий у Таллінні, якому присвоєно статус міжнародної військової організації. Центр відіграє важливу роль в навчанні та гарантуванні безпеки

країн альянсу. У роботі Центру беруть участь 26 країн. Україна також стала членом, отримавши статус учасника-контрибутора [121].

Естонія посутньо зміцнює свою кібербезпеку завдяки діяльності CERT Estonia [136], що функціонує під керівництвом Адміністрації інформаційних систем. У розробленні політик та ініціатив у галузі кіберзахисту країна активно співпрацює з Європейським Союзом та такими організаціями, як ENISA. Важливим напрямом міжнародного співробітництва є членство Естонії в Спільному центрі передового досвіду кіберзахисту НАТО (CCDCOE), де вона відіграє активну роль [72].

На основі зібраних матеріалів слід зазначити, що кібербезпека Естонії є однією з найбільш розвинених серед європейського регіону, що робить її прикладом для багатьох інших держав. Завдяки успішно впровадженим стратегіям та інноваційним рішенням Естонія змогла стати лідером цифрової трансформації та кібербезпеки. Ключовими елементами естонської кібербезпеки є міцна інфраструктура, високий рівень узаємодії між державним та приватним секторами, а також постійне удосконалення нормативно-правової бази, що забезпечує надійний захист цифрових інфраструктур.

Наступна країна, що перебуває на передовій цифрового розвитку, – це Данія. Її суспільство все більше покладається на Інтернет та цифрові рішення для забезпечення добробуту й процвітання. Водночас зростання діджиталізації одночасно підвищує вразливість перед кіберзагрозами, що вимагає належного захисту країни.

Тож кібербезпека є одним із пріоритетів національної безпеки Данії, оскільки сучасні цифрові технології все більшою мірою проникають у всі напряіми суспільного життя. Цифрова інфраструктура країни охоплює не лише критичні галузі, такі, як енергетика, транспорт і охорона здоров’я, а й державне управління та приватний бізнес. Збільшення кількості кіберзагроз і стрімкий розвиток технологій спричиняють посилення власної законодавчої та інституційної бази для захисту національних інтересів у кіберпросторі Данії. З огляду на це, країна розробила комплексну систему кібербезпеки, яка містить

закони, національні стратегії, спеціалізовані органи та визнає ключові елементи міжнародної співпраці.

Данія має комплексний підхід до кібербезпеки, зокрема через «Національну стратегію кібербезпеки» 2014 року, що охоплює критичні сектори, зокрема енергетику, транспорт та телекомунікації. Створення Центру кібербезпеки для моніторингу загроз і координації між державними та приватними організаціями стало ключовим елементом стратегії [137,138].

Країна адаптувала директиву NIS через Закон «Про мережеву та інформаційну безпеку» [139], а також суворо дотримується GDPR для захисту персональних даних. Законодавство також містить вимоги до кібербезпеки щодо охорони здоров'я, транспорту та інтернет-інфраструктури [140].

Данія оновила свою Стратегію кібербезпеки у 2018 році [141], зосередившись саме на захисті критичної інфраструктури та розширенні ресурсів для швидкого реагування на кіберінциденти. Були також переглянуті закони щодо кіберзлочинності та інтегровані положення Будапештської конвенції. Отже, як бачимо, Данія поєднує національні ініціативи з європейськими стандартами для зміцнення кіберзахисту, але їх реалізація вимагає тісної міжгалузевої співпраці.

Зазначимо, що Данія має розвинену систему кібербезпеки, в основі якої лежить співпраця ключових органів, зокрема Центру кібербезпеки [142], Данського агентства із захисту даних [143], Міністерства оборони [144] та Національної поліції [145]. Саме Центр кібербезпеки, що входить до складу Данської служби розвідки, відповідає за моніторинг кіберзагроз, оперативне реагування на інциденти та координацію дій між державними органами й приватним сектором. Згідно із законодавством, Центр має право обробляти дані без судового дозволу та вимагати підключення до своїх систем від державних органів і стратегічних компаній, що порушує питання щодо дотримання приватності.

Данське агентство із захисту даних відповідає за дотримання GDPR, накладаючи штрафи на організації за порушення правил обробки персональних

даних. Міністерство оборони забезпечує захист військових інформаційних систем, співпрацюючи з міжнародними партнерами. Важливим аспектом є роль Національної поліції, яка через спеціалізовані підрозділи займається розслідуванням кіберзлочинів [146].

Відзначається активна роль Данії у міжнародному співробітництві, зокрема через Європейське агентство з кібербезпеки (ENISA) та участь у програмі «Цифрова Європа», що дозволяє країні отримувати фінансування для національних проєктів. Данія також підтримує Україну в зміцненні кібербезпеки, надаючи технічну допомогу та обмінюючись досвідом.

Попри успіхи у сфері кібербезпеки, Данія постає перед дефіцитом кваліфікованих фахівців, що створює загрози для захисту інформаційних систем, особливо в малих і середніх підприємствах. Брак кадрів підвищує вразливість таких компаній до кібератак, що може призвести до фінансових втрат і зниження конкурентоспроможності. Для подолання цієї проблеми необхідні інвестиції в освіту, зокрема створення спеціалізованих курсів та підвищення кваліфікації працівників. Важливим напрямом є залучення іноземних фахівців шляхом спрощення візових процедур та створення сприятливих умов для працевлаштування.

Так, у 2022 році була затверджена нова стратегія, яка покликана була вирішити й цю проблему [147]. Ця стратегія передбачає впровадження передових технологій (порівняно з минулим), з метою забезпечення кібербезпеки на національному рівні. Стратегія також націлює на підтримку досліджень і технологічних інновацій у сфері кібербезпеки, розширення освітніх програм для підготовки фахівців з кібербезпеки, а також підвищення обізнаності населення про ризики у цифровому просторі. Таким чином, Данія прагне бути лідером у галузі кібербезпеки, використовуючи передові технології та адаптуючись до змінюваних викликів у кіберпросторі.

Важливо також звернути увагу на те, в Данії, як і в багатьох країнах, серед інституцій існує група реагування на інциденти комп’ютерної безпеки DKCERT [148], яка стежить за безпекою кібермережі. Крім того, функціонує

також NORDUnet CERT [149], який підтримує безпеку в освітньому середовищі та співпрацює з іншими міжнародними дослідницькими мережами. А в секторі енергетики головним постачальником послуг із кібербезпеки є EnergiCERT [150].

Отже, потрібно зазначити, що впроваджені Данією інституційні механізми протидії кібертероризму дозволяють оцінювати рівень її безпеки як високий, а готовність до кібератак на сьогодні дає можливість Данії розвивати кіберінфраструктуру для подальшої протидії кібертероризму.

Ще одним сильним «гравцем» в галузі кібербезпеки є Швеція, яка вже давно посідає провідну позицію серед європейських країн. Її лідерство в цій галузі, як ми вважаємо, зумовлено усвідомленням критичної важливості кібербезпеки для національної безпеки, економічної стабільності й загальної функціональності суспільства. В умовах стрімкої цифровізації усього суспільного життя уряд Швеції впровадив Національну тратегію кібербезпеки, створив низку спеціалізованих агентств та ухвалив кілька важливих законів для того, щоб захистити інтереси країни та її громадян. Такий комплексний підхід дає змогу Швеції ефективно реагувати на нові кіберзагрози та забезпечувати сталий розвиток на тлі швидкого поширення цифрових технологій.

У результаті аналізу наукової літератури та офіційних документів Швеції було виявлено, що національна стратегія кібербезпеки цієї країни затверджена у 2017 році . Вона визначає пріоритети політики, зокрема забезпечення конфіденційності, цілісності та доступності інформації. Головною метою стратегії є створення стійкого до кіберзагроз суспільства, здатного ефективно реагувати на цифрові виклики.

Одним із ключових напрямів кібербезпеки у Швеції подібно до Данії є розвиток кіберкультури та підвищення обізнаності населення. В освітніх закладах упроваджуються спеціальні програми з кібергігієни, які формують у молоді навички безпечної поведінки в цифровому середовищі. Для дорослих організовуються тренінги, що допомагають розпізнавати кіберзагрози та захищати особисті дані.

Особливу увагу приділяють підготовці державних службовців, які проходять навчання для швидкого реагування на кіберінциденти. Такі програми включають не лише теоретичні знання, а й практичні симуляції загроз, що дозволяє ефективно управляти кризовими ситуаціями.

Захист критично важливої інфраструктури в енергетиці, транспорті, фінансовому секторі та охороні здоров'я є пріоритетом. Упроваджуються жорсткі стандарти кібербезпеки, регулярні перевірки систем та аудити безпеки.

Основним законодавчим актом є «Säkerhetsskyddslag, 2018:585» [151], який визначає вимоги до організацій щодо проведення ризикових аналізів та впровадження заходів безпеки. Однак цей закон не враховує специфіки сучасних кіберзагроз, таких, як хакерські атаки чи фішинг, що створює прогалини в гарантуванні безпеки цифрових каналів.

Зокрема, закон не містить положень, які б охоплювали сучасні кіберзагрози, що ставить під загрозу безпеку національної інфраструктури. Включення кібербезпеки до цього закону дозволило б уніфікувати підходи до захисту даних і зобов'язати організації застосовувати складніші стандарти захисту, такі, як шифрування даних, моніторинг мережевої активності та багатоетапну автентифікацію.

Швеція також активно співпрацює з Європейським Союзом, упроваджуючи стандарти кібербезпеки в межах ініціатив, таких, як Закон «Про інформаційну безпеку соціально важливих послуг» [152], який є частиною європейської Директиви NIS і встановлює обов'язки для постачальників основних послуг у сферах транспорту, енергетики, фінансів та цифрових послуг. А Закон «Про електронні комунікації» [153] захищає комунікаційні мережі, проте жоден із них не має конкретних положень щодо кібербезпеки.

За практичну реалізацію також відповідає Національний центр кібербезпеки [154], створений у 2020 році, який координує зусилля щодо протидії кіберзагрозам. З 2024 року він став частиною Агентства оборонного радіомовлення, що покращить його здатність реагувати на загрози. Важливу роль у захисті даних відіграють команди реагування на комп'ютерні інциденти

(CSIRT), які працюють у різних секторах, зокрема в уряді, фінансових установах та телекомунікаціях.

Наступним інституційним механізмом є шведська мережа CSIRT, яка активно співпрацює на міжнародному рівні, що підвищує її здатність до ефективної протидії кіберзагрозам. Зокрема, CERT– SE, FM CERT та інші команди мають акредитацію Trusted Introducer, що підтверджує їх високий рівень професіоналізму і здатність до оперативної взаємодії з європейськими командами [155,156].

У результаті проведеного аналізу наукової літератури та офіційних документів країни, можемо констатувати, що підхід Швеції до кібербезпеки, на наш погляд, є одним із найбільш продуманих і всебічних серед європейських країн. Уряд зосередився на створенні комплексної правової основи для захисту державної та приватної цифрової інфраструктури, що включає спеціалізовані агентства та центри, які координують діяльність у галузі кібербезпеки. Завдяки поєднанню законодавчих заходів, стратегічного планування та міжнародної співпраці Швеція успішно захищає національні інтереси й готова реагувати на нові загрози.

Цифровізація перетворила й інформаційну інфраструктуру Німеччини на критично важливий компонент національної безпеки. Однак залежність від IT–систем підвищує вразливість до кібератак, які можуть дестабілізувати ключові сектори, зокрема енергетику, транспорт та фінанси.

Німеччина розробила комплексну правову та інституційну базу для забезпечення кібербезпеки, що містить ключові закони, такі, як Закон про Федеральне відомство з інформаційної безпеки (BSIG) [157], Загальний регламент про захист даних (GDPR) Німеччини [158] та Федеральний закон про захист даних (Bundesdatenschutzgesetz) Німеччини [159]. Ці нормативно-правові акти встановлюють мінімальні вимоги до безпеки та штрафи за їх порушення. Кримінальне законодавство Німеччини визначає відповідальність за кіберзлочини, зокрема хакерство, фішинг та інші кіберзагрози.

Законодавчі ініціативи Німеччини, наприклад, Акт про інформаційну безпеку [74], установлюють мінімальні стандарти для підприємств критично важливої інфраструктури. Важливим документом є Національна стратегія кібербезпеки, прийнята у 2011 році [160], яка визначає підходи до забезпечення кібербезпеки та співпраці між державними установами, приватним сектором і науковими установами.

Основним органом, відповідальним за кібербезпеку Німеччини, є Федеральний офіс з інформаційної безпеки (BSI) [161], який також займається сертифікацією безпеки та консультаціями. Окрім того, у Німеччині функціонує мережа організацій CERT/CSIRT, що реагують на кіберінциденти та аналізують загрози. Ці центри також розподілені за галузями і гарантують кібербезпеку Німеччини на всіх рівнях [162,163,164,165,166,167,168,169,170,171,172,173].

Останні оновлення Національної стратегії кібербезпеки Німеччини, зокрема у 2016 році [174] та 2021 році [175], підкреслюють важливість співпраці між різними секторами. Відповіддю на кіберзагрози, зокрема з боку Росії після початку її агресії в Україні, стало посилення захисту державних і приватних інфраструктур .

Попри високий рівень організованості, Німеччина постає перед проблемами в адаптації стандартів безпеки до нових кіберризиків та фрагментацією правил кібербезпеки в різних законах. Збільшення кількості кіберзагроз демонструє необхідність постійного удосконалення нормативної бази.

Кібербезпека в Німеччині є складним і багатогранним завданням, що передбачає постійне оновлення стратегій та співпрацю між державою, бізнесом і суспільством. Для розв’язання цього завдання Німеччина створила розгалужену систему кібербезпеки, що базується на комплексному законодавстві та координації між державним і приватним сектором. Проте збільшення кількості кіберзагроз і швидкий розвиток технологій вимагають постійного вдосконалення нормативно-правової бази та посилення

адаптивності системи кіберзахисту для забезпечення стабільності критично важливої інфраструктури.

Маючи одну з провідних економік світу, Велика Британія активно розвиває цифрову інфраструктуру, що водночас виступає й каталізатором її вразливості до кіберзагроз. З огляду на це британський уряд формує комплексний підхід до захисту національної кіберінфраструктури, залучаючи державний сектор, приватні підприємства та наукові установи до створення єдиної системи кіберзахисту.

Наприклад, Закон про неправильне використання комп'ютерів (Computer Misuse Act) у Великій Британії, ухвалений у 1990 році, став першим правовим актом Великої Британії, що встановив основи кібербезпеки, реагуючи на загрози комп'ютерних злочинів, зокрема несанкціонований доступ до систем та шкідливе програмне забезпечення. Цей закон став фундаментом для подальших ініціатив у сфері кіберзахисту [176].

У 2007 році Велика Британія змінила підхід до міжнародної кібербезпеки, наголошуючи на активному захисті національних інтересів. Ключовими нормативними актами стали Закон про захист даних 2018 року DPA [177] та Загальний регламент захисту даних Великої Британії (UK - GDPR) [178], що встановлюють високі стандарти обробки персональних даних.

Перша національна стратегія кібербезпеки Великої Британії [179] була ухвалена в 2009 році та зосереджувалася на підвищенні стійкості критично важливих інфраструктур. Подальші стратегії Великої Британії, зокрема у 2011 та 2016 роках, звертали увагу на партнерство між державою, приватний сектор та міжнародне співробітництво [180,181].

Остання стратегія Великої Британії на 2022–2030 роки в умовах глобальної нестабільності ставить у центр уваги захист критичної інфраструктури від кіберзагроз та готовність до потенційних конфліктів у кіберпросторі, особливо у відповідь на кібератаки з боку Росії. Важливим аспектом є зміцнення партнерств із Україною, Європою та НАТО для обміну розвідданими та зміцнення оборонних механізмів [182].

Кібербезпека у Великої Британії є частиною національної безпеки з акцентом на військові та квазівійськові загрози. Велика Британія, як і інші європейські держави, активно інвестує в технології, управління ризиками та підвищення готовності до кібератак через програми співпраці з міжнародними партнерами.

Крім того, країна дотримується міжнародних стандартів у галузі кібербезпеки, що свідчить про готовність адаптуватися до змінюваного кібернетичного ландшафту. Національний центр кібербезпеки (NCSC) Великої Британії, заснований у 2016 році [183], відіграє важливу роль у централізації кіберзахисту країни, надаючи підтримку у боротьбі з кіберзагрозами, а також щодо обміну інформацією між державними установами й приватним сектором.

Крім NCSC, важливу роль у захисті персональних даних у Великій Британії відіграє Управління комісара з питань інформації (ICO) [184], яке має повноваження розслідувати порушення конфіденційності та накладати штрафи за недотримання вимог законів, зокрема DPA та UK– GDPR. Регулятор телекомунікацій, відповідальний за безпеку телекомунікаційних мереж OFCOM [185], також отримав додаткові повноваження згідно із Законом про телекомунікації 2021 року Великої Британії, що підвищує загальний рівень кібербезпеки в країні.

Отже, Велика Британія активно розвиває кібербезпеку, ураховуючи залежність від цифрової інфраструктури та кіберзагроз. Країна створила комплексну правову та інституційну базу, уключаючи ключові закони та стратегії, що охоплюють захист персональних даних, національної інфраструктури та партнерство між державним і приватним сектором. Важливими органами є Національний центр кібербезпеки Великої Британії та Управління комісара з питань інформації у Великій Британії. Ця країна також активно співпрацює з міжнародними партнерами, зокрема з Україною та НАТО для зміцнення кіберзахисту й боротьби з новими загрозами, такими, як кібератаки з боку Росії.

Наступна країна, питання кіберзахисту якої були проаналізовані, – це Нідерланди. Держава вже понад десять років розробляє комплексну політику безпеки для кібероперацій, зокрема й наступальних. Вторгнення Росії в Україну посилило відчуття нагальної необхідності підвищити рівень кіберготовності військових і цифрової стійкості голландського суспільства. Попри те, що Нідерланди відіграють провідну роль у деяких аспектах цифрової економіки і є відомим міжнародним центром обміну даними, центрів обробки даних, однак, кіберсектор Нідерландів є невеликим порівняно з більшістю європейських сусідів.

Національний координаційний центр з кібербезпеки України та Національний центр кібербезпеки Нідерландів нещодавно в Гаазі на конференції ONE підписали Меморандум про взаєморозуміння. Ця угода знаменує собою значний крок уперед у партнерстві між двома країнами для боротьби з кіберзагрозами та обміну досвідом з кібербезпеки. Обидві країни стикаються з проблемами, пов’язаними зі зростанням кіберзагроз і гібридною війною, що підкреслює важливість співпраці. Заступник секретаря Ради національної безпеки і оборони України Сергій Демедюк наголосив на критичній ролі кібербезпеки в захисті України від російської агресії. Уряд Нідерландів визнає, що сучасна війна охоплює як фізичні, так і кібератаки, а Меморандум про взаєморозуміння є важливим продовженням двобічної угоди про безпеку. Це партнерство демонструє взаємне прагнення посилити можливості кібербезпеки через спільні ініціативи та постійну співпрацю, визнаючи, що кібербезпека як важливий аспект національної оборони та міжнародних відносин постійно зростає [186].

Ми виявили, що перша урядова публікація, в якій серйозно розглядався потенціал кібербезпеки, була оприлюднена в лютому 2011 року. У цей період кілька міністрів, зокрема з безпеки та юстиції, оборони, економічних і внутрішніх справ, представили першу Національну стратегію кібербезпеки Нідерландів [187]. Однією з головних цілей стратегії було позиціювання країни як міжнародного лідера з кібербезпеки. Вона заклала основи для інтегрованого

підходу до кібербезпеки, який передбачає співпрацю державних установ, приватних організацій та наукових кіл, що підкреслювало важливість міжгалузевої координації.

Основні напрями стратегії – комплексний аналіз загроз і ризиків для підвищення видимості потенційних небезпек, зміцнення стійкості критичної інфраструктури і т.ін. Такі ініціативи засвідчили проактивний підхід Нідерландів до розв'язання проблем кібербезпеки на національному та міжнародному рівнях.

Одним із найважливіших пунктів програми дій NCSS 2011 року стало створення Ради з кібербезпеки Нідерландів «Cyber Security Raad» [188] – Органу, який об'єднує державний і приватний сектори, а також наукові установи для покращення координації національних ініціатив, інформування громадськості та оперативного співробітництва. Важливою частиною реалізації стратегії було впровадження національних аналізів загроз і ризиків, а також формулювання ідеї про включення наступальних кіберпотужностей до складу військового потенціалу Збройних сил Нідерландів [189]. Це рішення спричинило створення Оборонного кібернетичного командування Нідерландів, яке стало відповідальним за розвиток наступальних кіберспроможностей та розробку оборонної кіберстратегії.

У 2013 році Нідерланди презентували другу Національну стратегію кібербезпеки [190], яка значно розширила підхід до кібербезпеки, залучивши, зокрема, соціально-економічні переваги, права людини, конфіденційність та інновації. Цей підхід ураховував не лише технологічні, а й соціальні аспекти кібербезпеки, що дозволило країні краще зрозуміти проблеми та сприяти міжсекторальній співпраці.

У 2018 році було оприлюднено Нідерландську програму кібербезпеки, яка вдосконалила національну стратегію [191], зосередивши увагу на семи основних цілях. Серед них було заявлено такі: розвиток можливостей для виявлення, пом'якшення та реагування на кіберзагрози, зміцнення міжнародної безпеки в кіберпросторі, упровадження безпечного апаратного і програмного

забезпечення, просування стійких цифрових процесів, боротьба з кіберзлочинністю, розвиток знань із питань кібербезпеки та сприяння співпраці між державним і приватним секторами.

Нідерландська програма кібербезпеки позначила перехід до проактивного підходу, який не тільки фокусується на захисті від загроз, але й використовує кібербезпеку як інструмент національної безпеки та економічної конкурентоспроможності. Стратегії, що були розроблені з 2011 по 2018 роки, демонструють зрілий і адаптивний підхід Нідерландів до кібербезпеки, зокрема через інтеграцію технологічних і соціальних аспектів, що допомагає країні ефективно реагувати на нові виклики та можливості у цифровому середовищі.

У жовтні 2022 року Нідерланди представили свою Стратегію кібербезпеки на 2022 – 2028 роки [192], що стало важливим кроком у захисті цифрової інфраструктури та громадян. Ця стратегія враховує зміни в кіберзагрозах і спрямована на підвищення стійкості всіх учасників цифрової сфери. Вона інтегрує національні дії для протидії кіберзагрозам та цифровій залежності, зміцнюючи стійкість суспільства.

Ця стратегія є значним оновленням попередніх планів, оскільки охоплює більш тривалий період і враховує як цивільні, так і військові аспекти кібербезпеки. Вона тісно пов’язана з іншими документами національної безпеки, зокрема з «Білою книгою оборони» 2022 року [193], яка також наголошує на розвитку кіберзахисту та інтегрованих кібероперація із союзниками. Загалом стратегія 2022 року відображає комплексний підхід до захисту цифрових інтересів Нідерландів та зміцнення оборонних можливостей у відповіді на сучасні загрози.

Підсумовуючи, скажемо, що стратегія кібербезпеки до 2022 року являє собою значну еволюцію підходу Нідерландів до кібербезпеки та одночасно зберігає основні принципи попередніх стратегій. Це відображає визнання Нідерландами взаємопов’язаного характеру сучасних загроз і потреби у комплексній довгостроковій Стратегії кібербезпеки, яка охоплює як цивільні, так і військові аспекти кібербезпеки.

На окрему увагу заслуговує сертифікація кібербезпеки, що стає критичним аспектом в умовах цифрової трансформації країни. Основним законодавчим актом для забезпечення кібербезпеки Нідерландів є Wet Beveiliging Netwerk– en Informatie Systemen (Wbni) [194], який зобов'язує державні органи та компанії гарантувати безпеку своїх інформаційних систем. Такий новий закони, як Закон «Про державний цифровий уряд Нідерландів» (Wdo) [195], визначає вимоги щодо кіберзахисту для державних установ і приватних компаній, зокрема щодо швидкості звітування про кіберінциденти.

У травні 2024 року уряд Нідерландів зробив ще один крок із посилення кібербезпеки, опублікувавши проект нового Закону «Про кібербезпеку – CSA» [196]. CSA імплементує Директиву (ЄС) 2022/2555 (Директива NIS2») у нідерландське законодавство. NIS2 розширює обов'язки для більшої кількості компаній, ніж попередня версія, установлює жорсткіші вимоги до кібербезпеки і визначає правила для звітування про значні інциденти (в терміни 24 години для первинного попередження, 72 години для повного звіту і місяць для фінального звіту) [197].

У Нідерландах кілька ключових організацій виконують важливу роль у забезпеченні кібербезпеки та реалізації відповідного законодавства. Національний центр кібербезпеки, підпорядкований Міністерству юстиції та безпеки, є основним контактним центром для питань кібербезпеки. Центр координує діяльність державних агентств, підтримує операторів критичних послуг, аналізує кіберзагрози та поширює інформацію щодо запобігання кібератакам, а також активно взаємодіє на міжнародному рівні [198].

Створення Центру оборонної кіберекспертизи DCEC [199] дало змогу Нідерландам зміцнити оборонне кіберкомандування. Цей центр забезпечує розвиток знань у кіберпросторі та сприяє інтеграції цих знань в оборонну стратегію країни. Оборонне кіберкомандування, що входить до складу Міністерства оборони, відповідає за розробку та реалізацію військових кібероперацій.

Служби розвідки, зокрема Служба загальної розвідки та безпеки (AIVD) і Служба військової розвідки та безпеки (MIVD), також відіграють суттєву роль у кібербезпеці. AIVD займається розслідуванням загроз, пов'язаних із тероризмом і екстремізмом, тоді як MIVD фокусується на аналізі зовнішніх військових загроз. Обидві служби співпрацюють у межах Об'єднаного кіберпідрозділу Sigint Cyber Unit (JSCU), який підтримує національну безпеку через перехоплення комунікацій та захист Інтернету [200].

Важливою частиною є Голландська асамблея кібербезпеки DCA [201], створена у 2021 році для підвищення рівня кібербезпеки в країні. Асамблея об'єднує державні установи, постачальників послуг безпеки та приватний сектор для спільної розробки рішень з проблем кібербезпеки. Вона також активно працює над підвищенням кіберстійкості, інтегруючи людей, процеси та технології для створення більш безпечного цифрового середовища в Нідерландах.

Ці організації та їх взаємодія є важливими частинами в забезпеченні національної безпеки в кіберпросторі Нідерландів, породжуючи потужну систему для протидії сучасним кіберзагрозам.

Отже, Нідерланди демонструють усебічний та стратегічний підхід до кібербезпеки, активно зміцнюючи як національну, так і міжнародну кіберстійкість на тлі збільшення загроз, особливо в умовах глобальних конфліктів. Завдяки гнучкій адаптації своєї політики та нормативної бази, країна інтегрує кібербезпеку в усі ключові сфери – від захисту критичної інфраструктури до підвищення рівня обізнаності в суспільстві. Уряд наголошує на важливості партнерства між державним і приватним секторами, підтримує наукові дослідження та сприяє міжнародній співпраці. Такий підхід Нідерландів спрямований на досягнення стійкості цифрової інфраструктури, зміцнення кіберготовності та розвитку фахівців з кібербезпеки. Нідерланди також потужно інвестують у розвиток своїх оборонних кіберможливостей, визнаючи, що сучасна війна вимагає комплексного захисту, де кіберпростір відіграє важливу роль.

Франція також є країною, яка має добре розвинену багаторівневу систему в галузі кібербезпеки, поєднуючи національні потреби в захисті від кіберзагроз із зобов'язаннями перед Європейським Союзом. Французька система базується на низці законодавчих актів, регламентів, директив та міжнародних угод, спрямованих на захист критичної інфраструктури, персональних даних, боротьбі з кіберзлочинністю та гарантування національної безпеки в цифровому просторі. Розвиток цієї системи відбувався поступово, інтегруючи національні ініціативи та європейські стандарти, що дозволило Франції стати одним із лідерів у сфері кібербезпеки.

Формування законодавчої бази Франції щодо кібербезпеки почалося з підписання Конвенції Ради Європи по боротьбі з кіберзлочинністю у 2001 році, ратифікованої у 2006 році. У 2008 році «Біла книга з питань національної оборони і безпеки» вперше визначила кіберзагрози основним ризиком для національної безпеки [202].

Уже в 2009 році було зроблено перший крок до практичної реалізації запланованих кроків із забезпечення кібербезпеки, створено Національне агентство з безпеки інформаційних систем (ANSSI) [203], яке до сьогодні координує розроблення стратегій кібербезпеки, проводить аудит і сертифікацію критичних інформаційних систем. ANSSI має складну структуру з кількома ключовими підрозділами, але демонструє інтеграцію функцій, що зміцнює національну кібербезпеку. Чітка організаційна структура дозволяє агентству не лише реагувати на загрози, а й формувати стратегії щод їх запобігання, підвищуючи загальний рівень кіберстійкості країни.

У 2011 році Франція оголосила про першу Національну стратегію кібероборони [204], визнавши кіберпростір п'ятим оборонним виміром, а в 2015 році стратегія була оновлена [205] з акцентом уже на захист критичних секторів та міжнародну співпрацю.

Франція також імплементувала Директиву NIS, що гарантує безпеку мереж й інформаційних систем у критичних секторах, таких, як енергетика, транспорт і охорона здоров'я. У 2018 році було ухвалено третю Національну

стратегію кібероборони [206], що акцентує на розвиток наступальних кіберспроможностей і міжнародній співпраці через НАТО та ЄС.

Ще одна стратегія Франції за 2021 рік – Національна стратегія кібербезпеки – спрямована на підвищення стійкості до кіберзагроз через інвестиції в кіберекосистему, розвиток досліджень, інновацій, підготовку фахівців та зміцнення міжнародної співпраці [207]. Таким чином була посилена активна співпраця Франції з міжнародними організаціями (Інтерполом і Європолом), які допомагають їй підтримувати належний рівень кібербезпеки.

Франція відчуває посилення нових загроз у кіберпросторі, що охоплюють злочинне використання Інтернету, кіберзлочинність, яка використовується в терористичних цілях, масштабну дезінформацію, шпигунство, спрямоване на політичні чи економічні інтереси, атаки на критичні інфраструктури, зокрема транспорт і енергетику. Основними особливостями цих атак є їх складність, невизначеність походження, а також використання державних або недержавних акторів.

Водночас відзначимо, що французька кібербезпека щодо заходів для захисту від цих загроз, постійно посилюється, а створена в країні національна система набирає обертів. Так, наприклад, Франція має розгалужену мережу Центрів реагування на інциденти комп'ютерної безпеки (CERT) та команд реагування на інциденти безпеки інформаційних систем (CSIRT) [208], які займаються виявленням, аналізом та реагуванням на кіберзагрози. Одним із ключових органів є CERT– FR, національний центр, який координує діяльність інших CERT та CSIRT, обмінюється інформацією про загрози та надає рекомендації щодо захисту. Існують також галузеві CERT, які зміцнюють кібербезпеку певних напрямків критичної інфраструктури.

Окрім того, забезпечення кібербезпеки Франції є одним із пріоритетів Міністерства Збройних Сил, яке забезпечує захист мереж, а також, інтегрує цифрові технології в проведення військових операцій [209].

Задля координації та об'єднання зусиль із Міністерством Збройних Сил у 2017 році було створено Командування Кіберзахисту COMCYBER [210], місія

якого полягає у протидії кіберзлочинності, зокрема захисті національних інтересів, органів державної влади громадянського суспільства. З метою виконання поставлених завдань COMCYBER оперативно скеровує спеціалізовані головні управління й територіальні підрозділи національної поліції, національної жандармерії та інших служб, відповідаючи за внутрішню безпеку.

Названі організації активно співпрацюють між собою та з міжнародними партнерами, а це в свою чергу дозволяє Франції ефективно реагувати на кіберзагрози й підтримувати високий рівень кібербезпеки на національному рівні.

Таким чином, база кібербезпеки Франції є комплексною, багаторівневою та всебічною. Вона успішно поєднує національні стратегії та закони з європейськими регламентами та директивами для забезпечення ефективного захисту від кіберзагроз, захисту персональних даних та підтримки національної безпеки в цифрову епоху. Франція активно розвиває свої захисні можливості від кіберзагроз, посилює міжнародну співпрацю та впроваджує новітні технології для безпеки в цифровому просторі, що робить її важливим гравцем на світовій арені кіберзахисту.

Польща як одна з країн Європи також активно впроваджує стратегії та механізми для безпеки своїх систем кібербезпеки. У 2019 році Польща затвердила Стратегію кібербезпеки на період 2019–2024 років, яка визначає основні цілі та завдання у цьому напрямку [211]. Основною метою стратегії є підвищення національної стійкості до кіберзагроз та створення ефективних механізмів реагування на інциденти. Ця стратегія охоплює комплекс заходів, спрямованих на захист критичної інфраструктури, поліпшення координації між державними органами та суспільством, а також на забезпечення належної підготовки кадрів із кібербезпеки. Цим аспектом політики Польща дуже схожа з Данією та Нідерландами, про які ми згадували вище. Наприклад, важливим аспектом стратегії є проведення регулярних аудитів та тестування безпеки

інформаційних систем, що дозволяє оцінювати їхню ефективність із певною періодичністю.

Однак, щоб зрозуміти, як розвивалася політика кібербезпеки Польщі, важливо розглянути етапи, що передували сучасним стратегіям.

Першим кроком у напрямку створення структурованого підходу до кібербезпеки в країні стала «Урядова програма захисту кіберпростору», затверджена у 2009 році, яка зосереджувалась на ранніх заходах кібербезпеки, уключаючи розробку базових принципів та стандартів [212].

У 2013 році Польща прийняла перший стратегічний документ щодо кібербезпеки – «Політику захисту кіберпростору» [213]. Згідно зі змістом основною метою було забезпечення належного рівня захисту національного кіберпростору з урахуванням наявних кіберзагроз. Цей документ став першим стратегічним документом у галузі кібербезпеки в державі.

Через три роки, у 2016 р., було ухвалено Стратегію кібербезпеки, яка окреслила основні напрями розвитку політики, зокрема підвищення готовності до кіберзагроз і захист інформаційних систем. Акцент був зроблений також на необхідності посилення захисту критичної інфраструктури та створення чіткої системи управління кібербезпекою, де основним координатором став Міністр цифровізації [214].

І вже у 2017 році була прийнята Національна структура політики кібербезпеки [215], яка визначила стратегічні цілі для державного та приватного секторів. Вона була спрямована на координацію дій на національному рівні, підвищення спроможності протидії кіберзагрозам і розвиток міжнародної співпраці. Для посилення зовнішньополітичної взаємодії у 2018 році Польща імплементувала Директиву NIS, прийнявши «Закон про національну систему кібербезпеки», що визначив основи для стійкості інформаційних систем і встановив обов’язки для учасників захисту кібербезпеки, уключаючи державні органи та приватний сектор.

Національна стратегія кібербезпеки 2020 року [216] продовжила попередні ініціативи, підкресливши важливість міжнародної співпраці для

боротьби з транснаціональними кіберзагрозами та адаптацію до нових викликів, таких, як кібертероризм і використання штучного інтелекту. Стратегії еволюціонували від вузького підходу до комплексного, акцентуючи на інтегрованій відповіді на кіберзагрози.

Польща також створила ефективну систему реагування на кіберзагрози через мережу команд CSIRT, зокрема CSIRT GOV, для захисту державних установ та CERT.PL для приватного сектору. Ці команди забезпечують обмін інформацією, надають оперативну підтримку та проводять тренінги. Окрім цього, Науково-академічна комп'ютерна мережа (NASK) займається підвищенням обізнаності про кібербезпеку через програми для молоді, що є важливим елементом у навчанні майбутнього покоління основам захисту даних в онлайн-середовищі [217, 218].

Попри досягнення у сфері кібербезпеки, Польща постає перед низкою суттєвих викликів. Однією з основних проблем є відсутність комплексних державних програм, які б охоплювали всі аспекти кібербезпеки для організацій та приватних осіб. Це свідчить про необхідність удосконалення політики в цій сфері для забезпечення більш цілісного підходу до захисту інформаційних систем. Крім того, важливою проблемою є недостатній рівень обізнаності підприємців і громадян щодо основ кібербезпеки. Багато організацій не мають належних протоколів для реагування на інциденти, що може призвести до серйозних наслідків.

Згідно зі звітом Урядового уповноваженого з питань кібербезпеки Міністерства цифровізації за 2023 рік [219] Польща залишалася об'єктом численних кібератак, спрямованих на отримання конфіденційної інформації, ідентифікацію вразливих інформаційно-комунікаційних систем, порушення роботи критичної інфраструктури, а також поширення дезінформації. Ці атаки підкреслюють важливість посилення національної системи кібербезпеки.

У відповідь на ці виклики у жовтні 2023 року було запущено проєкт зі створення Центру кібербезпеки NASK (CCN). Проєкт передбачає організацію спеціалізованих центрів і лабораторій, що сприятимуть зміцненню

національної системи кібербезпеки. Його реалізація має на меті підвищення стійкості та здатності ефективно реагувати на кіберінциденти, що є ключовим питанням для економічної безпеки країни [220].

Згідно з планами щодо вдосконалення національної системи кібербезпеки передбачена реалізація Директиви NIS2 та розробка нової Стратегії кібербезпеки на 2025– 2029 роки. Важливим аспектом цієї стратегії є лист від державного секретаря Павела Ольшевського, який наголошує на необхідності розробки стратегії з урахуванням захисту інвестицій в офшорну енергетику, обов'язків операторів вітрових електростанцій та можливості створення галузевих CSIRT для посилення ефективності управління кіберзагрозами [221].

Окрім технічних аспектів, важливими для розвитку кібербезпеки є етичні та правові питання. Уряд та відповідні структури повинні враховувати соціальні аспекти під час розроблення політик у цій сфері, зокрема, під час збору даних і моніторингу кіберзагроз необхідно забезпечувати захист прав громадян на приватність і безпеку їхніх особистих даних.

Таким чином, польська система кібербезпеки перебуває на етапі активного розвитку, проте потребує вдосконалення та розширення своїх функцій. Для досягнення успіху в цьому напрямку важливо не лише впроваджувати нові законодавчі ініціативи, а й вести активну освітню роботу серед населення, зокрема серед молоді. Тільки за умови усвідомлення важливості кібербезпеки на всіх рівнях суспільства можна досягти бажаного результату в забезпеченні безпеки інформаційних систем і захисті даних.

Відзначаючи поточні досягнення та враховуючи виклики, які стоять перед країною, Польща може стати прикладом ефективної політики у кібербезпеці для інших країн. Зокрема, важливо, щоб держава продовжувала інвестувати в технологічні рішення, підтримувала міжнародну співпрацю та працювала над підвищенням обізнаності суспільства щодо кіберзагроз.

Отже, кожна з досліджуваних нами країн на сьогодні має розгалужену систему забезпечення кібербезпеки у вигляді нормативно-правової бази, інституційних структур та особливостей міжнародного співробітництва. У

подальшому аналізі їхньої «успішності» щодо захищеності кіберпростору ми виокримо напрямки, які бажано було б перейняти Україні.

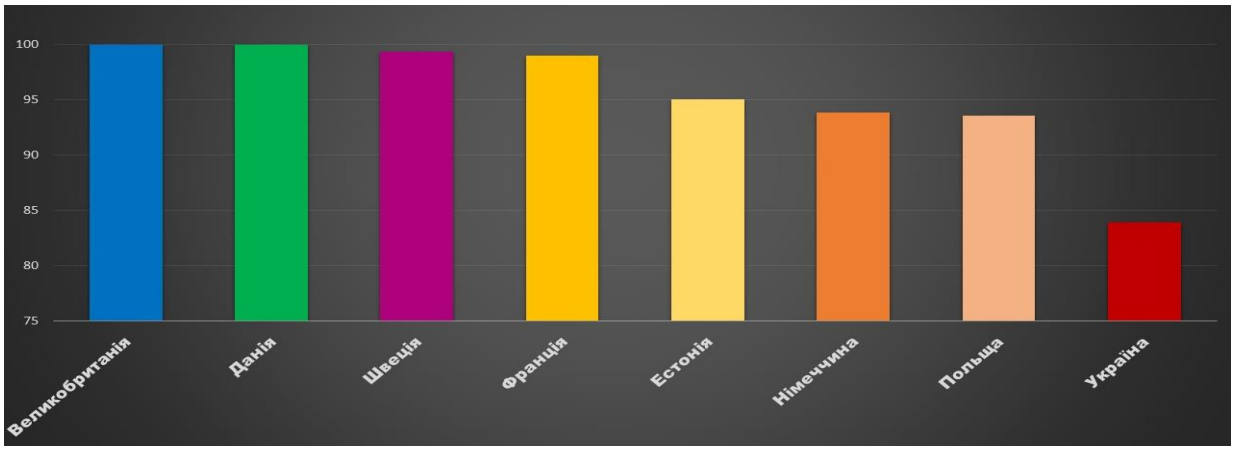
2.3. Досягнення країн Європейського регіону в забезпеченні кібербезпеки та їх роль у подальшому вдосконаленні шляхів протидії кібертероризму в Україні

Визначаючи сьогодні досягнення та недоліки в забезпеченні кібербезпеки кожної з країн зважають на так звані «індекси кібербезпеки». Кожен з цих індексів має власну методологію і згідно з кожним із них країни посідають різні позиції.

Найновіші дані щодо стану кібербезпеки на сьогодні викладені у GCI [222, с. 109 – 112, 119,121,125 – 127], виданий Міжнародною Спілкою електрозв'язку (МСЕ). Цей індекс демонструє комплексний підхід, акцентуючи увагу не лише на технологічних аспектах, а й на нормативно-правових, політичних, освітніх та організаційних компонентах. Така всеохопна методологія GCI дозволяє отримати всебічну картину стану кібербезпеки в кожній країні. Отже, країни, які активно працюють над розвитком нормативної бази, мають гарно розгалужену інституційну структуру, сильну кооперацію на міжнародному рівні та інвестують у підготовку спеціалістів, за індексом GCI мають вищі оцінки. Проаналізувавши звіт МСЕ за 2024 рік, вважаємо за доцільне продемонструвати результати по згадуваних країнах у такому графіку:

Рис.2.1

Загальна оцінка кібербезпеки згідно з GCI (укладено автором за матеріалами [222])



Ще одним індексом, який вимірює кібербезпеку, є NCSI [223]. Він розроблений Естонським департаментом інформаційних систем (RIA) для оцінювання рівня готовності країн до кіберзагроз та здатності забезпечити кібербезпеку. Цей індекс покликаний надати актуальну інформацію про національні заходи з кібербезпеки, допоможе з'ясувати практичні можливості країн щодо запобігання та реагування на кібератаки, а також забезпеченість їх законодавчої бази.

Порівнюючи ці індекси, звертаємо увагу, що МСЕ використовує комплексний підхід для оцінювання рівня кібербезпеки країн у межах Глобального індекса кібербезпеки. Він базується на п'яти основних позиціях, кожна з яких відповідає певному аспекту кібербезпеки, що дає змогу отримати всебічне розуміння рівня готовності країни до кіберзахисту.

Тож, перевагою підходу МСЕ є саме його всебічність, однак він також має свої недоліки, зокрема, методологія залежить від самозвітування країн, що може спотворювати результати. Підхід більшою мірою зосереджений на наявності політик, ніж на їх ефективності.

Першою ж перевагою NCSI можна назвати актуальність, адже, на відміну від GCI, який оновлюється раз на два роки, NCSI оновлюється динамічно та регулярно, що забезпечує більш актуальні дані та дозволяє швидко відображати зміни у національних політиках держав та їх заходах кібербезпеки. NCSI

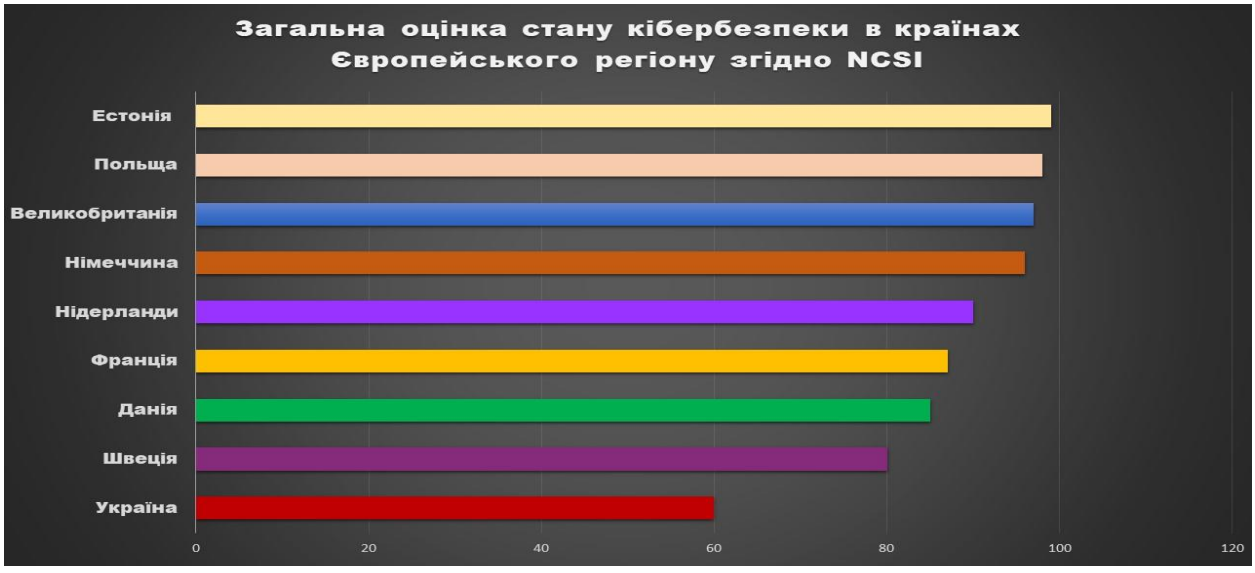
використовує відкриті джерела для збору даних, що знижує залежність від самозвітування країн і робить оцінювання більш об’єктивним. Що стосується індекса, то він більшою мірою зосереджується на практичній готовності країни до кіберзагроз, уключаючи наявність національних CERTs, на захисті критичної інфраструктури та реагуванні на кіберінциденти. Це дає змогу отримати більш точну оцінку реальної готовності країни до кіберзагроз, натомість МСЕ більше уваги акцентує на оцінці нормативно-правової та організаційної баз.

Методології МСЕ та NCSI можуть працювати комплементарно, доповнюючи одна одну у формуванні більш розгорнутої картини стану кібербезпеки кожної країни.

Проаналізувавши дані NCSI за період 2022 – 2024 рр., можемо презентувати загальний рейтинг забезпечення кібербезпеки держав Європейського регіону таким чином:

Рис.2.2

Загальна оцінка кібербезпеки згідно з NCSI (складено автором за матеріалами [223])



Порівнявши обидві діаграми, зауважимо, що загальна оцінка стану кібербезпеки держав та їх рейтинг є досить різними. У першій таблиці, яка демонструє загальну оцінку кібербезпеки, Велика Британія і Данія отримали загальну оцінку 100 балів зі 100 можливих. Це свідчить про те, що ці країни

досягли найвищого рівня кіберзахисту, відповідно до оцінюваних критеріїв і згідно з аналізом володіють усіма необхідними елементами ефективної кібербезпеки: законодавчою базою, технічними заходами, інституційними структурами, нарощуванням потенціалу та заходами співпраці. Хоч обидві країни не є абсолютними лідерами, але мають високі показники в рейтингах NCSI. Це вказує на те, що існують деякі відмінності в методах вимірювання.

Естонія є країною з високим рівнем кібербезпеки. Її загальний показник кібербезпеки становить 95,04, що є трохи нижчим від показника Франції, Нідерландів і Швеції, водночас Естонія посідає одну з найвищих позицій серед країн, представлених в рейтингу NCSI. Вважаємо, що це пов'язано із особливостями стратегії Естонії, яка орієнтована не тільки на внутрішню безпеку, але й на активне міжнародне співробітництво. Естонія вже давно є визнаним лідером в області цифрового управління і кібербезпеки, активно співпрацює з іншими державами та міжнародними організаціями. Участь у таких міжнародних ініціативах дозволяє їй підтримувати високу позицію в індексі NCSI, який оцінює глобальні зусилля країн.

Швеція і Нідерланди також показують відмінні результати. Швеція має 99,31 бали за загальним показником кібербезпеки, Нідерланди – 99,22. Це свідчить про те, що забезпечення кібербезпеки цих країн перебуває на дуже високому рівні. Згідно з індексом NCSI ці країни не є лідерами, але все ж займають провідні позиції. Можливим поясненням цього факту є те, що за останній рік названі країни не оновили інформації. Однак, незважаючи на відсутність останніх даних, динамічний аналіз протягом декількох років показує, що в обох країнах існує баланс між внутрішніми заходами кібербезпеки та міжнародною координацією. Їх високі показники можуть свідчити про наявність сильної нормативно-правової бази, ефективної політичної та інституційної структур.

Німеччина і Франція займають сильні позиції в загальному рейтингу кібербезпеки з 93,84 і 98,98 балами відповідно, що свідчить про добре розвинені в цих країнах заходи кіберзахисту. Їх показники дуже високі в рейтингах NCSI,

що, на нашу думку, підтверджує, що в країнах ефективна політика в галузі кібербезпеки, добре організована нормативно-правова база та приділяється значна увага міжнародному співробітництву.

Україна ж демонструє дещо нижчі результати порівняно з вищезазначеними країнами. Її загальний бал із забезпечення кібербезпеки згідно з нашим аналізом індексу GCI становить 83,93, що є найнижчим показником серед аналізованих країн. Це свідчить про те, що в нашій країні необхідно значно поліпшити політику кібербезпеки, а саме: вжити відповідні організаційні заходи, розширити інституційний складник, удосконалити нормативно-правову базу та підвищити рівень координації між державними й приватними організаціями. Позиція України в рейтингу NCSI також низька стосовно інших Європейських країн, хоча на сьогодні Україна посідає 21 місце в світі згідно з індексом NCSI, що є гарним показником. Занизький рівень багатьох компонентів, що є результатом нещодавніх викликів, з якими зіткнулася Україна, уключаючи кібератаки і загрози, пов'язаний із поточною геополітичною ситуацією. Однак, незважаючи на складність ситуації, необхідність розширення інституційного потенціалу та підвищення рівня координації з іншими країнами має стати одним із пріоритетів, адже зусилля зі створення більш стійкої системи кіберзахисту зможуть поліпшити становище України в майбутньому.

Отже, розглянувши досвід забезпечення кібербезпеки в державах Європи, структурувавши їх та визначивши основні досягнення й недоліки, можемо наголосити на тому, що забезпечення кібербезпеки в Україні повинно ґрунтуватися на комплексному підході, який поєднує вже наявні елементи з адаптацією передового досвіду провідних європейських держав, таких, як Естонія, Данія, Німеччина, Франція та інші, а також із впровадженням інноваційних рішень, відповідно до особливостей українського контексту. Такий підхід дозволить досягти максимального рівня ефективності та стійкості національних кіберсистем, ураховуючи новітні тенденції та загрози у сфері цифрової безпеки.

Отже, згідно з проведеним нами аналізом, виділимо основні переваги, на які ми звернули увагу під час дослідження кіберзахисту кожної країни і визначимо, які з них важливо було б перейняти українській політиці кібербезпеки.

По-перше, створення національних стратегій кібербезпеки. Багато країн Європи розробили чіткі національні стратегії кібербезпеки. Ідеальним прикладом ми вважаємо Естонію, яка реалізувала чотири послідовні стратегії кібербезпеки, що забезпечили системний розвиток кіберзахисту держави, створили основи національної стійкості, сприяли міжнародній співпраці й забезпечили інтеграцію кібербезпеки у всі сфери управління, що є вкрай важливим. Хоча Україна вже має Національну стратегію кібербезпеки [37], яка визначає ключові напрями розвитку, її необхідно розширювати з огляду на сучасні виклики, інтеграцію стандартів та угод, установлених у міжнародній політиці.

По-друге, розгляд внутрішньої нормативно-правової бази. Тут варто звернути увагу на національне законодавство щодо забезпечення кібербезпеки. Лідерами в цьому напрямку можна назвати Німеччину та Францію. Німеччина відрізняється більш деталізованим і всебічним законодавством, тоді як Франція робить акцент на захист критичної інфраструктури через зобов'язання дотримуватися встановлених кіберзахисних стандартів. Обидві країни є прикладами для інших держав Європи у створенні ефективного правового поля для кібербезпеки, однак Німеччина має більш комплексний підхід, що забезпечує ширший рівень захисту.

Розглядаючи досвід України щодо законодавчого підґрунтя, зауважимо, що на сьогодні в Україні діє понад тисячу законодавчих актів, які тим чи іншим чином регулюють питання кібербезпеки. Проаналізувавши їх, виділимо найбільш ключові.

Основним нормативним актом є Закон України «Про основні засади забезпечення кібербезпеки України» [36], який визначає принципи забезпечення кібербезпеки, окреслює основні напрямки державної політики та

визначає відповідальних за її реалізацію суб'єктів. Однак, попри визначені цілі, цей закон має суттєві недоліки в контексті реагування на новітні кіберзагрози, що швидко еволюціонують. Важливими залишаються питання втілення його положень на практиці та створення умов для інтеграції нових технологій захисту в критичні інфраструктури. Закон України «Про національну безпеку України» [39], основною метою якого є інтеграція кібербезпеки в загальну систему національної безпеки через створення механізму координації між національними відомствами та надання стратегічних рекомендації щодо запобігання кіберзагрозам. Однак вважаємо, що деякі положення в ньому є нечітко прописаними, недостатньою є деталізація заходів координаційної політики та застарілі підходи. Це, на нашу думку, завдає значних проблем в його практичній реалізації. Закон України «Про оборону України» [224] містить згадки про кібероборону та активний кіберзахист, однак не містить чіткого визначення кіберпростору як окремого самостійного напряму бою. Таке трактування залишає простір для інтерпретацій, що може ускладнювати координацію заходів з кібероборони, визначення повноважень органів державної влади та створення відповідних структур для захисту від кіберзагроз. Відсутність визначеного статусу кіберпростору як окремої сфери оборонної діяльності також може гальмувати розвиток законодавства, технологічних спроможностей, підготовки спеціалістів у цій сфері, а також політики її реалізації, що є критичним для забезпечення ефективного захисту національної безпеки в умовах сучасних викликів.

Стратегія воєнної безпеки України 2021 року [225] визначає всеохопну оборону, яка включає, зокрема, протидію загрозам у кіберпросторі. У ній наголошується на необхідності протидії агресії у кіберпросторі, а також забезпеченні кібербезпеки під час оборонних дій. Однак значна частина положень щодо кібербезпеки залишається узагальненою і потребує конкретизації з урахуванням сучасних викликів. Основний недолік документа полягає в тому, що Стратегія не відображає повного масштабу кіберзагроз, особливо в сучасній геополітичній ситуації, в якій опинилася Україна після

повномасштабного вторгнення у 2022 році, яке супроводжувалося активізацією кібератак на критичну інфраструктуру. Оновлення мають включати деталізований план розвитку кібероборони, чітку координацію дій з міжнародними партнерами та забезпечення посиленого кіберзахисту критично важливих об'єктів.

Закон України «Про боротьбу з тероризмом» [226] формує правові та організаційні основи боротьби з тероризмом, визначаючи компетенції державних органів, їх координацію та принципи захисту прав людини в умовах антитерористичної діяльності. Однак, попри наявні регулювальні положення, він не враховує сучасних форм терористичної діяльності в кіберпросторі, оскільки не дає конкретного визначення кібертероризму та не вказує на ефективні механізми боротьби з ним. Відсутня також координація між різними державними установами, що призводить до дублювання функцій або прогалин в безпеці. Незважаючи на заяви про дотримання прав людини, гарантії захисту громадян під час проведення антитерористичних операцій залишаються слабкими, що може призвести до порушення прав і свобод людини і зруйнувати суспільний порядок у державі. Термінологія в законі застаріла, зокрема для більш чіткого розуміння загроз у цифровому середовищі «технологічний тероризм» потрібно замінити на «кібертероризм». Крім того, уніфікація керівництва антитерористичного управління обмежує своєчасність реагування й вимагає більшої гнучкості у прийнятті рішень.

Постанова Кабінету Міністрів України «Про затвердження Правил антитерористичної безпеки» [38] установлює базові межі для захисту об'єктів від терористичних загроз, зокрема й кібертероризм, але, на нашу думку, демонструє недостатність системного підходу до сучасних кіберзагроз. Відсутність чітких механізмів моніторингу та реагування на кіберінциденти, а також слабке врахування проактивних методик і міжнародного співробітництва з кібербезпеки створюють серйозні прогалини в державному регулюванні та забезпеченні життєдіяльності суспільства.

Закони України «Про інформацію» [227], «Про доступ до публічної інформації» [228], «Про електронні комунікації» [229], «Про захист інформації в інформаційно-комунікаційних системах» [230], «Про державну таємницю» [231] та «Про захист персональних даних» [232] формують основу політико-правового регулювання інформаційного простору в Україні. Вони визначають принципи отримання, використання та захисту інформації, установлюють порядок доступу до публічної інформації, регламентують діяльність у сфері електронних комунікацій, захищають інформацію в інформаційно-комунікаційних системах, регулюють питання державної таємниці та забезпечують захист персональних даних громадян. Зі стрімким розвитком інформаційних технологій, а також із зростанням поширення кіберзагроз виникає проблема щодо необхідності включення положень про кібербезпеку в зазначені нормативно-правові акти. На наш погляд, такий крок забезпечить можливість комплексного характеру захисту інформаційного простору держави, підвищить рівень безпеки як громадян, так і державних установ, а також сприятиме гармонізації національного законодавства з міжнародними стандартами щодо забезпечення кібербезпеки. Зазначені дії вважаємо максимально корисними та адаптивними задля зміцнення національної безпеки у протистоянні сучасним викликам, спричиненим цифровою революцією.

Тож, підбиваючи підсумки проведеному аналізу нормативно-правового регулювання питання кібербезпеки в Україні, зазначимо, що в країні, попри наявність великого обсягу нормативних актів, правове регулювання кібербезпеки залишається недостатньо ефективним, оскільки вказані законодавчі акти часто не враховують специфіки сучасних кібертерористичних загроз, що постійно еволюціонують, а також діють нарізно, створюючи суттєві виклики для ефективного державного управління та забезпечення національної безпеки. Така фрагментація законодавства ускладнює формування цілісної державної політики у сфері кібербезпеки. Водночас велика кількість термінів (та їх синонімів) уживається розрізнено, часто терміни суперечать один одному.

Чинна законодавча база не охоплює всіх аспектів кібертероризму, що створює значні прогалини у правовому регулюванні цієї проблеми.

Відсутність єдиного підходу до регулювання кібербезпеки призводить до неузгодженості дій між різними державними органами, а також до конфлікту повноважень та неефективного використання ресурсів. Це послаблює здатність країни реагувати на кіберзагрози, що є викликом інформаційній, національній, політичній та економічній безпеці. Важливим уважаємо оновлення чи скасування положень застарілих законодавчих актів, які не враховують сучасного стану подій. Схожі між собою концепції законодавчих актів, перерахованих вище, доцільним, на нашу думку, було б, усебічно проаналізувавши, об'єднати в один. Таке реформування значно спростить регулювання питань кібербезпеки та активізує її розвиток в Україні. Щодо політичної перспективи, то уніфікація положень кібербезпеки в більш структуровану законодавчу базу матиме вирішальне значення. Такі зміни сприятимуть посиленню інституційної спроможності країни, підвищенню довіри громадян до державних структур та забезпеченню верховенства права в цифровому середовищі. Крім того, це дозволить Україні ефективніше співпрацювати з міжнародними партнерами й узгоджувати національні стандарти з міжнародною практикою та зобов'язаннями.

По-третє, важливим аспектом для дослідження політичних особливостей кібербезпеки є інституційний складник. Слід зазначити, що лідерами серед європейських країн, згідно з нашим аналізом, є Швеція та Нідерланди. Країни побудували найбільш розвинені і всебічні інституційні системи кібербезпеки, які забезпечують як національну, так і міжнародну стійкість до кіберзагроз, демонструючи комплексний підхід до координації на національному рівні, залучаючи державу, бізнес і громадськість до забезпечення стійкості країни до кіберзагроз. Україна, зіткнувшись з постійними кіберзагрозами, особливо від початку російської агресії, ще з 2014 року почала активно розвивати свої інституційні механізми кібербезпеки, проте поки що вони залишаються в процесі становлення порівняно з європейськими лідерами.

Одним із ключових органів, який відповідає за кібербезпеку України, є Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) [233]. Цей орган працює над захистом державних інформаційних ресурсів та координує роботу з кібербезпеки.

Важливу роль відіграє також Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони [234], що забезпечує координацію між різними відомствами для реагування на кіберзагрози. Крім того, в Україні існує Служба безпеки України [235], яка відповідає за протидію кіберзлочинності та кібертероризму, Міністерство оборони України, яке координує питання кібероборони, а також Національна поліція України, яка розслідує кіберзлочини, що впливають на цивільний сектор.

Міністерство цифрової трансформації України [236] додатково розробляє окремі питання політики цифрової безпеки, розвиваючи відповідну інфраструктуру. Важливими суб'єктами кібербезпеки є також Центр реагування на комп'ютерні надзвичайні події України CERT – UA [237], який здійснює моніторинг та реагування на кіберінциденти.

У цьому контексті важливо також з’ясувати наявні проблеми щодо діяльності цих структур. Ефективність їхньої діяльності часто вимагає удосконалення, адже обмежена кількість кваліфікованих фахівців, слабка координація між органами та низький рівень обізнаності громадян щодо основних принципів кібербезпеки є основними викликами кібербезпеці України.

ДССЗЗІ, яка є ключовим органом із кібербезпеки, часто стикається з труднощами у забезпеченні належного рівня захисту через обмеженість ресурсів та повноважень. CERT–UA як орган, що має завдання боротися з кіберзлочинами, також потребує посилення своїх можливостей для забезпечення своєчасного і адекватного реагування на загрози. Окрім того, пропонуємо крок реформування CERT–UA у вигляді розподілу повноважень між підструктурами, які б забезпечували належний рівень кібербезпеки в кожному секторі критичної інфраструктури окремо. Важливо, щоб він

виконував координаційну функцію державної політики щодо кіберзахисту, а його підгрупи, наприклад CERT – HC, відповідав би за кібербезпеку в охороні здоров'я; CERT – NE – за кібербезпеку в енергетиці; CERT – LR – відповідав би за кібербезпеку щодо здійснення правопорядку, правосуддя, тримання під вартою, а також цивільного захисту населення та територій; CERT – ECI – за кібербезпеку в галузі електронних комунікацій та інформаційних послуг і т. ін. Спеціалізовані підходи до кожної галузі допоможуть ефективніше реагувати на кіберзагрози, зменшуючи ризики поширення атак та забезпечуючи стійкість систем. Розмежування повноважень дозволить створити окремі підрозділи CERT– UA, які зможуть зосереджуватися на специфічних особливостях відповідних напрямів, підвищуючи рівень захисту та оперативність реагування. Це також допоможе покращити координацію з галузевими організаціями та експертами, що сприятиме ефективному обміну інформацією, проведенню профілактичних заходів та наданню швидкої допомоги у разі кіберінцидентів. Таким чином, спеціалізація підрозділів CERT – UA відповідно до галузей критичної інфраструктури може суттєво підвищити ефективність реагування на кіберзагрози й забезпечити більш адаптований захист кожної конкретної сфери, враховуючи її особливості.

На нашу думку, потребує більшої взаємодії з іншими відомствами та міжнародними партнерами для ефективної реалізації заходів безпеки й ще одна інституційна одиниця – СБУ, яка є відповідальною за протидію будь-яким видам злочинів, зокрема і в кіберпросторі.

Важливу роль у забезпеченні координації між державними органами відіграє Національний координаційний центр кібербезпеки при РНБО, але відсутність чітких регламентів взаємодії між різними суб'єктами кібербезпеки та приватним сектором значно ускладнює реалізацію комплексної стратегії кіберзахисту. Це особливо актуально в умовах, коли значна частина критичної інфраструктури належить приватним компаніям, а ефективна співпраця між державними і приватними структурами є ключовим чинником для забезпечення кібербезпеки.

Як засвідчує аналіз відповідних матеріалів, на Україну припадає 1/5 частина кібератак, особливо кібертерористичних, від загальної кількості світових атак [238]. З огляду на це можемо зробити висновок, що недостатня інституційна політика на практиці призводить до того, що реакція на кіберінциденти є повільною і часто неадекватною щодо масштабів загроз. Відсутність чітко прописаних механізмів координації між державними установами та приватним сектором ускладнює обмін інформацією і спільну протидію будь-яким виявам кіберзлочинності, у тому числі кібертероризму.

Задля часткового вирішення указаної проблеми варто звернути увагу на Антитерористичний Центр України [239], завдання якого полягають у виявленні та запобіганні терористичних загроз, захисті критичної інфраструктури, а також на забезпеченні реагування в разі терористичних актів. Центр співпрацює з державними та міжнародними структурами, однак, на нашу думку, потребує розширення функцій для протидії кібертероризму. У сучасних умовах гібридних загроз та зростання значення кіберпростору для національної безпеки інтеграція кібернетичного та фізичного захисту в межах діяльності Антитерористичного Центру є важливим напрямком для посилення ефективності протидії тероризму. Ідея поєднання фізичного захисту, тобто традиційних заходів з протидії терористичним атакам, та кібернетичного компоненту як відповіді на виклики у цифровому середовищі віддзеркалило б сучасний підхід до політики безпеки, який урахував би складність і багатошаровість сучасних кіберзагроз.

Діяльність Антитерористичного Центру при Службі Безпеки України потребує стратегічного переосмислення з урахуванням сучасних політичних викликів та загроз у кіберпросторі, які сьогодні дедалі більше зростають. У світі, де кібертероризм став потужним інструментом впливу на держави і суспільства, розширення можливостей Антитерористичного Центру в галузі кібербезпеки є не тільки внутрішньою необхідністю, а й важливим інструментом позиціонування зовнішньої політики України. Це питання є не лише технічною чи юридичною змінною, а й політичним сигналом про те, що

Україна, незважаючи на складність військово-політичного стану через війну, готова брати активну участь у забезпеченні регіональної та міжнародної безпеки.

Ще одним важливим політичним складником інтеграції кібертероризму в діяльність Антитерористичного Центру є перетворення України з держави, яка переважно захищає себе, в таку, що активно формує міжнародну політику безпеки. Для цього необхідно чітко пов'язати розширення функцій центру зі стратегічними цілями – вступом України до Європейського Союзу і Північноатлантичного альянсу. Оскільки цифрові загрози вже становлять одну з найбільших небезпек для держав – членів цих організацій, ЄС і НАТО насамперед зосереджені на зміцненні кібербезпеки. Володіючи унікальним досвідом протидії гібридним загрозам з боку Росії, Україна може надати інформацію і методики захисту кіберпростору, які є винятковими й дозволяють протягом довгого часу стримувати ворога, що стане важливим аргументом на користь інтеграції України до зазначених структур.

У цьому контексті розширення на національному рівні функцій Антитерористичного Центру має бути спрямоване на:

– внутрішню координацію з Кіберполіцією та CERT–UA у системну та скоординовану боротьбу з кіберзагрозами. Такий підхід вимагає створення на базі Антитерористичного Центру єдиного центру управління антитерористичними операціями, який об'єднуватиме технічний, оперативний і стратегічний потенціали різних органів. Новостворена структура має базуватися на стику Кіберполіції, яка може забезпечувати оперативне реагування та розслідування кіберзлочинів, CERT – UA, що відповідатиме за моніторинг, аналітику та технічну нейтралізацію загроз, і власне Антитерористичного Центру, який виконуватиме роль координатора, що інтегрує ці процеси в загальнодержавну антитерористичну стратегію. Пропонована структура має стати одним із департаментів Міністерства оборони України. Такий крок підкреслить, що протидія загрозам у кіберпросторі є настільки ж важливою, як і фізична безпека, а також визнає кіберпростір

окремою ареною військового протистояння. На нашу думку, така взаємодія не лише зміцнить національну стійкість до кіберзагроз, а й забезпечить політичну та стратегічну роль України в системі міжнародної безпеки;

– зовнішньо-політичну кооперацію з ключовими агенціями, що регулюють питання кібербезпеки в Європі та світі. Нинішня співпраця України з ENISA і CCDCOE має вийти на новий рівень, коли Україна є не тільки партнером, а й бере активну участь у встановленні стандартів кібербезпеки. Наприклад, у межах CCDCOE Україна може почати створення додаткового Центру по боротьбі з кібертероризмом, який буде виконувати як аналітичні, так і оперативні функції. Такий центр, що базуватиметься в Україні, буде платформою для спільних навчань, моделювання та розробки стратегій боротьби з терористичною загрозою в кіберпросторі.

Запропонована координація зможе стати платформою для спільних навчань, симуляцій та розробки стратегій протидії терористичним загрозам у кіберпросторі. Ця ініціатива дасть змогу розширити політичний порядок денний України в межах співробітництва з НАТО, створивши додаткові аргументи для вступу до Альянсу. Поглиблення співпраці з ENISA має включати систематичну участь України у створенні регіональної мережі центрів кібербезпеки. Це стане кроком на шляху інтеграції України в спільний європейський цифровий простір, що є важливим критерієм для вступу до ЄС. У політичному сенсі така ініціатива дозволила б Україні утвердитися як держава, здатна не лише використовувати здобутки, а й сприяти зміцненню колективної безпеки.

Інтеграція боротьби з кібертероризмом у пріоритети Антитерористичного Центру також повинна бути пов'язана з розробленням національного законодавства відповідно до стандартів ЄС та НАТО. Це буде означати не тільки технічні вдосконалення, а й створення політичної і правової баз, що забезпечить прозорість і ефективність роботи агентств кібербезпеки. Такий підхід підкреслює прагнення України дотримуватися принципів демократії, які є основними вимогами для об'єднання обох структур.

Важливим аспектом також є можливе майбутнє розширення функцій Антитерористичного Центру у створенні іміджу України як держави, готової взяти активну участь у формуванні нової системи глобальної безпеки. Відповідна ініціатива, яка буде спрямована на зміцнення співпраці між НАТО і ЄС в галузі кібербезпеки, є не тільки важливим кроком у захисті від сучасних загроз, а й політичним аргументом на користь інтеграції України в ці організації. У цьому контексті кібербезпека стане не тільки засобом захисту, але й механізмом зміцнення міжнародного статусу України та просування національних інтересів на світовому рівні.

Беручи до уваги сучасні політичні передумови, зокрема те, що методи ведення терористичної діяльності визначили новою «ареною протистояння» кіберпростір як основний засіб, варто підкреслити, що зараз гібридні загрози несуть в собі інше розуміння традиційного тероризму та поєднують діяльність у кіберпросторі з фізичним тероризмом, що, своєю чергою, вимагає модифікації органів безпеки.

Антитерористичний центр, який зараз займається фізичними аспектами тероризму, має перетворитися на агенцію, здатну об’єднати обидва аспекти безпеки в єдину систему реагування. Такий підхід, як нам видається, сприятиме швидшій та скоординованій реакції на різної складності загрози, усуненню адміністративних перешкод та прийняттю ефективних заходів протидії, а це ліквідує неузгодженість роботи різних органів безпеки, створить інституційну базу для нових форм внутрішньої та зовнішньої співпраці й дозволить Україні лідирувати у створенні норм боротьби із кібертероризмом в Європі. З точки зору євроатлантичної інтеграції це також буде політичним посилом, який засвідчить, що Україна готова долучитися до вирішення проблем глобальної безпеки.

На сьогодні в Україні немає прецеденту об’єднання фізичних і кібернетичних антитерористичних структур в одне «тіло», а тому запропонована модель може бути піонером такого роду в умовах гібридної війни, а також виступати гарним прикладом для інших країн, які стикаються з

подібними викликами і шукають інноваційні шляхи зміцнення національної безпеки.

Усі ці заходи разом створять умови для підвищення стійкості кіберсистем України до сучасних загроз, захисту національних інтересів та забезпечення безпеки громадян у цифровому середовищі.

Отже, стратегія забезпечення кібербезпеки України повинна спиратися на комплексний підхід, що передбачає вдосконалення законодавчої бази, розвиток інституційних механізмів, упровадження освітніх програм, технічне зміцнення критичних інфраструктур та розширення міжнародної співпраці. Усі ці заходи разом, на наше переконання, створять умови для підвищення стійкості України до сучасних кіберзагроз, захисту національних інтересів і забезпечення безпеки громадян у цифровому середовищі.

Задля досягнення цієї мети ми пропонуємо розробити певну «формулу забезпечення кібербезпеки», що містила б чотири ключові компоненти, які, згідно з проведеним нами дослідженням, найбільше впливають на стан кібербезпеки будь-якої держави: інтеграцію, адаптацію до загроз, інновації та прогресивну кіберосвіту суспільства. Інтеграція передбачає тісну співпрацю між різними секторами та міжнародними партнерами, що має стати одним із напрямків державної політики України. Адаптація забезпечує гнучкість у реагуванні на нові загрози та швидке вдосконалення законодавчої бази. Інновації стосуються впровадження новітніх технологій, таких, як штучний інтелект та машинне навчання для моніторингу й захисту від атак. Прогресивна кіберосвіта спрямована на підготовку фахівців і формування культури кібергігієни серед населення. Розглянута формула має потенціал стати основою для розробки нових стратегій та політик у галузі кібербезпеки, спрямованих на захист цифрового суверенітету України й забезпечення її стійкості до сучасних викликів у цифровому просторі.

Для забезпечення останнього складника з метою гарантування захисту в цифровому середовищі та підвищення обізнаності суспільства пропонуємо також розглянути створення «Національної програми кіберосвіти».

Аналізуючи можливі причини виникнення цієї ідеї, хочемо відмітити, що в Україні значно загострилася проблема кадрового дефіциту у всіх напрямках. Велика кількість фахівців, які раніше працювали в галузі кібербезпеки, була мобілізована до лав Збройних Сил України або змушена була покинути країну. Військова ситуація також уплинула на здобувачів і молодих фахівців, які планували або вже почали своє навчання в галузі кібербезпеки. Через руйнування освітньої інфраструктури, перебої в навчальному процесі та потребу деяких здобувачів брати участь у військових діях або виїжджати з країни процес підготовки нових фахівців значно ускладнився. Ці обставини призвели до відчутного кадрового дефіциту, що, своєю чергою, створило кілька критичних викликів для реалізації національної програми кіберосвіти. Зокрема, це вплинуло на здатність підтримувати необхідний рівень кіберзахисту критичної інфраструктури, державних інституцій та приватного сектора. Брак фахівців призвів до збільшення вразливості перед кіберзагрозами, особливо в умовах, коли інтенсивність кібератак з боку агресора зросла. Виклики також виникають і в частині навчання нових фахівців. Зменшення кількості досвідчених інструкторів та викладачів, які можуть ефективно передавати знання, ускладнило підготовку нових поколінь кіберспеціалістів. Багато кваліфікованих викладачів залучені до забезпечення обороноздатності країни або змушені перебувати за кордоном, що обмежує їхню можливість брати участь у навчальному процесі.

Крім цього, труднощі полягають і в організації практичних занять, які є надзвичайно важливими для підготовки фахівців з кібербезпеки. Обладнання, необхідне для проведення таких занять, часто залишається недоступним через військові дії або руйнування освітніх закладів. Таким чином, проблема кадрового «голоду» стає критичною перешкодою на шляху до підвищення кібербезпеки країни в умовах війни, що вимагає швидких та ефективних рішень, таких, як дистанційні програми навчання, співпраця з міжнародними партнерами, а також державні ініціативи щодо підтримки фахівців у країні.

Основною метою національної програми кіберосвіти є підготовка фахівців у галузі кібербезпеки та формування обізнаного суспільства, здатного протистояти кіберзагрозам. Щоб забезпечити комплексний підхід до безпеки в цифровому середовищі, програма має передбачати не лише навчання спеціалістів у галузі кібербезпеки, яке є постійним, а й уведення обов'язкового щорічного підвищення кваліфікації для представників усіх професій, які належать до забезпечення критичної інфраструктури.

Вважаємо, що завдання програми мають бути такі:

1) розроблення єдиного освітнього стандарту з кібербезпеки для всіх спеціальностей;

2) створення навчальних курсів та матеріалів, які будуть доступні через різноманітні платформи;

3) перепідготовка та сертифікація державних службовців, працівників критичної інфраструктури та приватного сектору;

4) масове інформування населення про проблеми кібербезпеки через засоби масової інформації та просвітницькі заходи.

Правове регулювання впровадження системи національної кіберосвіти має базуватися на чинному законодавстві України. Це допоможе не тільки зробити кіберосвіту ефективною, але й узгодити її з національними стратегіями щодо безпеки та освіти.

Ключовими серед нормативно-правових засад формування та функціонування такої системи мають бути:

– Закони України: «Про інформацію» [227], «Про захист інформації в інформаційно-телекомунікаційних системах» [230], «Про електронні документи та електронний документообіг» [240], «Про захист персональних даних» [232], «Про державну таємницю» [231], «Про основні засади забезпечення кібербезпеки України» [36], «Про Державну службу спеціального зв'язку та захисту інформації України» [241], «Про національну безпеку України» [39], «Про правовий режим воєнного стану» [242], «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [243];

– Національна стратегія кібербезпеки України [36];

– Постанови Кабінету Міністрів України: «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» [244], «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» [245], «Про затвердження Положення про організаційно-технічну модель кіберзахисту» [246], «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» [247], «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» [248].

Однак, окрім законодавства, яке забезпечує питання кібербезпеки України, необхідним для розробки Національної програми кіберосвіти в Україні є дотримання концепцій Законів України «Про вищу освіту» [249], «Про освіту дорослих» [250], «Про Національну програму інформатизації» [251].

Положення про впровадження програми Національної кіберосвіти, а також Закону України «Про критичну інфраструктуру» важливо включити в ці закони [252].

Ми вважаємо такі дії необхідними задля забезпечення професійної компетентності тих, хто працює із критичними об'єктами, а також їх кіберзахист. Уведення положень щодо освіти та підвищення кваліфікації забезпечить систематичну підготовку спеціалістів для ефективного захисту та стійкості критичної інфраструктури. Конкретно пропонуємо додати норму, яка б передбачала обов'язкову підготовку, перепідготовку та підвищення кваліфікації для працівників захисту критичної інфраструктури. Ми вважаємо, що обраний напрямок допоможе не тільки підвищити рівень знань, але й сприятиме адаптації до нових викликів та технологій щодо захисту критичної

інфраструктури. У додатках необхідно подати розроблені нові підзаконні акти щодо сертифікації та акредитації освітніх програм із кібербезпеки, які впроваджуватимуться для державних службовців та співробітників критичної інфраструктури.

Важливим елементом розробки Національної програми кіберосвіти є міжнародне співробітництво з освіти в галузі кібербезпеки. Співпраця з такими організаціями, як НАТО, ЄС, ОБСЄ, МСЕ, Інтерпол, дозволятиме інтегрувати передові стандарти кіберзахисту та покращувати кваліфікацію українських кіберфахівців. Однак важливо не тільки адаптувати міжнародний підхід, а й ураховувати особливості національної безпеки, удосконалити власну систему кібербезпеки, забезпечивши стійкість до особливих викликів України. Залучення НАТО до розбудови кіберстійкості є важливим аспектом цієї програми. Участь України в навчаннях і тренінгах НАТО дає змогу отримувати практичні навички відповідно до міжнародних стандартів. Проте важливо, щоб адаптація цих стандартів ураховувала національні інтереси та специфіку країни. Співпраця з Європейським Союзом, зокрема у впровадженні Директиви NIS2 та партнерства з ENISA, дозволить адаптувати європейські підходи до управління кіберзагрозами. Це сприятиме розробленню власних стратегій, що продемонструє активну участь України у формуванні європейських стандартів кібербезпеки.

ОБСЄ відіграє значну роль у кібердипломатії України, дозволяючи брати участь у міжнародних діалогах щодо запобігання кіберконфліктам. Це сприяє професійному розвитку українських фахівців та зміцненню міжнародної довіри до України як надійного партнера.

Співпраця з МСЕ допомагає використовувати глобальні стандарти для розроблення національної кіберосвіти та оцінювати ефективність національних заходів через Глобальний індекс кібербезпеки. Це забезпечує системний підхід до покращення підготовки фахівців.

Узаємодія з INTERPOL є важливою для боротьби з кіберзлочинністю та кібертероризмом. Технічна допомога та тренінги для правоохоронців

підвищують кваліфікацію українських фахівців і забезпечують ефективну боротьбу з глобальними загрозами.

Таким чином, посилення взаємодії між Україною та міжнародними організаціями сприятиме не тільки підвищенню рівня національної кіберстійкості, а й створенню сучасної кіберосвіти в Україні. За активної співпраці можна розробити відповідні освітні програми та укласти удосконалені практики із кібербезпеки, а також підвищити рівень підготовки кіберфахівців, що є вкрай важливим для посилення національної безпеки проти глобальних кіберзагроз. Співпраця з іноземними партнерами та використання зарубіжного досвіду дасть можливість упровадити усталені практики з кіберосвіти і не лише зміцнить позиції України на міжнародній арені, але й допоможе інтегруватися у світову систему кібербезпеки.

За нашим планом, навчання із кібербезпеки має передбачати отримання базових знань щодо архітектури комп'ютерних систем, основ мереж та інформаційної безпеки. Наступний рівень – це системний розвиток технічних дисциплін, що дозволить здобувачам мати комплексне бачення того, як здійснюються атаки на інформаційні системи та способи їх уникнення. Пов'язані з сучасними програмами кібербезпеки практичні тренінги та лабораторні роботи, на наш погляд, забезпечать конструктивне середовище для застосування отриманих знань.

Крім того, важливо щоб навчання з кібербезпеки охоплювало не лише технічні аспекти, а й етичні, правові та управлінські, що сприятиме, як ми передбачаємо, формуванню всебічно підготовлених спеціалістів.

На практиці це означає, що програма належним чином дбатиме про створення міждисциплінарних напрямків, які поєднуватимуть розуміння кібербезпеки, наприклад, з правом, менеджментом, бізнесом або медициною. Передбачається, що це дасть кандидату повне та загальне уявлення про те, наскільки кібербезпека стосується різних секторів. Навчальні програми мають бути пристосовані до потреб різних галузей, тож ми пропонуємо інтегрувати в ці сфери знання з кібербезпеки:

– кібербезпека для медичних працівників (захист медичних даних та інформаційних систем у галузі охорони здоров'я; особливості кібербезпеки в сфері електронної охорони здоров’я (eHealth); принципи швидкого реагування на кібератаки; управління медичними системами та обладнанням; стандарти кібербезпеки для управління закладами охорони здоров’я);

– кібербезпека для фінансистів та економістів (управління ризиками в банківській сфері; захист фінансових транзакцій та методи боротьби з шахрайством);

– кібербезпека для працівників енергетики (захист критичної інфраструктури, зокрема енергетичної системи, від кіберзагроз, особливо актуальним це стало сьогодні, коли Україна стикається з гібридними атаками на енергомережу);

– кібербезпека для науковців (захист наукових даних та інтелектуальної власності; захист від кіберзагроз результатів досліджень, баз даних, а також прав на інтелектуальну власність; кібергігієна в наукових проєктах; правила уникнення фішингових атак та безпечного користування науковими мережами і платформами для обміну інформацією);

– кібербезпека для державних службовців (захист державних інформаційних ресурсів; правила зберігання та обробки інформації в державних установах, щоб мінімізувати ризики витоку даних; процедури формування та впровадження ефективної політики інформаційної безпеки; навчання державних службовців швидко і ефективно реагувати на кібератаки, особливо в кризових ситуаціях або під час загроз критичній інфраструктурі; опанування навичками координації з іншими державними установами та міжнародними організаціями для спільної боротьби з кіберзагрозами; правила безпечного обміну даними між дослідниками на міжнародному рівні, зокрема дотримання законодавства про захист персональних даних і протоколів безпеки);

– кібербезпека для юристів (особливості законодавчого регулювання з кібербезпеки; огляд національних та міжнародних законодавчих актів, що регулюють питання кібербезпеки; поглиблене розуміння юридичних наслідків

кіберзлочинів, захист прав жертв кібератак та притягнення винних до відповідальності; основи цифрової експертизи, зокрема, як збирати, аналізувати та використовувати цифрові докази в суді, як забезпечити дотримання прав інтелектуальної власності в кіберпросторі та боротися з такими порушеннями, як піратство або незаконне використання авторських прав).

Така програма дасть можливість кожній професійній групі отримати саме ті необхідні знання, які знадобляться для ефективної роботи в цифровому просторі. Таким чином, розроблення навчальних програм із кібербезпеки буде комплексним процесом, який має включати всі складники – від базових технічних речей до юридичних та етичних питань. Такі плани повинні забезпечити як теорію, так і практичний досвід успішного захисту кіберпростору.

Ще однією ключовою метою Національної програми кіберосвіти в Україні є залучення широких верств населення через освітні програми, що є важливим складником формування кіберграмотності серед населення. Освітні програми для громадян повинні включати кібергігієну, безпечне користування Інтернетом, захист персональних даних, розпізнавання шахрайства та кібербулінгу, адже вкрай важливим завданням є допомогти кожному навчитися захищати себе від потенційних загроз у цифровому середовищі й таким чином підвищити загальний рівень обізнаності щодо кібербезпеки.

Організація громадських кампаній щодо інформування про кібербезпеку є одним із найважливіших компонентів плану. Такі кампанії можуть уключати семінари, вебінари, інформаційні брошури, що стане корисним та допоможе населенню зрозуміти не тільки ризики, але й те як їх уникнути. Одним із важливих інструментів реалізації Програми ми вбачаємо створення національної онлайн-платформи кіберосвіти, яка стане основою для доступу до якісних освітніх ресурсів з кібербезпеки. Платформа міститиме курси, вебінари, тести та сертифікацію з кібербезпеки, гарантуватиме доступ до навчання для всіх охочих. Вона повинна бути інтерактивною, з можливістю користувачів проходити курси на різних рівнях складності – від базового до передового.

Платформа також повинна використовувати новітні технології, такі, як віртуальні лабораторії та симулятори кіберзагроз. Це дозволить відпрацьовувати навички в реальних умовах, що є важливим для їх практичної підготовки.

Таким чином, ухвалення Національної програми кіберосвіти в Україні є відповіддю на сучасні потреби і має стати каталізатором у створенні безпечного кіберпростору в Україні. Така програма буде корисною для підтримки національної безпеки та захисту критичної інфраструктури, що є пріоритетом серед сучасних кіберзагроз. Передбачаємо, що це підвищить рівень кіберосвіти в Україні, посилить національну безпеку, а також підвищить стійкість до кіберзагроз.

Отже, як ми бачимо, забезпечення кібербезпеки в Україні потребує комплексного підходу: удосконалення нормативно-правової бази, розвитку інституційних структур, упровадження інноваційних рішень, адаптації кращих європейських практик та активного міжнародного співробітництва. Стратегію кібербезпеки необхідно розширити та зробити частиною кожного напрямку громадської діяльності, сформувати Національну програму кібербезпеки, яка б готувала професіоналів та підвищувала обізнаність громадськості. Лише завдяки таким зусиллям можна підвищити рівень національної безпеки в цифровому середовищі та стійкість України до кіберзагроз.

ВИСНОВКИ ДО РОЗДІЛУ 2

Таким чином, проблема кібертероризму стає актуальною для держав європейського регіону. Успіх у забезпеченні регіональної безпеки у кіберпросторі, забезпечення захисту секторів національної інфраструктури та створення глобального безпечного інформаційного простору значною мірою залежить від зусиль кожної з держав регіону. Однак технології чи внутрішня політика самі по собі не зможуть забезпечити ефективний захист від кібертероризму. Цей факт свідчить про необхідність широкої взаємодії та координації у вирішенні проблем кібербезпеки.

Як уже було зазначено, Конвенція Ради Європи «Про кіберзлочинність» та Рішення Ради Міністрів ОБСЄ під назвою «Боротьба з використанням Інтернету з терористичною метою» є важливим унеском у протидію кіберзлочинності. Крім того, на національному рівні стратегії кібербезпеки були прийняті в кожній державі Європи й створені органи, які повинні гарантувати належний рівень захисту людей і критичної інфраструктури від будь-якого виду кіберзагрози. Однак, згідно з нашим аналізом, зрозумілим стає те, що Конвенція та два Додаткових Протоколи до неї не містять жодних згадок про кібертероризм, як і Рішення Ради Міністрів ОБСЄ. Цей факт ми оцінюємо, як значний недогляд, зважаючи на загрозу згадуваного явища, що постійно зростає. Відповідно до цього, ми дотримуємося позиції, що аналізовані документи потребують реформування й модернізації, оскільки стан кібербезпеки на початку XXI століття і сьогодні дуже змінився.

Відповідно до нашої позиції і враховуючи сучасні події в Україні, а також посилення кібертерористичних атак, які, своєю чергою, завдають небезпечного впливу і на всю європейську систему безпеки, рекомендуємо водночас прийняти новий Третій Додатковий Протокол.

Указаний протокол має містити поняття кібертероризму, визначення його ознак, криміналізації та політичних інструментів протидії.

Отже, ми пропонуємо таке:

1) створення «кібертрибуналу» та встановлення його віддаленої дії для реагування на кіберінциденти в режимі реального часу або подальше розширення повноважень Міжнародного суду ООН та/або Міжнародного кримінального суду з цією метою;

2) «Конвенція про взаємні кіберзобов'язання», тобто, свого роду аналогія «колективної оборони», міжнародний пакт, згідно з яким держави, ратифікувавши його, швидко могли б ужити скоординованих заходів кіберзахисту в разі кібертерористичної атаки проти однієї зі сторін. Додатковим інструментом має бути «політичний тригер для міжнародного реагування», який автоматично ініціював би низку політичних заходів чи прискорення спеціальних тимчасових міжнародних правил щодо посилення безпеки;

3) «Політичний механізм кіберпосередництва» у вигляді створення органу – посередника в кіберпросторі, який діятиме як нейтральна сторона для вирішення конфліктів між країнами у випадках підозри в кібератаках або підтримці кібертероризму;

4) «Кіберімунітет» критичної інфраструктури для об'єктів стратегічного захисту, який базується на угодах про недоторканість;

5) концепція «мережевого нейтралітету», де жодна країна не погоджується проводити кібероперації, які можна розглядати як загрозу чи агресію, прогнозуємо цей крок як посилення довіри та безпеки в міжнародних відносинах;

6) «Політичний кіберкарантин», який полягав би в автоматичному припиненні можливостей використання мережевих ресурсів на певний період у разі «підтримки» кібертероризму чи нанесення кібертерористичних атак, стримання загрози, запобігання її подальшому поширенню;

7) політичний механізм «кіберпосередництва» для підтримання «кіберкарантину», у форматі посередницького органу в кіберпросторі, який виконував би роль арбітра у випадках підозри в кібератаках або підтримці кібертероризму. Цілком імовірно, що такий арбітраж допоможе запобігти ескалації конфлікту та сприятиме мирному вирішенню спорів у кіберпросторі;

Ще одним важливим чинником є досвід України для європейського регіону і, навпаки, практика таких держав, як Естонія, Польща, Німеччина, Велика Британія, Франція, Нідерланди, Данія та Швеція. З цією метою ми проаналізували два, на наш погляд, найточніші індекси, зокрема GCI та NCSI, за допомогою яких визначили рейтингові положення кожної з країн та, спираючись на аналіз державних систем забезпечення кібербезпеки, зробили припущення, чому та чи та країна посідає саме такі позиції. Використовуючи такий аналіз, ми визначили проблеми та перспективи перейняття досвіду й розробили певні рекомендації для України. Серед пропозицій виділимо:

– оновлення Стратегії кібербезпеки України, спираючись на сучасні кібертерористичні загрози в умовах війни;

– уніфікацію положень законодавчих актів, що стосуються кібербезпеки, в більш структуровану законодавчу базу, а саме: оновлення чи скасування застарілих законів та оптимізацію й об'єднання схожих між собою нормативних актів;

– реформування CERT–UA – розмежування повноважень між підструктурами у вигляді галузевого розподілу;

– розширення компетенцій Антитерористичного Центру України у вигляді збільшення сфери впливу, поєднання фізичного та кіберзахисту від терористичних атак, тобто розробка методів протидії, відповідно до сучасної політики безпеки, які б відображали новий погляд, ураховуючи багатошаровість кіберзагроз.

Останньою пропозицією відповідно до викликів сьогодення виступає створення «Національної програми кіберосвіти». Програма має бути адаптована до галузевих запитів, тобто спрямування на тих, хто забезпечує функціонування критичної інфраструктури різних рівнів, зокрема для медичних працівників, фінансистів та економістів, працівників енергетики, юристів, державних службовців і науковців. Однак додатковим завданням Національної програми кіберосвіти могло б стати підтримання кібергігієни українського суспільства.

РОЗДІЛ 3. ПРОБЛЕМИ ПРОТИДІЇ ВПЛИВУ КІБЕРТЕРОРИЗМУ НА КРИТИЧНУ ІНФРАСТРУКТУРУ УКРАЇНИ. ВИКЛИКИ ВОЄННОГО СТАНУ

3.1. Організація кібербезпеки енергетичної інфраструктури в Україні: стан і перспективи вдосконалення

Політична ситуація в Україні та її вплив на безпеку Європи, як ми вже визначили, є складною і багатогранною темою, що особливо актуальною стала з початком російської агресії проти України в 2014 році та повномасштабного вторгнення в лютому 2022 року. Війна змінила політичний сценарій в Україні, а також поставила перед європейськими державами нові виклики щодо безпеки, зокрема у кіберпросторі. На сьогодні на Україну припадає найбільша кількість російських кібератак, і це призвело до серйозних збоїв у роботі державних і приватних установ, критично важливої інфраструктури та національних засобів зв'язку. Кіберзагрози мають як прямі, так і непрямі наслідки для європейської безпеки, оскільки Україна має стратегічне значення та є фактично своєрідним «буфером» між Росією та Євросоюзом. Тому будь-яке порушення з кібербезпеки в Україні може зруйнувати загальну цифрову безпеку європейського регіону.

Проаналізувавши вплив кібератак в цілому на інфраструктуру України, вважаємо доцільним розглянути насамперед проблему забезпечення кібербезпеки енергетичної інфраструктури та системи електронної охорони здоров'я (eHealth), які є найважливішими в життєдіяльності держави.

Енергетичну інфраструктуру потрібно розглядати насамперед через призму загрози енергетичної безпеки, яка стосується не тільки України, але і Європи загалом. До початку військових дій можливість як кібертерористичних атак, так і фізичного захоплення критично важливих для України об'єктів, здавалась майже нереальною і розглядалась лише як теоретична для оцінки стійкості енергосистеми. Однак на сьогодні російські кібероперації часто

націлені на підрив української енергетичної інфраструктури, зокрема електромереж і систем енергопостачання. Такі атаки створюють ризики й для країн Європи, оскільки вони перебувають з Україною в одній енергомережі.

На підтвердження цього положення варто згадати захоплення російськими військами в березні 2022 року Запорізької АЕС [253]. Це створило новий і безпрецедентний випадок в історії міжнародної ядерної фізичної безпеки, зокрема й міжнародної. Важливо акцентувати на тому, що Запорізька атомна електростанція – це найбільша ядерна електростанція Європи. Досі у світі не було випадків, коли АЕС подібного масштабу окупували озброєні військові підрозділи. Це захоплення виявило невідомі раніше вразливості цивільних об'єктів ядерної інфраструктури країни, підкресливши необхідність нових підходів до їхнього захисту в умовах сучасних гібридних конфліктів і не тільки.

Експерти з використання ядерної енергії всього світу наголошували, що захоплення Запорізької АЕС у контексті військових дій не тільки порушує міжнародні стандарти, але й може призвести до катастрофічних наслідків, загрожуючи життю мільйонів людей [254, 255, 256, 257, 258, 259, 260, 261,262,263,264].

Загроза захоплення Запорізької АЕС полягає не лише в прямому військовому контролі над ядерною установкою, але й у забезпеченні безпеки від потенційних кібертерористичних атаках на критичні системи, які контролюють її роботу. З огляду на це, констатуємо, що системи охорони ядерних установок є недостатніми у випадку військової агресії, особливо, якщо вона супроводжується кібертерористичними атаками. Це підкреслює необхідність запровадження новітніх адаптивних концепцій захисту, здатних інтегрувати політичні стратегії з сучасними технологіями кібербезпеки [265]. Саме тому вважаємо за доцільне запропонувати створення новітньої концепції кіберзахисту ядерно та радіаційно небезпечних об'єктів інфраструктури (далі – Концепція).

Запорізька АЕС стала своєрідною «тригерною точкою» для світової спільноти, а її захоплення засвідчило те, що навіть високотехнологічні об’єкти можуть бути уразливими до гібридних загроз, коли поєднуються військові дії, кібернетичні атаки, інформаційна війна та політичний тиск. Унікальність ситуації полягає в тому, що навіть незначне втручання в роботу станції могло мати надзвичайно руйнівні наслідки. Міжнародне агентство з атомної енергії (МАГАТЕ) [266] і багато країн закликали до негайного припинення бойових дій поблизу станції, однак така ситуація показала, що зупинити військові дії навколо стратегічних об'єктів за допомогою лише політичного тиску не завжди можливо.

Варто пам’ятати, що, крім Запорізької, на території України існує ще декілька АЕС, наприкладд Хмельницька, Південноукраїнська, Рівненська та Чорнобильська АЕС (перебуває в стадії ліквідації, а кількість відходів, що там міститься, становлять небезпеку для населення не тільки України, але і Європи). І це тільки підсилює рівень небезпеки при їх фізичному захопленні чи нанесенні кібертерористичих атак. Тому запропонована нами Концепція передбачає комплексний захист ядерних об'єктів через можливість створення механізму підземного дистанційного керування об’єктами ядерної інфраструктури.

Центральною ідеєю концепції є механізм дистанційного управління, який може бути активований у випадку фізичного захоплення об’єкта. Запропонована система передбачає, що за певних обставин, коли існує ризик використання об’єкта ворогом, цей механізм може бути автоматично застосованим та повністю керованим із розгалуженої структури без загрози для самої станції. Для забезпечення максимального рівня захисту, такий механізм має базуватися на передових кібернетичних технологіях. Застосування такої системи унеможливить контроль над ядерними установками в разі захоплення, що дозволить уникнути сценаріїв катастрофічного втручання в роботу об'єкта. Це забезпечить не тільки захист станції від можливих аварійних ситуацій, а й посилить політичну стійкість держави до подібних загроз. Для цього необхідно створити єдину систему контролю, яка б містила декілька підземних пунктів

управління з їх локалізацією в різних куточках країни. Такий механізм, як один із ключових компонентів системи кібербезпеки, на наш погляд, дозволив би віддалено втручатися в процеси управління, запобігаючи можливому виникненню аварійних ситуацій, подій та інцидентів чи екологічній катастрофі.

Основним напрямком такої Концепції, безумовно, є технічний складник, оскільки забезпечення кібербезпеки прямо залежить від використання на практиці новітніх технологій. Однак через те, що це виходить за межі нашого дослідження, ми наведемо лише базовий комплекс із процедур та алгоритмів, які частково функціонують для захисту приватних підприємств, однак мало реалізованих у стратегічних системах держави.

Перше, про що варто потурбуватися, – це динамічне шифрування [267], тобто постійна зміна ключів. Це означає, що ключі, використовувані для шифрування інформації, змінюються з дуже високою частотою (кожну годину або навіть частіше). Такий підхід значно ускладнить роботу будь-якому потенційному зловмиснику: якщо навіть хтось отримає ключ, він одразу застаріє. Звичайно, таку постійну зміну досить важко реалізувати, це створює динамічне середовище, яке майже неможливо зламати.

Наступним важливим технічним кроком є модернізація інтегрованої системи багаторівневого доступу [268]. Такий компонент для забезпечення надійного контролю доступу до систем управління ядерними установками передбачає використання декількох рівнів безпеки. На сьогодні одним із основних елементів є біометрична автентифікація, яка використовує такі ознаки, як відбитки пальців або сітківка ока. На відміну від звичайних паролів або карток доступу, це може забезпечувати значно вищий рівень безпеки. Варто також насамперед виділити вироблення стандарту з аналізу поведінки користувачів із системним аналізом поведінки кожного користувача, хто взаємодіє із системами управління. Будь-яке відхилення від поведінкових патернів оцінюватиметься як потенційна загроза, і система покликана автоматично виконувати дії з підвищення рівня безпеки або ініціювати таку перевірку.

Для модернізації систем безпеки на українських АЕС можна впровадити гнучкі алгоритми штучного інтелекту, які зможуть не лише розпізнавати аномалії в поведінці користувачів, а й передбачати можливі загрози на основі великих даних. Важливо також посилити географічні обмеження доступу за допомогою квантових технологій, що нададуть безпечний зв'язок між системами лише в межах визначених зон. Безумовно, такі технічні заходи частково існують на сьогодні, окремі з них застосовуються на об'єктах критичної інфраструктури, однак, як показує аналіз, в українській практиці захисту стратегічних об'єктів їх упровадження недостатнє.

Однією з прогресивних ідей убачаємо застосування ДНК людини для підтвердження її особистості при доступі до систем управління. Генетичні маркери, що містяться в кожній клітині тіла, є абсолютно унікальними для кожної людини, що гарантує майже неможливість підробки чи обходу цієї системи. Така методика захисту має потенціал стати непереборним бар'єром для будь-якої спроби несанкціонованого доступу.

Окрім традиційних біометричних даних, важливо інтегрувати технології, які зчитують емоційні та стресові показники людини в процесі взаємодії з системою. Наприклад, використання сенсорів, які фіксують зміни в нервовій діяльності або пульсі співробітника. Виявлення ознак стресу або інших аномальних реакцій автоматично ініціює додаткову перевірку і за необхідності блокування доступу. Такий підхід дозволить урахувати психофізіологічний стан працівника та запобігти випадкам, коли, наприклад, при використанні примусу, співробітник може намагатися здійснити несанкціоновані або небезпечні акти.

Варто також звернути увагу на інтеграцію нейрокомп'ютерних інтерфейсів, які дозволять користувачам узаємодіяти з системами управління. Користувач зможе просто думати або виконувати фізичні рухи, щоб отримати доступ до системи, оскільки нейроімпульси, генеровані мозком, є унікальними для кожної людини. Така технологія допоможе, на наш погляд, значно посилити безпеку, оскільки зловмисники не зможуть відтворити або підробити ці

сигнали, і відповідно це забезпечить надійний захист навіть від найскладніших загроз.

І, звичайно ж, доцільним уважаємо впровадження автономних систем, які здатні прогнозувати кіберзагрози ще до того, як вони себе покажуть. За допомогою штучного інтелекту та машинного навчання такі системи покликані опанувати великим обсягом даних про попередні атаки, адаптуючи захист до нових загроз із можливістю самостійно змінювати рівень безпеки та автоматично коригувати заходи захисту, що своєю чергою, дасть можливість на кілька кроків випереджати кіберзлочинців.

Важливо зазначити, що технічний захист має бути підсиленим за допомогою фізичного, який також має використовувати новітні технології як додатковий «щит». Оскільки фізичний доступ на пром-майданчик ядерної електростанції все одно залишає ймовірність відкрити зловмисникам шлях до кіберсистеми, важливо забезпечити високий рівень стійкості об’єктів, використовуючи фізичні бар’єри та системи безпеки на об’єкті. Окрім військового потенціалу, для додаткового захисту мають бути встановлені системи безпеки із розумними датчиками, які можуть виявляти незвичні рухи навколо станції. Такі датчики покликані визначати, що саме наближається до території – людина, автомобіль чи дрон, що дозволяє точніше ідентифікувати потенційні загрози та швидше реагувати. Датчики зможуть аналізувати поведінку об'єктів, помічати незвичний рух, нетипові пересування, ефективно виявляти внутрішніх правопорушників. Важливим відтак є аналіз змін у поводженні чи поведінкових аномаліях персоналу станції або спроб обійти захисні бар'єри, що допомагає швидко виявити підозрілу діяльність. Такі заходи, на нашу думку, зроблять об’єкти критичної інфраструктури більш стійкими до проникнень та атак, що значно ускладнює спроби фізичного доступу до критичних зон. Усі ці заходи у сукупності уможливлять посилення фізичних бар'єрів, що доповнить кібернетичні засоби захисту задля комплексної безпеки ядерних електростанцій.

Контроль за такою діяльністю, на наш погляд, має здійснювати галузевий центр CERT – UA з робочою назвою CERT – NE (Група реагування на комп'ютерні надзвичайні події України з ядерної енергетики).

Окремо слід ще раз наголосити, що для успішної протидії загрозі руйнування енергетичної інфраструктури в Україні та Європі необхідні не лише технічні рішення, а й політична експансія, яка б призвела до створення спільної оборонної стратегії з метою здатності протистояти сучасним гібридним загрозам.

Отже, одним із найважливіших елементів, що, на нашу думку, має бути включеним до концепції, є необхідність об'єднаної співпраці в галузі ядерної безпеки та кібербезпеки, оскільки задля впровадження указаної концепції необхідна спеціалізована інституція. Вважаємо, що міжнародні стандарти повинні враховувати, що захоплення атомної електростанції в ході збройного конфлікту є новою реальністю, яку треба запобігати за допомогою скоординованих дій. Необхідно розробити нові міжнародні протоколи та угоди, які б регулювали механізми дистанційного керування і обмежували контроль над критичними об'єктами з боку ворожих сил. Пропонуємо, щоб питання управління об'єктами критичної інфраструктури, зокрема атомними електростанціями, було внесено до порядку денного міжнародних організацій, таких, як МАГАТЕ, мета якої сприяти мирному використанню ядерної енергії та перешкоджати її використанню в будь-яких військових цілях, зокрема ядерної зброї, та ENISA, яка працює над досягненням високого загального рівня кібербезпеки в Європі. Кожна з цих організацій має унікальні компетенції та можливості, які у сукупності здатні створити потужну міжнародну платформу для забезпечення надійного захисту. Так, безумовно, на сьогодні ENISA займається кіберзахистом у всіх напрямах критичної інфраструктури, зокрема ядерної, однак, як бачимо, одна структура не може сама протидіяти всьому масштабу загроз. Тож на базі цих організацій має бути створена зведена структура, яка б перебувала на стику названих і враховувала особливості їхньої діяльності з метою усунення прогалин у сучасних викликах.

Синергетичний ефект від об’єднання повноважень цих організацій дасть змогу створити потужну платформу для забезпечення комплексної безпеки ядерних об'єктів. МАГАТЕ зможе забезпечити експертний рівень в ядерній безпеці, а ENISA — технічний компонент кібербезпеки. Така структура здатна не лише забезпечити ефективний захист на міжнародному рівні, але й завдяки координації дій організацій реагувати на загрози швидко та злагоджено.

Важливо відмітити, що Україна є оптимальним місцем для створення головного офісу зведеної структури, і на це є ряд чинників.

По-перше, геополітичне розташування України є критичним рубежем європейської безпеки. Україна розташована на межі Європейського Союзу та Росії, що робить її важливим бар’єром поширення агресії й забезпечення стабільності у всьому регіоні. Саме Україна є першою лінією оборони проти потенційних загроз із боку Росії, яка використовує як фізичні методи, так і кібератаки. Розташування міжнародної структури в Україні дозволить забезпечити надійний кіберзахист критичної інфраструктури і тим самим створити додатковий рівень захисту для Європи. Україна – це свого роду стратегічний «форпост», де захист критичних об'єктів має безпосередній вплив на безпеку всього європейського регіону.

По-друге, Україна вже неодноразово зазнавала масштабних і складних кібертерористичних атак саме на ядерну інфраструктуру, зокрема актів кібертероризму, особливо з 2014 року, коли агресія із боку Росії перейшла у фазу повномасштабної війни. Одним із ключових напрямів атак стала енергетична інфраструктура, критично важлива для функціонування держави. Важливо підкреслити, що перші відомі кібератаки почалися в Україні у 2014 році, коли хакери, пов’язані з російськими спецслужбами, використовували шкідливе програмне забезпечення BlackEnergy для розвідки та збору відомостей про українські енергетичні системи [120, 269]. Ця діяльність хоч і не спричинила безпосередніх відключень, але заклала основу для подальших атак, які мали на меті паралізувати енергосистему країни. 23 грудня 2015 року сталася перша в історії успішна кібератака на енергетичну інфраструктуру, яка

призвела до відключення електроенергії для понад 225 тисяч споживачів. Зловмисники проникли в мережі трьох обласних енергетичних компаній: «Прикарпаттяобленерго», «Чернівціобленерго» та «Київобленерго». Використовуючи BlackEnergy [124, 270, 271], вони дистанційно вимкнули підстанції, що спричинило масштабні знеструмлення. Крім того, були виведені з ладу системи резервного зв'язку, що ускладнило відновлення нормальної роботи об'єктів енергосистеми. Цей приклад став показовим щодо того, як кіберзброя може бути застосована для реальних руйнувань. Через рік, у грудні 2016 року, Україна знову зазнала атаки на енергетичну інфраструктуру. Цього разу із застосуванням шкідливого програмного забезпечення Industroyer (Crashoverride). Мішенню стала підстанція «Північна» в Києві, що призвело до тимчасового знеструмлення частини міста. Хакери використали Industroyer, розроблений спеціально для роботи з протоколами управління енергетичними мережами, що продемонструвало новий рівень складності таких атак. Хоча наслідки були менш масштабними, ніж у 2015 році, ця подія стала черговим попередженням про загрози для критичної інфраструктури країни. У 2017 році відбулася одна з найбільших кібератак у світі, відома як NotPetya. Шкідливе ПЗ, замасковане під програму-вимагач, насправді було створене для максимального руйнування. Атака зачепила численні галузі в Україні, уключаючи енергетичний сектор, де була пошкоджена інфраструктура компанії «Укренерго». Хоча NotPetya не викликав відключень електроенергії, вірус порушив роботу систем управління та пошкодив критично важливі дані [124].

У 2022 році, після початку повномасштабного вторгнення Росії, кібератаки на енергетичну інфраструктуру України набули нового масштабу [272,273]. У квітні того ж року хакери з групи Sandworm, пов'язані з ГРУ РФ, здійснили атаку із використанням модифікованої версії Industroyer, відомої як Industroyer2. Їхньою метою були підстанції «Укренерго». Оперативні дії українських фахівців дозволили зупинити атаку, але потенційні наслідки могли б бути катастрофічними, ураховуючи воєнний час і критичну залежність населення від стабільного електропостачання. У 2023 році російські хакери

здійснили кілька атак на енергетичну інфраструктуру, часто поєднуючи її із фізичними ударами по об’єктах енергетики [274,275 ,276]. У жовтні 2023 року відбулася масштабна кібератака на енергосистему, що супроводжувалася відключенням електроенергії в окремих регіонах. У грудні 2023 року атака вплинула на зв’язок та управління енергетичною інфраструктурою, створюючи значні перебої в роботі операторів. У 2024 році атаки продовжилися, зокрема із застосуванням високоточних технологій, що дало змогу зловмисникам завдати ударів по менш захищених об’єктах [277].

Усі ці атаки мають спільні риси, які дозволяють класифікувати їх як акти кібертероризму, адже вони були спрямовані на критичну інфраструктуру, від якої залежить життєдіяльність суспільства, а наслідки цих атак мали широкий вплив на цивільне населення, спричиняючи соціальні та економічні втрати. Важливо також зауважити, що ці дії відбувалися в контексті воєнного або політичного конфлікту, маючи на меті залякування населення та дестабілізацію держави. Таким чином, описані кібератаки є не лише проявами гібридної війни, але і яскравим прикладом використання кібертероризму як інструмента досягнення політичних цілей. Цей досвід є унікальним і дозволяє Україні мати практичні знання щодо того, як у складних умовах протистояти сучасним кіберзагрозам. Розміщення структури саме в Україні надасть можливість використовувати її досвід для створення міжнародних стандартів і моделей кібербезпеки, які можуть бути адаптовані для інших країн Європи. Україна може стати експертним центром для навчання і підготовки кадрів із протидії кіберзагрозам у реальних умовах.

По-третє, на території України розташовані великі об'єкти ядерної інфраструктури, зокрема Запорізька АЕС – найбільша атомна електростанція в Європі, яка вже потрапляла під військовий контроль під час російської агресії. Створення міжнародної структури для забезпечення кібербезпеки саме в Україні дозволить організувати належний захист цих стратегічно важливих об'єктів. Такий підхід, на нашу думку, має вирішальне значення для енергетичної стабільності як України, так і Європи, оскільки ядерні об'єкти не

тільки виробляють електроенергію, але і є потенційними джерелами небезпеки для здоров’я людей та екології в разі порушення їхньої безпеки. Безпечна робота цих об'єктів гарантує стабільність енергопостачання, що є важливим для всього регіону.

По-четверте, військова агресія та постійні атаки зробили Україну своєрідним «полем бою» для новітніх кібератак. Заснування і розміщення вказаної Структури в Україні дозволить тестувати новітні рішення в реальних умовах. Це створить можливість для міжнародних партнерів спільно розробляти і вдосконалювати методи захисту, які будуть адаптовані під найскладніші виклики. Європа отримає реальні та перевірені рішення, що можуть бути впроваджені для захисту критичної інфраструктури у будь-якій точці регіону.

Нарешті, Україна вже бере активну участь у багатьох європейських ініціативах з кібербезпеки, і створення офісу саме на теренах України сприятиме ще більшій інтеграції нашої держави в європейську систему безпеки. Це створить глибшу координацію між Україною та іншими країнами Європи в питаннях кібернетичного захисту, дозволить обмінюватися інформацією про загрози і спільно реагувати на них. В умовах, коли безпека однієї країни залежить від загальної кіберстійкості регіону, створення такої організації саме в Україні стане важливим кроком у зміцненні колективної безпеки Європи.

Отже, організація Міжнародної Структури кібербезпеки на базі співробітництва МАГАТЕ та ENISA саме в Україні є критично важливим кроком для зміцнення колективної безпеки Європи. Геополітичне розташування України, її унікальний досвід у протидії гібридним загрозам, наявність стратегічно важливих ядерних об'єктів, можливість тестування нових рішень та політичний сигнал підтримки – усе це робить Україну оптимальним місцем для її розміщення. Це рішення дозволить не тільки забезпечити безпеку України, але й зміцнити стійкість усієї Європи перед сучасними загрозами, підвищивши рівень координації та готовності до викликів у майбутньому. Україна, на нашу думку, буде здатна забезпечити всеохопний підхід до безпеки,

який ураховує як політичні, так і технічні аспекти. Це особливо важливо в умовах зростання загроз кібертероризму і необхідності міжнародної співпраці для захисту критичної інфраструктури.

Ще одним значним показником, що підкреслює необхідність наведених нами дій, є чимала кількість кібератак по європейських країнах:

Рис.3.1.:

Кібератаки на енергетичну інфраструктуру країн Європи (складено автором за матеріалами [278,279,280,281,282,283,284,285,286,287,288,289])

Отже, як бачимо, сучасний світ стикається з безліччю загроз, серед яких кібератакам належить особливе місце. Ядерні об'єкти є ключовою частиною критичної інфраструктури багатьох країн, і їх вразливість може мати катастрофічні наслідки не лише для окремих держав, але й для усього європейського регіону. Захоплення Запорізької АЕС під час військових дій стало «сигналом тривоги», який продемонстрував, наскільки критично важливим є забезпечення кіберзахисту цих об'єктів.

Концепція для забезпечення комплексного захисту ядерних установок від фізичних і кібератак передбачає створення багаторівневої системи захисту, яка

поєднує інноваційні рішення з кібербезпеки, механізми аналізу поведінкових аспектів, дистанційного керування та фізичного захисту. Такий підхід дає змогу не тільки виявляти загрози, але й ефективно на них реагувати, забезпечуючи зупинку роботи ядерного реактора або блокування доступу до важливих систем у випадку небезпеки.

Зрозуміло, що для реалізації такої концепції необхідна підтримка не лише України, але й багатьох інших європейських країн. Польща як близький сусід України, швидше за все, буде мати значний інтерес у підтримці цієї ініціативи, адже будь-яка аварія на ядерних об'єктах України становитиме безпосередню загрозу для польських громадян та екології. Німеччина й Франція як провідні європейські держави з великим досвідом у сфері ядерної енергетики також можуть підтримати концепцію для забезпечення стабільності та безпеки в регіоні. Країни Балтії (Латвія, Литва, Естонія) відчувають значний тиск з боку Росії і регулярно стають об'єктами кібератак. Підтримка Концепції дозволить цим країнам зміцнити свою кібербезпеку та отримати додатковий захист для критичних об'єктів інфраструктури. Велика Британія і США, які вже мають досвід співпраці з Україною в галузі безпеки можуть бачити в цій ініціативі можливість зміцнити свої зв'язки з європейськими партнерами та посилити захист від кібертероризму.

Водночас існують країни, які можуть не підтримати впровадження цієї концепції. Імовірно, Росія стане основним противником. Вона може бачити у зміцненні кібербезпеки в Україні пряму загрозу своїм інтересам, особливо враховуючи важливість контролю над критичною інфраструктурою інших країн для посилення свого політичного впливу на них. Білорусь, як союзник Росії, також, швидше за все, не підтримає цей проект. Іран може виступити проти концепції, оскільки має побоювання міжнародного втручання у свої національні процеси кібербезпеки. Крім того, певні країни Європи, які перебувають під політичним або економічним тиском з боку Росії, можуть не підтримати цю ініціативу. Це можуть бути держави, які залежать від російських енергетичних ресурсів або мають тісні економічні зв'язки з Росією, і тому

остерігаються можливих санкцій або інших наслідків у разі підтримки Концепції.

Підтримка Концепції, на нашу думку, надасть низку значних переваг країнам-учасникам. Насамперед це підвищення рівня безпеки критичної інфраструктури, що є ключовим елементом для забезпечення стабільності кібербезпеки ядерної сфери. Захист ядерних об'єктів означає зменшення ризиків не тільки для країни, де вони розташовані, але й для всіх сусідніх держав, які можуть зазнати шкоди в разі аварії. Технологічний розвиток також є однією з переваг. Країни, які підтримають Концепцію, матимуть доступ до передових технологій і рішень з кібербезпеки, зможуть інтегрувати ці системи у свою інфраструктуру, підвищивши рівень власної кібербезпеки. Це включає нові методи аналізу поведінки, дистанційного управління та багатофакторної автентифікації, які можуть використовуватися для захисту інших важливих об'єктів.

Крім того, міжнародне співробітництво з питань кібербезпеки дозволить країнам обмінюватися досвідом, створювати спільні протоколи реагування на загрози та проводити навчання і симуляції кібератак. Це зміцнить колективну безпеку і знизить ризики глобальних кібератак. Політична підтримка України в цьому контексті є важливим чинником, який підкреслює солідарність європейських країн перед агресією, а також їх готовність захищати критичну інфраструктуру від загроз, що виникають у сучасному світі.

Економічні вигоди також варто врахувати. Підвищення рівня безпеки ядерних установок означає зменшення ризиків потенційних аварій, що може значно скоротити витрати на ліквідацію наслідків і стабілізацію ситуації. Це також знижує ризики енергетичних збоїв, що можуть мати суттєвий вплив на економіку регіону.

Однак важливо також урахувати потенційні виклики при впровадженні Концепції, адже вони можуть бути досить різноманітними. По-перше, це політичні виклики, пов'язані з опором з боку країн, які не зацікавлені у зміцненні незалежності України або регіональної безпеки. Деякі країни,

зокрема Росія, можуть бачити в цій ініціативі загрозу своєму впливу і можуть намагатися перешкоджати її впровадженню через дипломатичні або економічні інструменти. По-друге, технологічні виклики також є значними. Інтеграція новітніх технологій потребує значних ресурсів, часу і кваліфікованого персоналу. Крім того, необхідно забезпечити високий рівень координації між різними країнами та організаціями, що є досить складним завданням.

Створення міжнародної зведеної структури для кіберзахисту ядерних об'єктів в Україні є виправданим через геополітичне розташування країни як стратегічного бар'єру між Європейським Союзом та Росією, наявність унікального досвіду протидії кібертерористичним атакам та стратегічно важливих ядерних об'єктів, безпека яких має значення для всього європейського регіону.

На основі вищевикладеної Концепції важливо також акцентувати на створенні визначення поняття «ядерна кібербезпека» та його включення до міжнародно- правової бази, адже матиме стратегічне значення для України та Європи. Це пов'язано з низкою важливих факторів, які визначають сучасні виклики для національної і регіональної безпеки, такі, як ситуація із захопленням Запорізької АЕС у 2022 році. Уведення цього терміна дозволить Україні і Європі запровадити спільні стандарти для протидії кібертероризму та інших форм гібридної агресії, спрямованих на ядерні об’єкти.

Зважаючи на зміст запропонованої Концепції та сучасних викликів воєнного стану, найбільш влучним вважаємо таке визначення: «ядерна кібербезпека – це сукупність технічних, організаційних, правових та процедурних заходів, спрямованих на забезпечення захисту ядерних об’єктів, інформаційних систем та мереж їх управління від кібернетичних загроз і кібератак, з метою недопущення несанкціонованого втручання, яке може призвести до серйозних аварій, загрози навколишньому середовищу, життю і здоров’ю людей, а також порушенню міжнародної безпеки».

Таке визначення вважаємо найбільш переконливим, оскільки воно охоплює всі ключові аспекти захисту ядерних об’єктів від кіберзагроз,

зосереджене на технічних, організаційних, правових і процедурних заходах. Воно акцентує на запобіганні несанкціонованому втручанню, здатному спричинити серйозні аварії, загрозі довкіллю, життю людей і міжнародній безпеці, що є сутністю ядерної кібербезпеки, а включення його до міжнародно-правової бази дозволить Україні та Європі створити нові механізми для захисту критичних об'єктів у гібридних конфліктах, забезпечити координацію дій у разі кібернетичних атак і підвищити рівень безпеки ядерної інфраструктури на глобальному рівні. Це є важливим кроком для зміцнення колективної безпеки, що враховує нові виклики сучасного світу.

Отже, політична ситуація в Україні, особливо після початку збройної агресії Росії у 2014 році та повномасштабного вторгнення у 2022 році, докорінно змінила безпекову ситуацію Європи. Захоплення Запорізької АЕС російськими військовими формуваннями продемонструвало критичну вразливість ядерної інфраструктури до гібридних загроз, що поєднують фізичні та кібернетичні атаки. Ця подія не лише порушила міжнародні правила, але й спричинила перегляд того, як забезпечити ядерну кібербезпеку в усьому світі.

Традиційні методи захисту виявилися недостатніми у відповідь на сучасні загрози. Необхідність поєднання політичних стратегій із передовими технологіями кібербезпеки стала очевидною. Запропонована ідея захисту критичної інфраструктури передбачає створення комплексної системи захисту, а такий методологічний підхід може забезпечити комплексну охорону ядерних об’єктів як у фізичному, так і в кібернетичному вимірах, зменшуючи ймовірність несанкціонованого вторгнення та потенційних катастрофічних наслідків.

З політичної точки зору ця ідея акцентує увагу на важливості міжнародної співпраці та координації. Створення зведеної організації на базі МАГАТЕ та ENISA з головним офісом в Україні є, на нашу думку, стратегічним кроком. Україна, маючи унікальні знання щодо протидії кібератакам на критичну інфраструктуру та географічне розташування на кордоні з Росією, може стати значним партнером у зміцненні європейської безпеки. Це також може бути

показником політичної волі європейського уряду допомогти Україні в її зусиллях протистояти у викликах війни та визнати її роль у підтримці регіональної стабільності.

Пріоритетом також має стати включення терміна «ядерної кібербезпеки» як в українську, так, можливо, і в європейську регіональну правову базу. Уведення цього терміна та закріплення його в угодах сприятиме розробленню єдиних принципів і протоколів безпеки, більш ефективному реагуванню на виклики, підвищить ступінь довіри між державами та сприятиме розвитку глобальної системи кібербезпеки.

Зрештою, захист ядерної інфраструктури є не лише технічною, але й політичною необхідністю. Об’єднання зусиль держав, міжнародних організацій і наукового співтовариства має важливе значення. Лише шляхом колективних дій та інноваційних методів ми зможемо забезпечити безпеку критично важливих об’єктів

перед обличчям останніх викликів і підтримувати міжнародну безпеку та стабільність.

3.2. Кібербезпека в галузі електронної охорони здоров’я в Україні

Ще однією ідеальною жертвою кібератак є галузь охорони здоров’я, оскільки на сьогодні в забезпеченні догляду за пацієнтами вона майже повністю залежить від технологій. Вважаємо, що в межах нашого дослідження варто розглянути кібербезпеку в галузі охорони здоров’я, оскільки названий напрямок критичної інфраструктури за останні роки став важливою віхою для суспільства та держави. Більш детально зупинимося саме на системі електронної охорони здоров’я, оскільки за останні декілька років ця галузь отримала стрімкий перехід до цифрової трансформації та діджиталізації. Установи охорони здоров'я володіють великими обсягами конфіденційних даних та критично важливої медичної інформації, серед них: історії хвороб, результати аналізів, діагнози та лікування, інформація про страхування,

платіжні реквізити, електронні медичні картки. Медичне обладнання керується та обслуговується із використанням мережевих технологій, і, на жаль, за останні роки можна спостерігати, що воно стає дедалі вразливішим до кібератак, адже такі атаки можуть завдати шкоди обладнанню для спостереження, лікування та підтримання життєдіяльності пацієнтів, іноді тимчасово виводячи з ладу пристрої, що може значно вплинути на перебіг лікування, завдати значної шкоди життю та здоров'ю пацієнтів, а в окремих ситуаціях призвести й до летальних випадків.

З одного боку, інновації поліпшили та полегшили процес догляду за пацієнтами, унаслідок автоматизації спростили перебіг управління даними та покращили керувальний апарат закладів охорони здоров'я, але, другого – вони наразили цю галузь на значні ризики порушення кібербезпеки. Такі обставини вимагають від медичної спільноти не лише знань і навичок користування цифровими базами, а й знань основ кібербезпеки, володіння навичками захисту власних даних і даних пацієнтів у кіберпросторі. Якщо певні відомості потраплять до рук зловмисників, це може поставити життя та здоров'я пацієнтів під загрозу, наприклад, позбавивши їх своєчасної та належної медичної допомоги.

Отже, так само, як система охорони здоров'я поступово переходить під віртуальний контроль, нагальною стає проблема забезпечення кібербезпеки як окремих людей, так і системи охорони здоров'я загалом. Щоб запобігти цим кіберзагрозам, необхідно впроваджувати комплексні заходи кібербезпеки.

Відповідно до статті 3 Закону України «Основи законодавства України про охорону здоров'я» система електронної охорони здоров'я – система взаємоприйнятних інформаційних відносин усіх суб'єктів охорони здоров'я, які базуються на використанні методів, заходів та технологій із застосуванням цифрового середовища, зокрема й інформаційно-комунікаційних технологій, спрямованих на підтримку сфери охорони здоров'я, уключаючи медичні послуги, профілактичний нагляд за здоров'ям населення та його зміцненням, покращення якості та збільшення тривалості життя населення. Система

електронної охорони здоров’я стосується також медичної освіти, використання цифрових сервісів з метою отримання необхідної інформації, знань і навичок для надання медичної та/або реабілітаційної допомоги, виконання оперативних функцій системи громадського здоров’я. Ця інформаційно-комунікаційна система забезпечує автоматизацію ведення обліку медичних послуг та управління інформацією про охорону здоров’я, зокрема медичною інформацією шляхом створення, розміщення, оприлюднення та обміну інформацією, відомостями й документами в електронному вигляді, до складу якої входять центральна база даних та електронні медичні інформаційні системи, між якими забезпечено автоматичний обмін інформацією, даними та документами через відкритий програмний інтерфейс (API) [290].

Електронна охорона здоров’я (е-здоров’я, eHealth) – система взаємоприйнятних інформаційних відносин усіх суб’єктів сфери охорони здоров’я, які базуються на використанні методів, заходів та технологій із застосуванням цифрового середовища, у тому числі інформаційно-комунікаційних технологій, спрямованих на підтримку сфери охорони здоров’я, уключаючи медичні послуги, профілактичний нагляд за здоров’ям населення та його зміцненням, покращення якості та збільшення тривалості життя населення, медичну літературу та освіту у сфері охорони здоров’я, знання та дослідження, використання цифрових сервісів з метою отримання необхідної інформації, знань і навичок для надання медичної та/або реабілітаційної допомоги, виконання оперативних функцій системи громадського здоров’я [291].

Дослідивши обидва поняття, маємо зауважити, що вони дуже схожі між собою, хоча й мають певні відмінності. eHealth – це широке поняття, яке включає застосування сучасних цифрових технологій, що допомагають покращити роботу медицини: онлайн-консультацій із лікарем, мобільних додатків, які нагадують про прийом ліків чи фіксують показники здоров’я. eHealth також охоплює освітні програми для лікарів і пацієнтів, різні медичні дослідження та засоби для обміну медичною інформацією. ЕСОЗ же займається

збором, збереженням і обміном медичних даних, наприклад, коли пацієнт отримує електронний рецепт або лікар заповнює медичну картку на комп'ютері, саме ЕСОЗ забезпечує, щоб ця інформація зберігалася в правильному місці й була доступною в разі потреби іншому лікареві. Вона автоматизує багато процесів, які раніше були ручними: облік послуг чи зберігання паперових карток. Подаємо порівняльну таблицю особливостей кожного з понять:

Табл.3.1:

Відмінність eHealth та ЕСОЗ (складено автором за матеріалами [290,291])

Критерій	eHealth	ЕСОЗ
Сутність поняття	широке поняття, що включає всі цифрові технології та сервіси для покращення охорони здоров'я	технічна інфраструктура для збору, зберігання, обробки та обміну медичними даними
Масштаб	охоплює всі цифрові інновації в медицині: мобільні додатки, телемедицину, освітні програми, електронні сервіси тощо	Обмежується виключно автоматизацією процесів ведення медичної інформації
Мета	забезпечити цифрову трансформацію медицини: зробити послуги доступнішими, ефективнішими та зручнішими для всіх	налагодити чіткий облік медичних послуг та обмін даними між лікарями й установами
Компоненти	містить усі цифрові рішення, пов'язані з охороною здоров'я, наприклад, онлайн-консультації, мобільні додатки, освітні платформи для лікарів і пацієнтів тощо	складається з центральної бази даних, електронних медичних систем і API для автоматизованого обміну інформацією
Користувачі	пацієнти, лікарі, аптеки, розробники технологій, уряди, освітні установи	лікарі, медичні установи, аптеки, що працюють із медичними даними пацієнтів
Приклади	телемедицина, мобільні додатки для контролю здоров'я, сервіси для запису до лікаря чи отримання результатів аналізів	електронні медичні картки, електронні рецепти, збереження даних про послуги

Продовження Табл.3.1:

Призначення	інтегрує цифрові технології для поліпшення всіх аспектів охорони здоров’я, зокрема профілактики, лікування, освіти, управління
Взаємозв’язок	eHealth є великим напрямком, частиною якого є ЕСОЗ як технічна база для зберігання та обміну інформацією

Система eHealth стала ключовим напрямом цифрової трансформації медичних послуг як в Україні, так і в Європейському Союзі. Ця ініціатива має на меті створити ефективну, прозору та доступну структуру, яка полегшить узаємодію між пацієнтами, медичними працівниками та установами за допомогою сучасних інформаційних та комунікаційних технологій. У Європі стратегічні програми та законодавча підтримка активно підтримують такі ініціативи, тоді як в Україні впровадження eHealth є вирішальним етапом у реформі охорони здоров’я, який має на меті покращити якість медичних послуг та сприяти фінансовій прозорості.

Одна з найважливіших ініціатив, яку варто розглянути,– глобальне партнерство у сфері цифрового здоров'я (GDHP) [292]. Це міжнародна ініціатива, яка об'єднує уряди, урядові агентства та організації з різних країн для співпраці в галузі eHealth. Метою GDHP є обмін знаннями, досвідом та найкращими практиками для покращення здоров'я населення через ефективне використання цифрових технологій і охорони здоров'я. Це сприяє глобальному розвитку цифрової медицини та підвищенню ефективності систем охорони здоров'я в різних країнах. Україна також приєдналася до GDHP [293], що стало важливим кроком у напрямку інтеграції сучасних цифрових рішень у національну систему охорони здоров'я. Це дозволило Україні брати участь у глобальному обміні досвідом та впроваджувати передові цифрові сервіси в медичній сфері. Завдяки участі в GDHP Україна отримала можливість інтегрувати передові цифрові рішення у свою систему охорони здоров'я, що сприяє підвищенню її ефективності та доступності для громадян. Це, своєю

чергою, підвищує якість медичних послуг та забезпечує кращий захист здоров'я населення. Участь України в GDHP сприяє також гармонізації національної політики у сфері eHealth з міжнародними стандартами, що є важливим аспектом інтеграції до глобальної спільноти та підвищення конкурентоспроможності на світовій арені.

У 2024 році був опублікований Документ «Guidance for Medical Device Cybersecurity» (GMDC) [294], у якому сформульовано чотири рівні вимог до кібербезпеки для виробників медичних пристроїв та організацій охорони здоров'я, які спрямовані на захист пацієнтів і забезпечення безперервності медичних послуг. Упровадження цих рекомендацій сприяє гармонізації міжнародних стандартів та підвищенню довіри між країнами в галузі охорони здоров'я. З політичної точки зору реалізація таких рекомендацій сприяє гармонізації міжнародних стандартів і підвищує довіру між країнами в галузі медицини. Він також підкреслює важливість міжнародного співробітництва у боротьбі з кіберзагрозами, які не знають кордонів. Для України інтеграція таких стандартів є важливим кроком у зміцненні національної системи охорони здоров'я та дотриманні міжнародних вимог.

Ключовим складником інтеграції є нова європейська політика «Здоров'я–2020» [295], орієнтована на конкретні дії у відповідь на виклики громадському здоров'ю. Основними завданнями політики є забезпечення умов для максимального реалізації потенціалу здоров'я і добробуту кожної людини, скорочення нерівності в доступі до медичних послуг, стратегічне керівництво охороною здоров'я, інвестиції в ефективні заходи для вирішення проблем громадського здоров'я, а також підтримка інновацій і прогнозування змін. Виконання цих цілей значно прискорює вирішення основних проблем електронної охорони здоров’я і спрощує процес лікування через використання таких інструментів, як електронні рецепти, історії хвороб, електронні картки та онлайн-форми. Важливим аспектом є також впровадження транскордонних послуг електронної охорони здоров'я, які надають можливість отримувати медичні послуги як в країні проживання, так і за її межами.

Транскордонні ініціативи ЄС (myHealth@EU [296]) забезпечують доступ до електронних рецептів та медичних звітів для громадян країн-учасниць, що сприяє розширенню можливостей електронної охорони здоров’я. Нові електронні транскордонні медичні послуги планується встановити в 25 країнах ЄС до кінця 2025 року, що є важливим кроком до інтеграції систем охорони здоров’я. Крім того, програма «Цифрове десятиліття» ставить за мету забезпечення 100% громадян ЄС доступом до їх електронних медичних записів до 2030 року, що відображено у звіті «2024 Digital Decade eHealth Indicator Study» [297]. Ця ініціатива спрямована на цифрову трансформацію системи охорони здоров'я з метою підвищення якості надання медичних послуг та забезпечення рівноправного доступу для всіх громадян.

Пандемія COVID-19 також підкреслила необхідність покращення готовності системи охорони здоров'я до кризових ситуацій, що стало основою для запуску програми EU4Health [298]. Програма прийнята на 2021 – 2027 роки і розвиває можливості реагування та вирішення проблем у системі електронної охорони здоров’я, сприяючи побудові стійкіших і доступніших систем. Україна, як асоційована країна, бере участь у цій програмі, здійснюючи фінансові внески та співпрацюючи з іншими державами у побудові стійкої системи охорони здоров'я.

Отже, зміцнення співпраці між європейськими країнами та залучення України до спільних ініціатив свідчить про прагнення створити єдину та стійку систему охорони здоров'я, яка могла б швидко реагувати на виклики та підвищувати рівень доступності послуг. З європейської політичної перспективи така інтеграція не лише підвищує рівень медичних послуг, але й слугує механізмом посилення політичної єдності та солідарності між державами, водночас сприяючи зменшенню нерівності у доступі до медичної допомоги. Для України участь у цих процесах є важливим кроком у напрямку європейської інтеграції та посилення спроможності власної системи охорони здоров’я шляхом доступу до інновацій та новітніх практик. Завдяки таким

інноваціям та доступу до новітніх методів можна покращити власну систему охорони здоров'я.

Однак мусимо звернути увагу на зворотній бік успішного впровадження ініціатив та програм – на кібербезпеку системи eHealth. Європейський Союз стикається з численними викликами у сфері охорони здоров’я, що вимагає модернізації медичних послуг. Водночас ENISA попереджає про зростання загрози програм-вимагачів, тоді як лише 27% організацій охорони здоров'я мають спеціальні програми захисту [299]. У межах стратегій цифровізації ЄС запроваджує нормативну базу для електронної медицини, уключаючи регулювання медичних пристроїв, захист даних про здоров’я, цифрову ідентифікацію та вторинне використання медичних даних. Швидке ухвалення стратегій електронної охорони здоров’я дозволяє ефективніше надавати послуги. Ці заходи мають на меті зміцнити незалежність від цифрових технологій та зміцнити кібербезпеку. Європейський простір даних охорони здоров'я (EHDS) також заплановано використовувати для обміну даними з метою досліджень та інновацій.

На сьогодні Європейська комісія активізує дії щодо кібербезпеки в секторі охорони здоров’я, який стає дедалі більш залежним від цифрової інфраструктури та часто піддається кібератакам. Політичні рекомендації на 2024–2029 роки передбачають новий план дій із кібербезпеки для лікарень [300]. Наразі в ЄС на етапі впровадження перебувають кілька ініціатив, наприклад EHDS [301], – Європейський простір даних охорони здоров'я і регулювання медичних пристроїв. EHDS, затверджений інституціями ЄС, що встановлює єдину європейську структуру для обміну даними про здоров'я з метою досліджень, інновацій, охорони здоров'я, розробки політики та регулювання. З цією метою утворена Експертна група ENISA eHealth Security Experts [302, 303] для залучення фахівців з охорони здоров’я для обговорення кіберзагроз, проблем і рішень, що виникають у цій сфері. Вона також підтримує ENISA в її діяльності, ураховуючи новий мандат Агентства. Роль експертів у групі полягає у підготовці політичних документів та позицій щодо питань

безпеки в охороні здоров’я, обміні знаннями та забезпеченні координації поточних і майбутніх зусиль у галузі кібербезпеки.

EHDS є важливим елементом Європейського союзу з охорони здоров’я і ґрунтується на загальних європейських стандартах конфіденційності, визначених GDPR та директивою NIS2. Він має на меті підвищити координацію між країнами ЄС для запобігання кризам у сфері охорони здоров'я, а також для їх ефективного подолання. EHDS є важливим кроком до створення цифрових і більш стійких систем охорони здоров'я в ЄС, дозволяючи ефективний доступ до відомостей про здоров'я для громадян і дослідників, забезпечуючи при цьому високі стандарти захисту конфіденційності та безпеки. Однак одним із основних викликів є забезпечення конфіденційності, цілісності та доступності медичних даних, оскільки кібератаки можуть ставити під загрозу не лише інформацію, але й безпеку пацієнтів.

Отже, важливо відмітити, що всі європейські ініціативи спрямовані на структуризацію та реформування eHealth, однак, на жаль, не містять прямих положень про забезпечення кібербезпеки. Переконані, що для України як учасниці зазначених ініціатив потрібно запропонувати та запровадити введення такого положення в усі попередні проєкти, які на сьогодні продовжують дію, а також, під час створення нових ураховувати вказаний аспект. Важливим також є пояснення сутності поняття «кібербезпеки електронної охорони здоров’я» та його складників.

Проаналізувавши відповідні документи, формулюємо таке робоче визначення: «кібербезпека eHealth– це забезпечення організації своєчасних доступних та якісних медичних послуг, під час використання кіберпростору, яке гарантується шляхом виконання особливих вимог, зокрема захищеність життєво важливої інформації та даних пацієнта (історії хвороб, результати аналізів, діагнози та плани лікування), належна робота медичних систем і обладнання, збереження безпеки та безперервності роботи у випадках надзвичайних ситуацій і дотримання правил, що включає необхідні методи захисту від зовнішніх і внутрішніх кіберзагроз) [304]. Наведені пропозиції

мають бути включені до законів, які регулюють безпеку держави, а також їх необхідно внести до окремих положень законів України «Про кібербезпеку» та «Основи законодавства України про охорону здоров'я».

3.2.1. *Використання досвіду європейських країн в галузі забезпечення кіербезпеки eHealth*

Аналізуючи національний досвід Європейських держав у забезпеченні кібербезпеки системи eHealth, маємо відмітити насамперед Естонію, яка стала однією з перших держав, яка ще в 2008 році запровадила систему електронного урядування та цифрових ініціатив у галузі охорони здоров'я. На початку система надавала дані пацієнтів в режимі онлайн, а згодом була розширена новими послугами та можливостями для інтегрування партнерів з приватного сектора та технологією Blockchain для доступу до системи та цілісності даних. На сьогодні в Естонії 95% медичних даних зберігаються у форматі онлайн. Важливо також зазначити, що на сьогодні Естонія має найнижчий відсоток кібератак, які стосуються охорони здоров'я. Пацієнти можуть переглядати свої дані в будь-який час, а медичні працівники можуть приймати рішення, маючи всі медичні документи в постійному доступі, а держава відтак економить значні ресурси. Усі медичні документи з 2009 року завантажені в систему (критичні для часу дані, відвідування лікаря та медичні зображення). Уряд наглядає за системою, щоб переконатися, що вимоги до прав доступу виконуються як постачальником, так і користувачем, і проводить щорічні перевірки для її вдосконалення. Для захисту від кібератак убудовано два важливі засоби безпеки: система є самопідтримуваною без єдиної точки входу, і всі входи в систему відстежуються, щоб побачити, чи вони збігаються з даними, до яких намагаються отримати доступ, перш ніж дозволити доступ [305]. Україні, на нашу думку, важливо перейняти цей підхід, розробивши децентралізовану архітектуру для своєї системи eHealth. Це передбачає розподіл функцій між різними серверами та вузлами, що зменшить ризик масових збоїв або атак.

Крім того, важливо впровадити багаторівневий захист, уключаючи шифрування даних, регулярні оновлення та контроль доступу. Це сприятиме підвищенню довіри користувачів до системи та забезпечить надійний захист від потенційних загроз.

Німеччина визначає охорону здоров'я важливим складником життя громадян та показником процвітання, сили та солідарності суспільства. Система охорони здоров'я країни вважається однією з найкращих у світі завдяки інтеграції цифрових технологій у її роботу. Система eHealth, яка включає електронні карти пацієнтів, цифрове зберігання та обробку медичних даних, а також відеоконсультації — це лише кілька прикладів технологій, що кардинально змінюють медичний сектор Німеччини, полегшуючи життя людей, скорочуючи час на поїздки та очікування, а також даючи змогу швидше надавати медичну допомогу в екстрених ситуаціях.

Проте, як і в будь-якій країні, цифровізація не може існувати без забезпечення належного рівня кібербезпеки. Зважаючи на розвитком цифрових технологій, зростають ризики кібератак, і охорона здоров'я не є винятком. Це підтверджують численні інциденти за останні роки, коли лікарні були змушені перейти на послуги екстреної допомоги після кіберзагроз, а мільйони медичних записів пацієнтів були викрадені або залишалися без належного захисту. У гіршому випадку зловмисники можуть маніпулювати медичними пристроями, такими, як інсулінові помпи, монітори пацієнтів або апарати ШВЛ, що може мати серйозні наслідки для здоров'я пацієнтів, не виключаючи фатальні.

Це можна побачити на прикладі, коли Німеччина у 2020 році мала кібератаку на університетську лікарню Дюссельдорфа і зазнала атаки програм-вимагачів [306], яка вплинула на її ІТ-системи. Програмне забезпечення-вимагач вторглося на 30 серверів лікарні, вивівши з ладу системи та змусивши лікарню відмовитися від надання допомоги екстреним пацієнтам. Атака була пов’язана з програмою-вимагачем Ryuk, яка скомпрометувала мережу лікарні, що зрештою призвело до порушення роботи й побічно спричинило смерть жінки [307]. Тоді лікарня оголосила, що не може обслуговувати амбулаторних

пацієнтів і служби швидкої допомоги. Атака скомпроментувала цифрову інфраструктуру, на яку лікарня покладається для координації роботи лікарів, відповідного лікування, що призвело до скасування сотень операцій та інших процедур [308]. Наслідком цього стало те, що жінка в тяжкому стані була відправлена до лікарні за 20 миль у Вуппералі, але їй не змогли надати вчасної допомоги, що призвело до її смерті. Цей приклад є яскравою демонстрацією атаки в кіберпросторі, що спричиняє відвертий кібертероризм.

Законодавчі ініціативи Німеччини, на які ми звертали увагу у попередніх розділах, підкреслюють важливість забезпечення кібербезпеки інформаційних систем у медичному секторі, зобов'язуючи заклади охорони здоров'я та постачальників страхових послуг дотримуватись стандартів захисту даних і вживати відповідних заходів для кібербезпеки. Водночас уряд регулярно оновлює нормативну базу та стандарти, щоб реагувати на нові кіберзагрози й ризики, приділяючи наразі увагу покращенню кібербезпеки медичних пристроїв. При цьому необхідно знайти баланс між рівнем захисту і зручністю, щоб забезпечити швидку реакцію медичного персоналу в критичних ситуаціях.

Аналізуючи досвід Данії у впровадженні національного порталу eHealth, можемо підкреслити рівень довіри громадян до системи охорони здоров'я та захисту їхніх даних. Під час пандемії було розширено доступ до даних для медичних працівників муніципалітетів, що дозволило їм брати участь у надзвичайних заходах і надавати медичну допомогу на місцевому рівні. Це розширення доступу супроводжувалося заходами з управління цього процесу для різних професій, що підкреслює важливість кібербезпеки та захисту даних рід час цифровізації охорони здоров'я [309]. З політичної точки зору, данський досвід підкреслює важливість децентралізації, оскільки система охорони здоров'я Данії характеризується автономною структурою, де муніципалітети відіграють значну роль у наданні медичних послуг. Це дозволяє швидко адаптуватися до місцевих потреб і забезпечувати гнучкість у реагуванні на кризи. Для України, яка також має децентралізовану систему, важливо зміцнювати спроможність місцевих органів влади й забезпечувати їх

необхідними ресурсами для ефективного надання медичних послуг. Інтеграція цифрових технологій, згідно з досвідом Данії, підвищує прозорість і доступність медичних послуг. Важливо також продовжувати розвиток національної електронної системи охорони здоров'я, забезпечуючи її інтероперабельність та захист пацієнтів. Активне залучення громадян до використання цифрових медичних послуг сприяє підвищенню їх довіри до системи охорони здоров'я. Данський приклад показує, що це можливо за умови проведення освітніх кампаній та тренінгів для підвищення цифрової грамотності населення, особливо в сільських та віддалених районах. На це ми також звертали увагу в аспекті впровадження Національної програми кіберосвіти, зокрема і в галузі охорони здоров’я.

Як бачимо, прогрес у впровадженні eHealth в країнах Європи супроводжується значними викликами з кібербезпеки та конфіденційності даних. Лідери, зокрема Естонія та Данія, демонструють високий рівень зрілості, проте навіть вони стикаються з ризиками, пов'язаними з доступом до чутливих даних.

Для досягнення мети та ініціатив, запланованих для виконання до 2030 року, ми вважаємо, що потрібний комплексний підхід, що включає зокрема й покращення кібербезпеки, а з політичного погляду реалізація цих змін потребує посилення координації на рівні ЄС, створення єдиних стандартів захисту даних та забезпечення політичної волі для проведення реформ. До цього належить також гармонізація законодавства та підтримка ініціатив, спрямованих на подолання цифрової нерівності, що є критичним для забезпечення національної безпеки й стабільності в регіоні.

На нашу думку, успішне реформування eHealth в європейських країнах залежить не лише від технічних чи адміністративних рішень, але й від політичної мобілізації на всіх рівнях влади. Уразливість кіберінфраструктури охорони здоров'я може мати дестабілізувальний вплив, оскільки атаки на системи eHealth здатні підірвати довіру громадян до державних інституцій та спричинити значні соціально-політичні наслідки. Крім того, важливо врахувати

політичні інтереси різних країн. Лише завдяки спільним зусиллям можливо досягти цілей, зазначених в ініціативах і забезпечити стабільність, охорону та добробут громадян європейських країн.

Як було зазначено раніше, Польща виступає одним із лідерів у питаннях забезпечення кібербезпеки всієї критичної інфраструктури. Однак, проаналізувавши її інструменти захищеності, нами виявлено, що країна не має такої всеохопної Національної стратегії кібербезпеки, як наприклад, Естонія, розгорнутої нормативно-правової бази, як Німеччина, Франція чи Україна, у Польщі не така розгалужена інституційна система, як в Нідерландах чи Великобританії, однак країна займає провідні позиції з огляду на комплексність системи. Польський уряд, імовірно, не приділяє уваги окремим механізмам, а навпаки – виробляє стратегію всеохопної безпеки, де всі структури не перекликаються у своїх повноваженнях (наприклад, це ми можемо спостерігати, аналізуючи ситуацію в Україні), а, навпаки, акумулюються в забезпеченні кібербезпеки держави. Ще одним важливим досягненням Польщі вважаємо швидкість прийняття рішень, що є значною перевагою в питаннях суспільної та державної безпеки будь-якого напрямку.

Так, наприклад, протягом 2022 – 2023 років на систему було здійснено декілька дестабілізуючих кібератак, серед найгучніших:

– кібератака на службу швидкої медичної допомоги, тоді понад тиждень після атаки кіберзлочинців підрозділи LPR по всій країні були позбавлені можливості користуватися своїми комп’ютерними системами. Ключові системи роботи екстреної служби, такі, як система передавання інформації про поточні втручання, веб-сайт та електронна пошта, були недоступні. Хакери вимагали викуп у розмірі 390 тисяч доларів);

– кібератака на «Інститут польського центру здоров’я матері» в Лодзі, яка серйозно порушила нормальне функціонування цієї установи, що спрчинило затримання видачі медичної документації, виписку пацієнтів та низку інших надзвичайно делікатних процедур [310].

Кібератаки в Польщі серйозно порушили функціонування систем охорони здоров'я, спричинивши перебої в роботі ключових медичних установ і затримку в наданні важливих послуг. Міністерство цифровізації, аналізуючи інциденти, визначило, що за ці роки кількість зареєстрованих кібератак на заклади охорони здоров’я в Польщі зросла втричі, і така тенденція є небезпечною не лише для життя та здоров’я пацієнтів, а й навіть для стабільності суспільного порядку в державі. Тому було визначено необхідним вироблення концепції протидії кібератакам та забезпечення кібербезеки іншими, ніж існують, додатковими заходами.

Уже 29 травня 2024 року Фундація Healthcare Poland разом зі своїми членами-засновниками – Центральним центром досліджень інновацій та освіти, Польською федерацією лікарень та Національною палатою будинків престарілих – уклали Коаліцію за кібербезпеку в охороні здоров’я [311]. Основні завдання Коаліції полягають у підготовці тренінгів для медичного персоналу щодо кібербезпеки, залучення державних коштів для цифрового захисту даних. Також було зазначено, що освіта з кібербезпеки підвищує ефективність захисту медичних даних, а подальше інвестування в навчання може суттєво зміцнити кібербезпеку польської системи охорони здоров'я, зменшуючи вразливість лікарень до кібератак.

Кібербезпека є одним із найбільш важливих факторів забезпечення ефективного функціонування системи охорони здоров'я і в Нідерландах. Нещодавні кібератаки на голландські медичні установи, зокрема атаки російської хакерської групи Killnet на десятки лікарень, призвели до того, що система охорони здоров'я зіткнулася з погрозами з боку державних суб'єктів, що призвело до збоїв у їх роботі, оскільки Killnet працював з іншими хакерами для проведення DDoS-атак на веб-сайти лікарень. Лікарня в Гронінгені особливо постраждала, і через хвилю нападів район був недоступний для медичних послуг на регулярній основі. Атака в основному вплинула на зовнішні веб-сайти і внутрішні системи, а електронні записи пацієнтів особливо

не постраждали. Ці атаки мали політичний відтінок, оскільки хакери заявили про свої дії як про помсту за підтримку Нідерландами України [312].

Тож, важливо відзначити, що перехід охорони здоров’я в цифровий простір має багато переваг, уключаючи покращення доступу, якості лікування та ефективності управління. Але водночас використання цифрових рішень в секторі охорони здоров'я створює нові проблеми і загрози, що вимагає стратегічного підходу до забезпечення кібербезпеки. Цей баланс важливий для надійного функціонування закладів охорони здоров'я, тому Управління охорони здоров'я та охорони здоров'я молоді Нідерландів працює над досягненням балансу між перевагами та ризиками системи eHealth, використовуючи системний підхід, залучаючи пацієнтів до процесу охорони здоров'я, обміну інформацією та кібербезпеки. Така методичність, на нашу думку, дає змогу враховувати всі аспекти цифрової трансформації в охороні здоров'я – від первинної медичної допомоги до складних інтегрованих систем даних. Приділення особливої уваги законам і стандартам, що регулюють кібербезпеку в галузі медицини і забезпечення дотримання всіма медичними установами відповідних стандартів кібербезпеки, є найвищим пріоритетом [313]. Ці стандарти особливо важливі для забезпечення належного рівня контролю доступу до конфіденційної інформації, що є основою довіри пацієнтів до системи охорони здоров'я

Зважаючи на голландський досвід, ми можемо зробити висновок, що кібербезпека є ключовим чинником успішного функціонування системи eHealth у цій державі. Україні, на нашу думку, необхідно перейняти такий комплексний підхід, який уключає як технічні, так і організаційні заходи, зокрема забезпечення належної правової бази, розробку стандартів інформаційної безпеки та введення регулярних незалежних перевірок кібербезпеки. Беручи до уваги вимоги щодо кібербезпеки, для її забезпечення та оптимізації процесу лікування слід приділяти особливу увагу залученню пацієнтів та медичних працівників до розроблення новітніх технологій. Тільки в цих умовах може бути гарантована безпечна і ефективна робота системи eHealth не тільки для

поліпшення доступу до медичних послуг, але й для високого рівня якості й безпеки.

Медична галузь за останні роки, на жаль, стала легкою мішенню для кіберзлочинців через низку вразливостей, зумовлених використанням застарілого програмного забезпечення та відсутністю ефективних заходів кіберзахисту. Проблема поглиблюється тим, що більшість дій із підвищення рівня кібербезпеки впроваджується після вже здійснених атак, що є відображенням реактивного підходу до безпеки. Як бачимо, недооцінювання значення кібербезпеки у медичній галузі та сприйняття її як другорядного аспекту, веде до того, що організації не готові вкладати кошти й ресурси у превентивні заходи та відповідно наражають себе на небезпеку.

Доречно підкреслити важливість проактивного підходу до кібербезпеки. Він уключає впровадження сучасних технологій, постійне оновлення систем та навчання персоналу. І тут варто згадати Францію, яка створила важливий політичний прецедент для реформи системи охорони здоров'я, розробивши національну систему електронних медичних записів Dossier Medical Partage (DMP). Упровадження DMP було спрямоване на підвищення ефективності медичних послуг за рахунок поліпшення співпраці між медичними працівниками та пацієнтами. Такий крок має значний політичний сенс, оскільки відображає бажання французької держави створити більш інтегровану систему охорони здоров'я. Хоча DMP покращує доступ до медичних даних та може оптимізувати прийняття клінічних рішень, він стикається з багатьма проблемами, що впливають на ефективність його застосування [314]. Франція прагнула створити систему, яка могла б підвищити доступність медичних послуг та ефективно керувати медичними даними, але політичні чинники, особливо недосконаліть нормативно-правової бази та відсутність належної координації на державному рівні, значно ускладнили цей процес.

У цьому контексті важливим кроком стало створення Agence nationale de la sécurité des systèmes d'information, яка з 2012 року розробляє загальну безпекову політику для інформаційних систем, зокрема й охорони здоров'я, а

також створення структури сумісності для визначення технічних стандартів. Цей крок, на нашу думку, демонструє, що Франція визнала необхідність інтеграції кібербезпеки в охорону здоров’я як критичний елемент забезпечення ефективного її функціонування. Водночас це підтверджує, що цифровізація охорони здоров'я не може відбуватися без розроблення надійної політики кіберзахисту, що є фундаментальною умовою для підтримки довіри громадян до нових технологій.

Пандемія COVID-19 створила особливо благодатний ґрунт для кібератак у Франції. Установи охорони здоров'я, як і решта суспільства, що пережили стрімку цифровізацію, отримали негативні наслідки – масштабні кібератаки на систему охорони здоров’я.

У лютому 2021 року на продаж було виставлено 500 000 французьких медичних документів, викрадених з лабораторних баз у Бретоні та Нормандії (випадок «особливої серйозності», як зазначив тоді Луї Дютейє де Ламот – генеральний секретар національної комісії з інформаційних технологій та свобод) [315].

Діяльність лікарні, яка постраждала від кібератаки, що вивела з ладу її IT-систему, відновлювалася «дуже поступово». Лікарняний центр Дакс Ланд став жертвою кібератаки, яка паралізувала майже всі інформаційні системи [316].

Лікарня поблизу французької столиці Парижа також стала жертвою кібератаки. Тоді вона була змушена відмовляти у прийомі екстрених пацієнтів. Окрім іншого, атака тимчасово перешкоджала доступу до програмного забезпечення лікарні та інформаційної системи для прийому пацієнтів. У лікарні Версаля в Івелині кібератака порушила роботу медперсоналу та прийом пацієнтів. Кібератака була націлена на всю установу, уключаючи лікарню Андре-Міньо (будинок для людей похилого віку Деспань) і лікарню Рішо у Версалі, розташовану за кілька кілометрів від нього. Для безпеки пацієнтів було мобілізовано всі сили, додатковий персонал був викликаний для надання інтенсивної терапії та безперервного догляду, було також надано змінне обладнання [317].

Усього за кілька днів лікарня Вільфранш-сюр-Сон (Рон) також стала жертвою кібератаки. За погодженням із Регіональним агентством охорони здоров'я пацієнти, які потребували екстрених служб у Вільфранші та Тарарі, направлялися до інших лікарень для подальшого лікування. Особи, які звернулися до відділення невідкладної допомоги самостійно, за необхідності могли бути направлені до інших медичних установ. Безпека пацієнтів, які перебували на лікуванні у відділенні безперервної терапії та інтенсивної терапії Вільфранша, була належним чином забезпечена. Те саме стосувалося і немовлят, які перебували у неонатальному відділенні. Пологовий будинок був здатний прийняти майбутніх мам і пологи. Продовжувалася також кампанія з вакцинації проти Covid-19, проте всі заплановані хірургічні процедури були відкладені [318].

Таким чином, у 2022 році у лікарнях було зареєстровано 730 повідомлень про інциденти. Найбільш яскравим прикладом залишиться кібератака на лікарню Корбей-Ессон, оскільки вона поєднала різні типи кібератак. 20 серпня 2022 року російськомовна хакерська група Lockbit 3.0 спровокувала масштабний витік даних і поширила в даркнеті більше 11 гігабайт персональних даних [319].

Отже, можемо зазначити, що на сьогодні Франція має значні кібератаки на електронну охорону здоров’я. Незважаючи на велику кількість розроблених методик протидії та шляхів їх упровадження, загроза кібератак на критично важливу медичну інфраструктуру та інформацію загалом усе ще залишається високою. Упровадження цифрових технологій в охорону здоров'я є складним завданням, що вимагає не лише технічних рішень, але й значних організаційних змін. Трансформація eHealth потребує адаптації умінь і навичок медичних працівників до нових моделей роботи, що включає навчання використанню технологій та інтеграцію великих баз даних у політику охорони здоров'я. З цього погляду Франція продемонструвала готовність інвестувати в інновації, що підтверджено створенням наприкінці 2022 року Агентства інновацій в

охороні здоров'я (AIS). Цей захід спрямований на підтримку умов для ефективної інтеграції новітніх технологій у медичну сферу.

Франція також взяла на себе лідерство у впровадженні цифрових інновацій у систему охорони здоров’я через Програму пріоритетних досліджень та інфраструктури цифрової охорони здоров'я (PEPR), запущену у червні 2023 року [320]. Ця програма має суттєве політичне значення, адже Франція прагне стати європейським лідером щодо цифрової охорони здоров'я, що сприятиме не лише її внутрішньому розвитку, але й міжнародному впливу у цій галузі. Це створює передумови для того, щоб Франція виступала експортером інноваційних практик з охорони здоров'я для інших країн Європи.

Водночас розбудова системи електронної охорони здоров’я стикається з ключовими викликами, зокрема щодо забезпечення конфіденційності та безпеки даних. Збір, зберігання та оброблення чутливої інформації про пацієнтів робить систему потенційною мішенню для кіберзлочинців, а порушення безпеки, як ми наголошували, може мати катастрофічні наслідки як для окремих осіб, так і для національної безпеки загалом. Тому Франція приділяє особливу увагу розвитку нормативно-правових стандартів у кібербезпеці, що дозволяє забезпечити відповідність системи eHealth міжнародним вимогам безпеки. А це, своєю чергою, демонструє бажання уряду забезпечити надійність цифрової інфраструктури як важливої частини національної стратегії безпеки.

Дорожня карта цифрової охорони здоров'я на 2023 – 2027 роки є черговим свідченням прагнення Франції інтегрувати цифрові технології в охорону здоров'я на всіх рівнях. Координація цієї дорожньої карти здійснюється Делегацією цифрової охорони здоров'я (DNS) спільно з Агентством цифрової охорони здоров'я (ANS), що вказує на високий рівень співпраці між державними та приватними інституціями [321,322]. На нашу думку, політичний вимір цієї співпраці є надзвичайно важливим, оскільки лише синхронізація дій різних учасників уможливлює ефективну реалізацію цифрового трансформування охорони здоров'я.

Отже, можемо зробити висновок, що приклад Франції є необхідним до перейняття Україною, яка також перебуває на шляху до розбудови власної системи електронної охорони здоров'я. Виклики кібербезпеки, з якими стикається Франція, є релевантними й для України, що робить досвід Франції цінним джерелом для формування політики щодо цифровізації охорони здоров'я. Підходи до забезпечення безпеки, сумісності систем та впровадження інновацій, що застосовуються у Франції, можуть бути використані як приклади для адаптації у вітчизняних умовах. Тож Франція не лише виступає як зразок для наслідування, але й як партнер у спільній боротьбі з викликами цифрової ери, що є ключовим для забезпечення національної безпеки. Однак, на наш погляд, все ж таки, ураховуючи сучасне геополітичне становище, в Україні потрібна більш системна конструкція реформування eHealth.

Одним із прикладів такої системи виступає Сполучене Королівство, де системи eHealth побудована найскладніше. Кожна з чотирьох країн, які належать Сполученому Королівству (Англія, Шотландія, Уельс і Північна Ірландія), мають власну окрему службу охорони здоров’я, однак єдине фінансування Національною службою охорони здоров’я (NHS). Чотири служби охорони здоров'я працюють незалежно, при цьому існує тісна співпраця для гарантування, що всі громадяни отримують однакову якість обслуговування. У деяких прикордонних районах жителі однієї країни можуть отримувати медичні послуги від сусідньої служби охорони здоров’я. NHS діє за принципом безкоштовного медичного обслуговування для всіх і фінансується за рахунок загального оподаткування. Поточна структура управління охороною здоров'я в Англії набула чинності 1 липня 2006 року. Національна служба охорони здоров’я в Уельсі є підпорядкованою Уряду Асамблеї Уельсу. Уельська асамблея – децентралізована адміністрація, яка отримує свої повноваження від парламенту Великобританії та відповідає за ряд питань, зокрема й тих, що стосуються охорони здоров'я. У 2010 році NHS Уельсу видав власну програму з розроблення нових методів, інструментів та інформаційних технологій для трансформації медичних послуг для жителів Уельсу [323]. Щоб підвищити

ефективність роботи лікарень Нового Південного Уельсу, eHealth NSW хотіла впровадити нову платформу управління послугами в межах 10-річної цифрової трансформації. Стратегія електронної охорони здоров’я на 2016–2026 рр. має на меті спрямувати охорону здоров’я Нового Уельсу на надання послуг світового рівня. Відповідно до цієї системи Міністерство охорони здоров'я Нового Південного Уельсу в масштабах штату контролюватиме прогрес у реалізації стратегії, політики та інвестицій у галузі електронної охорони здоров'я. Стратегія акцентує на основних принципах для реалізації концепції «Цифрової та інтегрованої системи охорони здоров'я, що забезпечує орієнтований на пацієнта досвід у галузі охорони здоров'я та якісні результати щодо здоров'я» [324].

Як бачимо, зростання впровадження цифрових технологій та можливості інформаційних систем у системі охорони здоров'я Нового Південного Уельсу становить складне завдання, яке постійно розвивається.

Національна служба охорони здоров’я в Шотландії є підпорядкованою уряду Шотландії, у якій є власний парламент і виконавча влада, що отримують повноваження від парламенту Великобританії, а також відповідають за охорону здоров’я. Шотландія має власну стратегію електронної охорони здоров’я, якою керує Департамент охорони здоров’я країни. Перша стратегія відомостей щодо охорони здоров’я та соціальної допомоги опублікована в лютому 2023 року. Стратегія формулює положення щодо найкращого використання даних в організації надання послуг. Вона закладає основу для трансформації того, як члени громадськості отримують доступ до даних і використовують їх для покращення власного здоров’я та благополуччя. Визначені також пріоритети для покращення надання медичної та соціальної допомоги, уключаючи вдосконалення систем та інфраструктури [325].

Національна служба охорони здоров’я Північної Ірландії дещо відрізняється від інших служб охорони здоров’я Великобританії тим, що вона має комбіноване управління охороною здоров’я та соціальною допомогою. Північна Ірландія зберігає власну окрему адміністрацію під керівництвом

Управління Північної Ірландії уряду Великобританії. Охорона здоров’я та соціальна допомога в Північній Ірландії підпорядкована Департаменту охорони здоров’я, соціальних послуг і громадської безпеки уряду Північної Ірландії з власною стратегією електронної охорони здоров’я. Стратегічні органи охорони здоров’я відповідають за координацію та ефективне управління прогресом місцевих органів Національної служби охорони здоров’я. NHS Connecting for Health – це агентство Департаменту охорони здоров’я Великобританії, яке відповідає за реалізацію Національної програми з IT (NPfIT) в Англії. Міністерство охорони здоров’я, соціальних служб і громадської безпеки (DHSSPS) Північної Ірландії має узгоджену стратегію електронної охорони здоров’я. У Північній Ірландії розпочато шлях трансформації того, як надаються послуги з охорони здоров'я та соціальної допомоги населенню. У 2022 році прийнято стратегію «Здоров’я та благополуччя до 2026 року – Діятимемо разом». У новій стратегії описано, як розв’язуватимуться завдання забезпечення цифрової трансформації, необхідної для покращення результатів у галузі охорони здоров'я в майбутньому, що буде забезпечено скоординованим регіональним управлінням. Цифрова трансформація будується навколо ключових пріоритетних програм та ініціатив, які будуть реалізовані протягом наступних 4 – 5 років. Вони дозволять покращити роботу організації та допоможуть співробітникам працювати гнучкіше. Названа програма є найбільшою та значущою цифровою інвестицією й забезпечить єдиний цифровий запис про медичне обслуговування для кожного громадянина, якому надаються медичні послуги та догляд, і буде доступною для всіх постачальників медичних послуг. Однак, охорона здоров'я та соціальне забезпечення Північної Ірландії прагне створити стабільну та ефективну систему охорони здоров'я, оскільки системи охорони здоров'я стають дедалі сприйнятливішими до кіберзлочинності. Так, ураховуючи зростання частоти та серйозності кібератак у всьому світі, кібербезпека буде пріоритетом для надання послуг на багато років уперед. У світлі цього до цифрової Стратегії охорони здоров’я на 2022 – 2026 додано додаткову Стратегію кібербезпеки охорони здоров'я та соціального

забезпечення на 2022— 2030 рр. Для покращення позиції з кібербезпеки ця стратегія додає впровадження інноваційних продуктів, постачальників та нових структур управління безпекою. В організаційному контексті HSC визначає кібербезпеку як таку, що включає інформацію, програми, інфраструктуру та фізичне розташування технологічних активів. Правила передбачають правові заходи щодо підвищення загального рівня безпеки як кібер-, так і фізичної стійкості мереж та інформаційних систем. Це передбачає безпечне надання цифрових послуг, уключаючи транспорт, енергетику, водопостачання, цифрову інфраструктуру та охорону здоров'я [326].

Цифрова охорона здоров’я відіграє неабику роль у покращенні охоплення, впливу та ефективності сучасної охорони здоров’я. Сектор охорони здоров’я Великобританії визнав це понад 30 років тому і зараз розробляє одні з найдосконаліших систем у світі для відстеження, управління та надання послуг, орієнтованих на пацієнта. «Цифрове здоров’я» принесло величезні переваги первинній медичній допомозі у Великобританії. Універсальна електронна система обліку пацієнтів дозволяє лікарям працювати ефективніше, отже, пацієнти отримують кращий сервіс. Система також надає лікарям відгуки про їхню роботу [327].

Розвиток електронної охорони здоров’я передбачає і посилення кібербезпеки. Через діджиталізацію всі системи держав, зокрема охорона здоров’я, опинилися під новими викликами, які можуть не тільки пошкодити чи зруйнувати систему, а й навіть привести до загибелі людей. Кількість кібератак на електронну систему охорони здоров’я, на жаль постійно зростає, а не всі системи готові до таких випробувань.

Так, одна з кібератак сталася 12 травня 2017 року, коли програма-вимагач WannaCry вразила організації по всьому світу. Але особливо постраждали лікарні загальної практики в Англії та Шотландії. Значну кількість послуг було порушено, оскільки зловмисне програмне забезпечення зашифрувало комп’ютери, що призвело до скасування тисяч прийомів та зміни маршрутів машин швидкої допомоги. Від атаки постраждали понад 60 фондів

Національної служби охорони здоров'я Великої Британії (NHS), оскільки вірус поширився на понад 200 000 комп'ютерних систем у 150 країнах світу. Це була і залишається найбільшою кібератакою у Великій Британії, і навіть якщо Національна служба охорони здоров’я насправді не була конкретною мішенню WannaCry, це був тривожний сигнал про те, як програмне забезпечення-вимагач та інші кіберкампанії можуть бути ризиком для організації з 1,5 мільйонів співробітників, яка надає медичні послуги по всій країні [328]. Ще 603 заклади первинної медичної допомоги та інші організації Національної служби охорони здоров'я були інфіковані WannaCry, зокрема 8% лікарських амбулаторій [324]. Перебої у наданні вторинної медичної допомоги вплинули на первинну медичну допомогу, наприклад, на доступ до результатів аналізів. Постраждали також сторонні системи, наприклад DocMan42, що вплинуло на електронний потік клінічної інформації від вторинної до первинної медичної допомоги [329].

2024 рік приніс ще сильнішу кібератаку на NHS Trust, який відповідає за групу лікарень у північно-західній Англії. Атака призвела до оголошення про «великий інцидент», який сигналізував про кризу в системі охорони здоров'я через серйозні ризики для здоров'я населення, коли амбулаторні прийоми були скасовані, а персонал лікарні перейшов на ручні операції через утрату доступу до електронних даних. Інцидент став частиною серії нападів на Національну службу охорони здоров'я, уключаючи атаку на постачальника медичних послуг Synnovis [330], яка припинила медичні послуги та скасувала тисячі процедур. Це підкреслює нагальну необхідність зміцнення кібербезпеки національної служби охорони здоров'я для забезпечення стійкості системи. І такі атаки як найкраще підкреслюють, що кібертероризм – уже загроза не «теоретичного» характеру, а та, що може призводити до значних руйнацій.

Управління охорони здоров’я Ірландії (HSE) зіткнулося із значною атакою програм-вимагачів у травні 2021 року. Зловмисники використовували програми-вимагачі Conti, щоб отримати викуп за розшифрування файлів і відновлення доступу до уражених систем. Атака Conti була спрямована на велику кількість лікарень Ірландії, що спричинило збій по всій країні. Злочинці

вимагали викуп у розмірі майже 20 мільйонів доларів, але уряд відмовився його платити. Через напад різні медичні служби були закриті, а прийоми скасовані. Страйк також закрив портал COVID-19. Унаслідок цього країна протягом багатьох тижнів зосереджувалася на відновленні своєї електронної системи охорони здоров’я. Багато служб екстреної допомоги все ще працювали, але також були й затримки із записами, результатами COVID19, видачею свідоцтв про народження та смерть. Постраждало близько 40 лікарень. Система охорони здоров’я країни співпрацювала з міжнародними та національними оборонними групами, такими, як Національний центр кібербезпеки, GradaSiochana, Ірландські сили оборони, Інтерпол та Європол. Оссіан Сміт, державний міністр державних закупівель та електронного уряду, заявив, що атака була міжнародною та найзначнішою кібератакою на ірландську державу [331].

На сьогодні Великобританія продовжує вживати значних заходів для підвищення кібербезпеки в своїй системі eHealth, визнаючи критичну важливість захисту чутливих даних пацієнтів та забезпечення стійкості медичних послуг перед кіберзагрозами.

У 2023 році Міністерство охорони здоров'я та соціального забезпечення Великобританії випустило «Стратегію кібербезпеки для охорони здоров'я та соціального забезпечення: 2023— 2030 роки» [332], яка стала керівними принципами політики підвищення стійкості галузі до 2030 року. Така стратегія, на нашу думку, не тільки підкреслює важливість захисту пацієнтів та персоналу, але й забезпечує основу для охоплення інфраструктури охорони здоров'я на всіх рівнях. У політичному сенсі це знаменує собою перехід від фрагментарних заходів до всеосяжного та спільного підходу до кібербезпеки в охороні здоров'я.

Інтеграція медичних і соціальних організацій із центром кібербезпеки національної служби охорони здоров'я Великобританії демонструє прагнення створити національну мережу захисту, що працює в режимі реального часу. Такий підхід, що охоплює мільйони пристроїв і блокує мільйони загроз, демонструє прагнення держави забезпечити стійкість кіберпростору як

елемента національної безпеки. Такі заходи також свідчать про ефективну політичну координацію між різними установами, спрямовану на забезпечення захисту від зовнішніх загроз.

Великобританія також запровадила розширені регуляторні заходи для приватних підрядників, які надають ключові державні послуги, уключаючи сектор охорони здоров'я. Політичне значення цього кроку полягає в тому, що приватні компанії, які працюють у галузі медицини, повинні дотримуватися тих самих стандартів безпеки, що і державні установи. Це створить єдині вимоги до кібербезпеки по всій країні, зменшить вразливості в системах охорони здоров'я та підвищить загальну стійкість до кіберзагроз. Таким чином, Великобританія є прикладом держави, для якої кібербезпека стала пріоритетом у політичному порядку денному.

Швеція активно впроваджує електронне здоров'я та технології добробуту для підвищення якості медичних і соціальних послуг. Електронне здоров'я охоплює використання цифрових інструментів і обмін інформацією в цифровому форматі для забезпечення фізичного, психічного та соціального благополуччя. Socialstyrelsen, центральний орган у цій сфері, сприяє розвитку структурованої та ефективної документації в галузі охорони здоров'я та соціального захисту, забезпечуючи семантичну інтероперабельність між персоналом і системами [333].

Ураховуючи високий рівень цифровізації, галузь охорони здоров'я стала особливо вразливою до кіберзагроз. У відповідь уряд Швеції визначив її одним із 6 ключових соціальних секторів та розробив Національну стратегію кібербезпеки й інформаційної безпеки для цього сектору. 1 стратегія включає 17 конкретних ініціатив, спрямованих на підвищення здатності систем охорони здоров'я прогнозувати, запобігати, виявляти та реагувати на кіберзагрози. PwC вносить пропозиції щодо пом'якшення та управління кіберзагрозами в державних установах, особливо в секторі охорони здоров'я. Ці рекомендації спрямовані на зниження ймовірності кібератак і мінімізацію наслідків у разі їх виникнення. Цей підхід передбачає зменшення вразливостей та підвищення

здатності виявляти загрози та швидко реагувати на них. Швеція також реалізує концепцію електронного здоров'я 2025 року, яка є спільним проєктом між урядом та шведською Асоціацією муніципалітетів та регіонів (SKR) і має на меті стати світовим лідером у галузі eHealth до 2025 року. Стратегія охоплює 4 ключові напрямки: індивідуальну участь, точну інформацію та доступ до інформації, безпечне управління інформацією та спільний розвиток цифрових перетворень.

Тож можна вважати, що Швеція є одним із лідерів у впровадженні забезпечення кібербезпеки eHealth у цій галузі. Україні варто перейняти досвід Швеції у створенні національної стратегії кібербезпеки для eHealth, зокрема, це стосується упровадження цифрових рішень у медичну практику та підвищення цифрової компетентності медичного персоналу. Це сприятиме підвищенню ефективності та безпеки електронної системи охорони здоров'я в Україні.

Отже, перейняття досвіду європейських країн із забезпечення кібербезпеки eHealth у викликах сучасності зможе дати Україні значний поштовх, оскільки в сучасних умовах гібридної війни політика соціального захисту населення, особливо щодо охорони здоров’я, є надзвичайно важливою.

Тож, дослідивши приклад держав Європи, важливим вважаємо створити перелік тих дій, які, на нашу думку, доцільно було б інтегрувати в Україні. Насамперед укажемо на нинішні механізми, які забезпечують захист державної політики у сфері охорони здоров’я, забезпечуючи її кібербезпеку.

eHealth в Україні є вагомим прикладом реформування та цифрової трансформації в державному секторі, яка здійснюється у межах реалізації політики національної безпеки. Це впровадження не лише покращило медичні послуги для громадян, але й стало важливим політичним інструментом зміцнення системи охорони здоров'я відповідно до європейських стандартів. Слід також розглянути політичні аспекти забезпечення кібербезпеки eHealth, ураховуючи її потенціал як у зміцненні, так і в підриві національної безпеки.

Еволюція eHealth розпочалася з ухвалення Концепції реформи фінансування системи охорони здоров'я у 2016 році [334]. Це рішення стало

одним із стратегічних політичних кроків, яке передбачало використання цифрових технологій для реалізації принципу «гроші йдуть за пацієнтом». Особливо важливим є політичний вимір цієї реформи, адже вона забезпечує прозорість та ефективність розподілу бюджетних коштів. Однак ця відкритість може мати зворотній ефект у випадку недостатнього забезпечення кібербезпеки, що ставить під загрозу не лише персональні дані пацієнтів, але й системну стабільність усього медичного сектору.

Починаючи з 2017 року, eHealth поступово розвивалася, долучаючи все більшу кількість медичних закладів до електронної системи, упроваджуючи нові функції, зокрема електронні рецепти та медичні картки [335]. Цей процес супроводжувався розширенням ролі державних інституцій, зокрема Міністерства охорони здоров’я, яке здійснює нормативне регулювання, та Національної служби здоров’я України, що адмініструє фінансування. Однак цей процес не призвів до необхідності підвищення рівня кібербезпеки.

Упровадження eHealth досягло значних успіхів, таких, як забезпечення прозорості фінансування охорони здоров'я, підвищення ефективності використання ресурсів, пришвидшеної доступності медичних послуг та створення умов для більш активної участі громадян у системі охорони здоров'я. Але ці позитивні зміни можуть бути втрачені через відсутність належної кібербезпеки, що робить життя та здоров’я пацієнтів вразливими до поведінки зловмисників.

Така складність має особливе значення для державної та соціальної політики України, адже проблема забезпечення кібербезпеки eHealth безпосередньо пов'язана з національною безпекою. Кібератаки на системи можуть негативно вплинути як на здоров'я окремих громадян, так і на функціонування державних установ, що призведе до втрати даних і погіршення життєво важливих медичних послуг. Таким чином, державна політика в цій галузі повинна бути спрямована на зміцнення кібербезпеки, розробку власних технічних рішень, перейняття та інтегрування досвіду від іноземних партнерів. Таким чином, забезпечення кібербезпеки eHealth повинно стати одним із

пріоритетних напрямів державної політики України з охорони здоров'я та національної безпеки.

У виступі Дениса Цвайга, президента Національної асоціації кібербезпеки, під час виставки «PublicHealth 2020» було наголошено на вразливості електронної системи охорони здоров’я в умовах потенційних кібератак. Він висловив, що, незважаючи на зручність використання електронної системи, небезпечним є той факт, що натискуванням однієї кнопки можна вимкнути будь-яку клініку, будь-який апарат штучного дихання. Він також наголосив, що важливо усвідомлювати, що ці ризики існують і є питанням національної безпеки. Окрім того, на його думку, доцільним є на державному рівні окремо визначити стратегію з кібербезпеки в системі охорони здоров’я, а також необхідно прописати інструкції щодо дій під час застосування кіберзброї та як попередити кібератаку. Більше того, з точки зору доповідача, необхідно передбачити кримінальну відповідальність посадових осіб, які пропускають кібератаки, а також запровадити освітній проект, спрямований на ліквідацію невігластва у сфері кібербезпеки [336].

Уважаємо, що побоювання, висловлені спікером, є реальними, адже через те що нововведена система розвивається дуже стрімко, зосереджуючись на питаннях автоматизації процесів та покращення доступу до медичних сервісів, кібербезпека відходить на другий план, що спрощує можливість атак на систему та є вкрай небезпечним як для конкретної особи, так і для держави загалом.

28 грудня Кабінет Міністрів України затвердив Концепцію розвитку електронної системи охорони здоров'я [337]. Реалізація Концепції прогнозована на період до 2025 року й передбачає розв’язання нинішніх проблем і викликів шляхом забезпечення виконання комплексних заходів за такими напрямками: нормативне забезпечення розвитку електронної системи охорони здоров’я; організаційне, управлінське та технічне забезпечення розвитку електронної системи охорони здоров’я, ресурсне забезпечення; забезпечення якості, безпечності та доступності електронної системи охорони здоров’я [338].

Політична важливість цієї проблеми полягає в тому, що держава має визнати кібербезпеку елементом національної безпеки. Зручність електронної системи може стати ахіллесовою п’ятою, якщо не буде належної уваги до захисту від кібератак. Наразі у випадку серйозних збоїв або атак можлива повна втрата функціональності певних сегментів медичної інфраструктури, що в умовах війни чи кризи може призвести до катастрофічних наслідків.

У цьому контексті важливо згадати про певні кроки, спрямовані на закріплення відповідальності посадових осіб за забезпечення належного рівня кібербезпеки. Запровадження кримінальної відповідальності за халатність у цій галузі, на нашу думку, могло б стати ефективним інструментом для підвищення персональної відповідальності керівників. Крім того, необхідність чітких інструкцій та сценаріїв реагування на кіберзагрози стала б фундаментом для підготовки системи охорони здоров'я до можливих надзвичайних ситуацій. На рівні політичної стратегії Україна повинна зробити кібербезпеку eHealth пріоритетним напрямом розвитку, що має бути закріплено в національних планах та концепціях розвитку.

3.2.2. Проблема захисту критичної інфраструктури України в умовах воєнного стану та практичні заходи щодо її вдосконалення

Військова агресія Росії проти України робить проблему кібербезпеки ще більш актуальною. Умови гібридної війни, в яких перебуває Україна, вимагають особливого акценту на захисті критичної інфраструктури, до якої належить і система eHealth. Атака на електронну систему охорони здоров’я може бути частиною ширшої стратегії дестабілізації держави, оскільки впливає на життя сотень тисяч громадян. Таким чином, посилення кібербезпеки eHealth не лише забезпечить безперервність надання медичних послуг, але й стане елементом захисту національної безпеки в умовах зовнішніх загроз.

Після початку повномасштабної війни в Україні значна кількість громадян почала стикатися з потребою в отриманні медичних та психологічних послуг. Війна і масове переміщення людей стали рушійною силою для

інновацій у медицині. Реформування стало вимогою часу і прискорило використання інформаційних технологій та електронної медичної допомоги. Електронна система охорони здоров’я в умовах війни перепланувала свою роботу з урахуванням нових обставин. Війна підштовхнула до розвитку комфортного та доступного для всіх українців сервісу, а також використання сучасних методів діагностики й лікування.

Сектор охорони здоров’я є одним із найбільш постраждалих унаслідок війни. Станом на 21 червня 2022 року повністю було зруйновано 118 об'єктів закладів охорони здоров’я, частково зруйновано 633 об'єкти закладів охорони здоров’я. Окрім того, на жаль, система електронної охорони здоров’я України стала об’єктом ворожих кібератак.

Захист даних відповідає українському законодавству, зокрема наявний атестат комплексної системи захисту інформації, тобто вона відповідає національним стандартам забезпечення захисту даних та запобігання втручанням. Система періодично проходить безпекові аудити, ведеться також робота з перевірки стресостійкості й інших безпекових характеристик. Окрім того, ураховано принципи GDPR [339] і міжнародні стандарти захисту інформації. Система захисту побудована таким чином, що персональні дані людини й медичні дані зберігаються окремо. Якщо навіть і відбувається хакерська атака, то отримати інформацію щодо медичних даних конкретної людини неможливо.

Для протидії хакерським атакам і забезпечення належного рівня кібербезпеки Міністерство охорони здоров'я України видало Наказ від 15 червня 2022 року «Про утворення Робочої групи з питань розробки й реалізації Концепції стратегічних напрямів розвитку кібербезпеки з електронної охорони здоров'я». Згідно з наказом робоча група з питань реалізації «Концепції стратегічних напрямів розвитку кібербезпеки у сфері електронної охорони здоров'я» є дорадчим органом Міністерства охорони здоров'я України. Її мета – здійснювати експертнй супровід процесів підготовки, опрацювання, узгодження позицій під час підготовки пропозицій щодо її реалізації.

Серед основних завдань Робочої групи можна виділити такі:

– здійснення аналізу поточного стану кібербезпеки з електронної охорони здоров'я;

– визначення шляхів розв’язання проблемних питань, що виникають під час забезпечення кібербезпеки електронної охорони здоров'я;

– сприяння забезпеченню узгоджених дій органів державної влади щодо визначення пріоритетів розвитку галузевої системи кібербезпеки електронної охорони здоров'я;

– напрацювання пропозицій щодо здійснення заходів із впровадження стандартів кібербезпеки на основі стратегічних напрямів розвитку кібербезпеки електронної охорони здоров'я,

– забезпечення міжвідомчої взаємодії та організації діяльності всіх учасників, залучених до виконання завдань Робочої групи.

Додатково МОЗ спільно з партнерами розробили план відновлення медичної системи від наслідків війни, який дозволить не просто відбудувати зруйновану медичну інфраструктуру. Головною метою реалізації цього плану є відновлення та розвиток системи охорони здоров’я з новою якістю і доступністю послуг для задоволення потреб громадян. Для реалізації цієї мети План відновлення охорони здоров’я [340] передбачає забезпечення фінансової стабільності системи охорони здоров’я, розширення програми медичних гарантій, розвитку ринку добровільного медичного страхування, посилення медичних послуг для задоволення особливих потреб людей, викликаних війною, зміцнення та посилення кадрових ресурсів системи охорони здоров’я, посилення системи громадського здоров'я та готовності до надзвичайних ситуацій у сфері охорони здоров’я. Важливим є зосередження уваги на розвитку електронної охорони здоров'я та посилення кібербезпеки шляхом формування єдиного медичного інформаційного простору з національною і транскордонною інтероперабельністю та наскрізними процесами й сервісами. Окрім того, визначено порядок забезпечення інфраструктурних та технічних умов надання якісних медичних послуг із використанням інформаційно-комунікаційних

систем на всіх рівнях, створення зручних та прозорих механізмів доступу користувачів до повних даних про своє здоров'я, управління цією інформацією [341].

На сьогодні в державах Європи одним із основних засобів захисту від кібератак уважаються міжмережеві екрани (firewalls), які забезпечують захист від несанкціонованого доступу до внутрішніх мереж. Проте їхня ефективність без належного налаштування та оновлення може бути низькою. В Україні ці системи в основному використовуються в комерційному секторі, натомість медичні установи часто ігнорують їх через нестачу фінансування [342]. Важливо зазначити, що проблема фінансування потребує вирішення на державному рівні. Підтримка медичних установ у впровадженні та обслуговуванні систем кібербезпеки є інвестицією в захист здоров'я нації.

Іншим важливим засобом є системи виявлення та запобігання вторгненням (IDS/IPS), які дозволяють виявляти аномалії в реальному часі [343]. У країнах Європи ці системи вже впроваджені на рівні державних медичних платформ, що забезпечує централізовану координацію та своєчасне виявлення загроз. Такі країни, як Велика Британія чи Естонія, активно впровадили указаний механізм захисту в систему кібербезпеки охорони здоров’я. В Україні наразі відсутня централізована система виявлення та запобігання вторгненням (IDS/IPS) на рівні державних медичних платформ, що є суттєвою проблемою, зважаючи на величезний обсяг чутливих даних, які містить eHealth. Зростання кіберзагроз, особливо в умовах війни, робить медичні установи та eHealth привабливими цілями для зловмисників, а наслідки кібератак можуть бути катастрофічними, уключаючи порушення надання медичної допомоги та загрозу життю пацієнтів.

Упровадження IDS/IPS в eHealth, на нашу думку, є критично важливим для забезпечення надійного захисту медичних даних, вчасної ідентифікації та блокування кібератак, а також централізованого контролю й координації заходів кібербезпеки в масштабах країни. Це дозволить підвищити надійність eHealth та забезпечити безперебійне надання медичних послуг. Для досягнення

цієї мети було б доцільно розробити та затвердити державну стратегію кібербезпеки eHealth, яка передбачатиме впровадження IDS/IPS, виділити необхідне фінансування та залучити провідних експертів із кібербезпеки. Важливо також інтегрувати IDS/IPS з нинішніми системами захисту eHealth для забезпечення комплексного захисту.

Особливу увагу також слід приділити захисту переданих даних, для цього використовуються віртуальні приватні мережі (VPN) [344]. Вони шифрують відомості, що особливо важливі для медичних установ, де передаються конфіденційні дані пацієнтів. Однак, як показує європейський досвід, слабкі паролі та відсутність оновлень можуть призвести до порушень безпеки. В Україні впровадження VPN потребує суворих вимог до автентифікації та регулярних перевірок.

Шифрування даних є одним із найефективніших способів захисту конфіденційної інформації [345]. Проте для його ефективного застосування необхідно ретельно управляти криптографічними ключами, а їх утрата може призвести до незворотної втрати даних. В українських медичних установах шифрування застосовується лише частково, що збільшує ризик витоків інформації. Тому потрібно розробити державні регламенти, які вимагатимуть обов'язкового шифрування медичних записів.

Однак технічні засоби захисту є недостатніми, а людський чинник найбільш вразливий. Недостатня підготовка медичного персоналу часто стає причиною успішних кібератакатак. У країнах Європи існують обов’язкові програми навчання медичних працівників, які підвищують їх обізнаність про кіберзагрози. В Україні такі програми тільки починають розроблятися, що створює значні ризики для кібербезпеки.

Щодо практичних заходів, то можемо відзначити організацію USAID, що співпрацює з українським урядом, громадянським суспільством, неурядовими організаціями та партнерами для розбудови загальної системи охорони здоров’я України. Організація сприяє розбудові системи, яка служить народу України та гарантує, що медичні працівники мають інструменти, знання й ресурси для

надання високоякісної сучасної медичної допомоги всім українцям. USAID здіснює велику кількість проектів з Україною, мета одного із них полягає у підтримці місцевих систем охорони здоров'я для реагування на критичні потреби та відновлення базових медичних послуг, щоб знизити рівень захворюваності і смертності, спричинених війною та нерегулярним доступом до медичної допомоги (період реалізації проекту – з 24 березня 2023 р. по 30 вересня 2024 р.) [346].

Оскільки, як уже було зазначено, з початку повномасштабної війни значно зросла кількість кібератак на критично важливу інфраструктуру, а заклади охорони здоров'я знаходяться на передовій атак зловмисників, які прагнуть порушити їх роботу, викрасти та використати медичні дані мільйонів українців, то зосередження діяльності проекту стосується таких напрямків:

– адаптації та зміцнення управління в секторі охорони здоров'я в умовах війни;

– усунення ризиків для стабільного та прозорого фінансування охорони здоров'я;

– сприяння відновленню та розбудові кадрового потенціалу охорони здоров'я;

– покращення стабільної та безпечної роботи медичних інформаційних систем;

– сприяння відновленню та адаптації механізму надання послуг у воєнний та післявоєнний час [347,348].

Ураховуючи все вищезазначене, можемо зробити висновок, що забезпечення кібербезпеки в медичному секторі потребує комплексних і системних рішень, які б поєднували передові технології, навчання персоналу, управлінські процедури та дотримання нормативних стандартів. Лише такий підхід дозволить ефективно захистити дані пацієнтів і забезпечити безперервність роботи медичних установ, зберігаючи їх репутацію й довіру пацієнтів. Цікаво, що більшість атак на медичні установи не є складними і базуються на використанні відомих вразливостей. Це свідчить про те, що

медичний сектор часто не готовий до сучасних загроз, що створює великі ризики для безпеки пацієнтів та їхніх даних. На нашу думку, ключова проблема полягає в недооцінці важливості кібербезпеки з боку медичних установ. Сектор охорони здоров'я є важливою мішенню через велику кількість цінних і конфіденційних даних, таких, як особиста інформація пацієнтів, історії захворювань та результати медичних тестів. Водночас використання застарілих технологій робить ці установи вразливими до простих атак, які могли бути знешкодженими за допомогою оновлення програмного забезпечення й використання сучасних систем захисту. Тому медичні заклади повинні переглянути свої підходи до безпеки. Система охорони здоров'я, яка тісно пов'язана з новими технологіями, повинна бути готовою до нових викликів та загроз. Зіткнувшись із реальністю кібератак, медичні установи повинні змінити свою культуру щодо безпеки, зробивши її пріоритетом у своїй діяльності. Тільки завдяки комплексному підходу можна досягти належного рівня захисту даних пацієнтів та забезпечити безперервність роботи ключових медичних систем.

Отже, можемо зазначити, що на сьогодні сектор охорони здоров'я посідає перше місце в списку хакерських цілей по всьому світу, і зокрема, в Україні. Цей факт викликає занепокоєння, адже кібербезпека системи охорони здоров'я є одним із найважливіших напрямів забезпечення кібербезпеки держави. Розуміючи значущість загроз, упроваджуючи надійний захист і формуючи культуру обізнаності про кіберзагрози, організації з охорони здоров'я можуть захистити дані пацієнтів і забезпечити безперервність якісного лікування. Завдяки колективним зусиллям можна дати можливість сектору охорони здоров'я безпечно функціонувати в цифрову епоху.

Переходячи до соціальних особливостей впровадження eHealth, варто відзначити, що цифровізація охорони здоров'я сприяє підвищенню рівня довіри до державних інституцій, оскільки громадяни отримують доступ до прозорих та ефективних медичних послуг. Однак держава має забезпечити, щоб ця довіра не була зруйнована внаслідок вразливостей системи. Підтримка високого рівня

кібербезпеки є запорукою того, що громадяни продовжать довіряти новим технологіям і користуватимуться їх перевагами.

Загалом вважаємо, що розвиток eHealth в Україні є важливим політичним інструментом модернізації системи охорони здоров'я. Однак забезпечення її кібербезпеки вимагає серйозного політичного підходу, що включає створення національної стратегії захисту, розвиток національних компетенцій і зменшення залежності від зовнішніх партнерів. Лише так можна досягти, щоб цифрова трансформація медичної галузі була не лише інноваційною, але й безпечною, сприяла загальному зміцненню національної безпеки України.

Тож можемо узагальнити, що Україна за досить короткий час у тяжких умовах воєнного стану розвинула систему електронної охорони здоров’я: проводяться проекти із вдосконалення системи, а також забезпечується розвиток партнерства з країнами ЄС та США. Ураховуючи високу розвиненість галузі в багатьох країнах ЄС, Україна намагається вживати усіх можливих заходів для покращення цієї системи, виведення її на високий рівень функціонування, переймаючи досвід передових європейських країн не тільки в організації системи електронної охорони здоров’я, а ще й забезпечуючи вирішення однієї із нагальних проблем, що виступає перешкодою для успішного функціонування системи, – її кібербезпеки.

Узагальнивши, подаємо ключові європейські національні ініціативи:

Табл.3.2

Досвід європейських національних ініціатив із забезпечення кібербезпеки eHealth в Україні (укладено автором за матеріалами [303])

КРАЇНА	ВАЖЛИВИЙ ДОСВІД
Естонія	1) децентралізована архітектура системи eHealth, розподілення функцій між різними серверами та вузлами для зменшення ризику масових збоїв або атак; 2) багаторівневий захист, уключаючи шифрування даних, регулярні оновлення та контроль доступу; 3) відстеження всіх входів у систему для контролю за доступом до даних.
Німеччина	1) посилена нормативно-правова база для забезпечення кібербезпеки в медичному секторі; 2) дотримання медичними установами та страховими компаніями стандартів захисту даних; 3) баланс між рівнем захисту і зручністю для медичного персоналу, щоб забезпечити швидку реакцію в критичних ситуаціях.
Данія	1) зміцнення спроможності місцевих органів влади та забезпечення їх необхідними ресурсами для ефективного надання медичних послуг; 2) розвиток національної електронної системи охорони здоров'я, забезпечення її інтероперабельності та захист даних пацієнтів; 3) активне залучення громадян до використання цифрових медичних послуг через освітні кампанії та підвищення цифрової грамотності.
Польща	1) комплексний підхід до кібербезпеки, де всі структури акумулюють зусилля без перетину повноважень; 2) швидкість прийняття рішень у питаннях суспільної та державної безпеки; 3) формація коаліції або партнерства для підвищення кібербезпеки в охороні здоров'я, уключаючи навчання та розподіл ресурсів.
Нідерланди	1) комплексний підхід, що включає технічні та організаційні заходи кібербезпеки; 2) належна правова база, зокрема розроблення та дотримання стандартів кібербезпеки й регулярні незалежні перевірки із виконання; 3) залучення пацієнтів та медичних працівників до розробки новітніх технологій для забезпечення безпеки та оптимізації лікувального процесу.
Франція	1) міцна політика та правові стандарти з кібербезпеки для охорони здоров'я; 2) високий рівень координації між державними інституціями та приватним сектором; 3) інтеграція цифрових технологій у медицину на всіх рівнях, акцент на конфіденційність та захист даних.

Продовження *Табл.3.2*

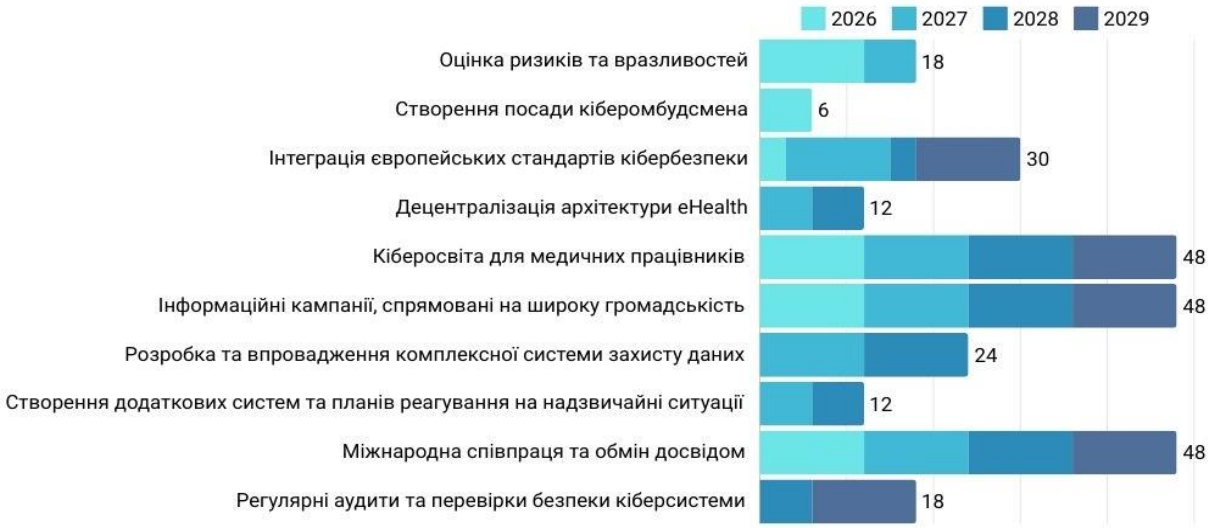
Велика Британія	1) всеосяжний та колаборативний підхід до кібербезпеки в охороні здоров'я; 2) національні стратегії з чіткими керівними принципами та координацією між установами; 3) регуляторні заходи для забезпечення того, щоб приватні компанії в медицині дотримувалися тих самих стандартів безпеки, що й державні установи.
Швеція	1) застосування цифровізації в медичній практиці та підвищення цифрової компетентності медичного персоналу; 2) безпечне управління інформацією та спільний розвиток цифрових трансформацій; 3) національна стратегія кібербезпеки для системи eHealth.

Україна перебуває на вирішальному етапі цифрової трансформації системи охорони здоров’я, яка відкриває нові можливості для покращення доступу до медичних послуг та підвищення ефективності управління інформацією. Однак цей перехід також має нові небезпеки, пов’язані з кіберпростором. З метою забезпечення стійкості системи eHealth до кібератак, необхідно впровадити комплексний підхід, що враховує як технічні, так і політичні аспекти кібербезпеки.

Нижче наведемо Вектор кіберстійкості eHealth, який згідно з нашим аналізом, допоможе Україні у зміцненні кібербезпеки системи електронної охорони здоров’я:

Рис.3.2.

Вектор кіберстійкості eHealth в Україні



Більш детально перераховані заходи подаємо в таблиці зі структурованою інформацією за кожним етапом, уключаючи опис заходів, терміни їх виконання, відповідальних осіб, необхідні ресурси та очікувані результати. Такий підхід сприятиме кращому сприйняттю та організації процесу виконання поставлених завдань.

Табл. 3.3.

Сутність елементів Вектору кіберстійкості eHealth

ЕЛЕМЕНТ	ПЕРІОД	СУТНІСТЬ
Оцінка ризиків та вразливостей	2026 – перше півріччя 2027 рр.	Проведення всебічного дослідження нинішніх загроз для кібербезпеки і виявлення недоліків системи eHealth. Цей аспект передбачає розпізнавання можливих варіантів порушення кібербезпеки, вивчення попередніх випадків атак на медичні системи та визначення ступеня вразливості технологічної інфраструктури, пов'язаної з медичною сферою. Зібрані дані допоможуть визначити основні проблеми та запропонувати рішення, які, як прогнозується, зменшать ризик кібертерористичних атак.

Продовження табл.3.3

Створення посади «кіберомбудсмен»	перше півріччя 2026 р.	Особливості діяльності увеї посади були з'ясовані в попередніх розділах. Серед його повноважень також має бути нагляд за впровадженням політики кібербезпеки та захист прав громадян у кіберпросторі, уключаючи охорони здоров'я. Кіберомбудсмен прийматиме скарги щодо захисту даних у медичних установах та перевірятиме дотримання правил забезпечення кібербезпеки. На нашу думку, результати такої діяльності посилять політичний нагляд і підвищать довіру громадян до цифрової медицини.
Інтеграція європейських стандартів безпеки	протягом 30 місяців з 2026 по 2028 рр.	Упровадження європейських стандартів кібербезпеки в систему eHealth, а саме: забезпечення конфіденційності даних, безпеки медичних пристроїв і нормативних актів, які забезпечать довгострокову життєздатність цифрової інфраструктури. Інтеграція стандартів гарантуватиме високий рівень кібербезпеки та сприятиме високому рівню взаємодії з європейською практикою.

Продовж. Табл. 3.3

Децентралізація архітектури eHealth	друге півріччя 2026 р. – перше півріччя 2027 р.	Таке впровадження означає, що різні сервери та вузли повинні розподіляти функції, що зменшить імовірність великої кількості збоїв або кібератак.
Кіберосвіта для медичних працівників	постійно	Уведення обов'язкового підвищенні кваліфікації для медичних працівників усіх ланок згідно з запропонованою Національною програмою кіберосвіти в Україні. Весь медичний штат, ураховуючи немедичних працівників медичної галузі, тобто супутніх фахівців, повинні розуміти, як зберігати інформацію про пацієнтів, реагувати на кібератаки та безпечно співпрацювати з електронними медичними записами.
Інформаційні кампанії для широкої громадськості	постійно	Допомога та інформування громадян про небезпеку кіберзлочинності та безпечне використання цифрової медичної допомоги. За нашим аналізом, це сприятиме довірі системі eHealth та формуватиме дисциплінованість у дотриманні належної поведінки в ситуації кібербезпеки.
Розробка та впровадження комплексної системи захисту даних	2027 – 2028 рр.	Розробка та прийняття багаторівневого підходу до захисту даних, який уключатиме шифрування, регулярні оновлення програмного забезпечення, використання таких технологій, як міжмережеві екрани, IDS/IPS та VPN, контроль доступу до системи й постійний моніторинг кіберзагроз, що також покликані забезпечити достатній захист і зменшити ймовірність порушення даних пацієнтів.
Створення додаткових систем та планів реагування на надзвичайні ситуації	друге півріччя 2028 р. – перше півріччя 2029 р.	Створення резервних системи, які забезпечуватимуть безперервну роботу медичних закладів у разі кіберзагроз, атак чи технічних збоїв. Логічно припустити, що такий план реагування на надзвичайні ситуації мінімізує наслідки нещасних випадків під час кібертерористичних атак і забезпечить доступність медичної допомоги в будь-якій ситуації.

Продовж. Табл. 3.3

Міжнародна співпраця та обмін досвідом	постійно	Участь у міжнародних ініціативах із кібербезпеки, пов'язаних з охороною здоров'я, таких як Глобальне партнерство з цифрової охорони здоров'я (GDHP), унесення пропозицій по реформуванню, обмін досвідом з іншими країнами, який сприятиме впровадженню передових методів кібербезпеки та розробці ефективних стратегій боротьби з кібертероризмом.
Регулярні аудити та перевірки безпеки кіберсистем	постійно, починаючи з другого півріччя 2028 р.	Проведення регулярних незалежних аудитів системи eHealth для оцінки ефективності заходів кібербезпеки та виявлення потенційних проблем. Подібна інспекція та контроль дозволять підтримувати постійний нагляд і посилювати заходи кібербезпеки.

Саме такі кроки, на нашу думку, сприятимуть активізації безпечної системи кібербезпеки eHealth в Україні та гарантуватимуть захищений обмін медичними даними між закладами охорони здоров'я, що суттєво підвищить ефективність медичних послуг. Це сприятиме створенню надійного кіберпростору в галузі охорони здоров'я, що мінімізуватиме ризики витоку конфіденційної інформації та гарантуватиме безпеку даних пацієнтів.

Запропонований Вектор кіберстійкості eHealth розрахований на період з 2026 по 2029 роки та поєднує в собі найкращі європейські практики, однак необхідним є також урахування політичних, соціальних та технічних аспектів кібербезпеки в Україні, що дозволить забезпечити комплексний підхід до захисту системи eHealth. Інтеграція стандартів, децентралізація архітектури, підвищення кіберграмотності, а також міжнародне співробітництво за комплексного підходу зможуть створити багаторівневу систему кібербезпеки, стійку до сучасних кіберзагроз. Такого роду підхід, на наш погляд, забезпечить захист конфіденційних даних, підвищить довіру громадян до цифрової

медицини й дасть змогу адаптувати систему eHealth до нових викликів, знижуючи ризики кібератак на медичні установи. У кінцевому підсумку це сприятиме зміцненню національної безпеки та підвищенню якості медичних послуг, надаваних населенню України.

ВИСНОВКИ ДО РОЗДІЛУ 3

Розглянувши соціально-політичну ситуацію в Україні, можемо зробити висновок, що гібридна війна порушує стан кібербезпеки держави. Оскільки серед сучасних видів кібератак ми виділили кібертероризм як найнебезпечнішу, важливим стало питання захисту критичної інфраструктури від таких атак.

Незважаючи на те що до критичної інфраструктури віднесено багато систем (енергетичну, фінансову, водопостачання, охорони здоров'я, державної безпеки, правопорядку, електронних систем, інформаційних послуг, цивільного захисту, урядування, дослідницької діяльності та ін.), указану проблему ми розглядаємо на прикладі двох із них – ядерної кібербезпеки та кібербезпеки системи eHealth. Указаний вибір пояснюємо кількома чинниками: по-перше, ці інфраструктури –найважливіші в життєдіяльності, а по-друге, обидві містять в собі додаткові стратегічні системи. Так, наприклад, ядерна безпека включає державну безпеку, правопорядок та захист населенння. Натомість eHealth є частиною охорони здоров'я, додатково поєднуючи цивільний захист населення, служби порятунку, інформаційні послуги, електронні комунікації, хімічну, фармацевтичну та наукову діяльність та впливає на їхнє функціонування.

Нинішня ситуація в Україні, зокрема після повномасштабного вторгнення, спричинила фундаментальну зміну безпекової ситуації в Європі.

Захоплення Запорізької АЕС російськими військовими формуваннями у 2022 та здійснення кібертерористичних атак на енергетичну інфраструктуру України, починаючи з 2014 р., показали надзвичайну вразливість такої інфраструктури до гібридних загроз, які поєднують як фізичні, так і кібератаки.

Ураховуючи вищезазначені чинники, уважаємо за доцільне реалізувати такі пропозиції:

1. Запропонована до впровадження підземна розгалужена система управління із декількома пунктами керування. Прогнозується, що вона втілюватиме захист об'єктів, використовуючи методику віддаленої «заморозки» контролю ворожими військами апаратного забезпечення станції. Такий методологічний підхід може здійснювати повний захист ядерних

установок у кібернетичних вимірах і може зменшити ймовірність несанкціонованого вторгнення та катастрофічних наслідків, що випливають з цього.

2. Спираючись на представлену Концепцію, украй важливо підкреслити встановлення термінології «ядерної кібербезпеки» та її закріплення в міжнародній правовій системі, оскільки це є стратегічно важливим не тільки для України, а й для Європи загалом. Це пояснюємо низкою принципових тенденцій, що визначають сучасні виклики національній та регіональній безпеці.

3. Зрештою, захист ядерної інфраструктури в сучасному суспільстві є не лише технічною, а й політичною необхідністю. Вона потребує об'єднання зусиль держав, міжнародних організацій, наукової спільноти. Лише за допомогою колективних дій та інноваційних методів можливо підтримувати безпеку критично важливих об’єктів перед обличчям останніх викликів, міжнародну безпеку та стабільність.

4. Охорона здоров’я – одна з найважливіших ланок критичної інфраструктури, тому забезпечення кібербезпеки в системі eHealth має неабияке значення. Проаналізувавши поточний стан кібербезпеки eHealth в Україні та порівнявши його з обраними країнами європейського регіону, ми розробили рекомендації для українського напрямку.

5. Рекомендуємо розробити законодавчу базу, яка б вичерпно розглядала аспекти кібербезпеки в системі електронної охорони здоров’я, правила та методи систем захисту в закладах охорони здоров’я. Ці положення рекомендовано включити до Законів «Про кібербезпеку» та «Основи законодавства України про охорону здоров'я»», що сприятиме підвищенню ефективності заходів щодо забезпечення кібербезпеки з охорони здоров’я.

6. Необхідним є перейняття досвіду європейських держав у захисті медичних систем від кібератак. Кожна з проаналізованих нами країн має свій власний унікальний приклад, механізм та особливості протистояння

кібератакам. Це допоможе Україні боротися із загрозою кібертероризму на вкрай важливу систему життєдіяльності суспільства.

7. Нами створено «Вектор кіберстійкості eHealth» для України щодо забезпечення кібербезпеки eHealth, яка показує деталізований опис кожної дії, які необхідно реалізувати Україні задля реформування і покращення у цьому напрямку. «Дорожня Карта» розрахована на період із 2026 по 2029 роки, що дає тим самим можливість у 2030 році показати успішні результати такої діяльності.

ВИСНОВКИ

1. Реалізовано всебічний аналіз поняття «кібертероризм», окреслено його елементи та обґрунтовано необхідність регулювання через європейське законодавство. Із урахуванням досвіду України було запропоновано загальноєвропейський стандарт боротьби з кібертероризмом. Такий підхід, на нашу думку, слугуватиме системності та координації дій різних держав як у запобіганні, так і в боротьбі з ним. Проаналізувавши різні підходи до розуміння кібертероризму, подаємо власне уточнене визначення цього поняття: кібертероризм – це свідоме використання інформаційно-комунікаційних технологій для здійснення нападів на критичні об’єкти інфраструктури з метою досягнення політичних або ідеологічних цілей, створення паніки серед населення чи підриву державної стабільності, суспільств і міжнародних структур через маніпуляцію інформаційними потоками, руйнацію цифрових інфраструктур або дестабілізацію стратегічних систем управління.

2. З’ясовано основні недоліки визначення поняття «кібербезпека», а також недоліки чинного українського законодавства щодо кваліфікації цього терміна. Визначення, як було доведено, має охоплювати соціально-економічні наслідки кіберзагроз і враховувати необхідність адаптації до нових проблем і викликів. Згідно з нашим розумінням, кібербезпека – це комплексний стратегічний процес гарантування безпеки національного суверенітету, політичної стабільності, критичної інфраструктури та забезпечення захисту інтересів прав і свобод громадян у кіберпросторі від деструктивного впливу будь-яких внутрішніх і зовнішніх кіберзагроз із використанням багаторівневих політико-правових, технічних та соціальних інструментів.

3. Розроблено рекомендації для вдосконалення національної політики кібербезпеки, зокрема висунуто пропозицію створення посади «кіберомбудсмена» як уповноваженого представника держави, діяльність якого полягатиме в захисті суспільних інтересів, прав та свобод громадян у цифровому просторі. Його додатковими функціями буде проведення перевірок

державних організацій щодо того, чи відповідають вони вимогам кібербезпеки, виявлення вразливості та рекомендації щодо їхнього усунення. Ця структурна одиниця зможе також брати участь у законодавчих ініціативах та національних стратегіях з кібербезпеки, де інтереси громадян були б належним чином враховані. На міждержавному рівні завдання кіберомбудсмена полягатиме в участі в міжнародних форумах і представництві України в питаннях громадської політики в цифровому середовищі.

4. Запропоновано до впровадження нові соціально-політичні концепції задля посилення рівня забезпечення кібербезпеки в Україні, зокрема «кіберсоціальну адаптацію» та формування «кіберімунітету» суспільства. Такі нові підходи забезпечать, на наш погляд, комплексний захист громадянських і національних інтересів у кіберпросторі. Специфіка «кіберімунітету» полягає у використанні політичних і соціальних інструментів для спільного створення «імунітету суспільства» до деструктивного впливу кібертероризму. «Кіберсоціальна адаптація» має на меті соціальну та культурну специфіки забезпечення кібербезпеки. Це зробить запроваджені заходи для зміцнення кібербезпеки більш ефективними й такими, що відповідатимуть моральним і правовим нормам, соціальним структурам і особистим відмінностям, що уможливить пристосування їх до конкретної соціальної основи.

5. Була вдосконалена міждисциплінарна методологія вивчення кібертероризму, що зумовлює необхідність уніфікації правових підходів та посилення міжнародного співробітництва. Рекомендації щодо подальших досліджень містять реалізацію запропонованих ідей, зокрема створення національних підрозділів кіберполіції, оновлення стратегій кібербезпеки та активного моніторингу критичної інфраструктури. Крім того, окреслені напрямки подальших досліджень щодо розроблення нових заходів протидії та здатності гармонізувати кіберполітику.

6. Рекомендовано ратифікувати новий Третій Додатковий Протокол до Будапештської Конвенції про Кіберзлочинність 2001 року. Зазначений протокол включатиме ідею кібертероризму, його характеристики,

криміналізацію та політичний інструментарій протидії йому. Серед них кіберімунітет для критичної інфраструктури», «політичний кіберкарантин», а також створення нових структур протидії з метою забезпечення «політичного механізму кіберпосередництва». Особливим механізмом запропоновано формування міжнародного суду у справах злочинів у кіберпросторі, «кібертрибуналу», який функціонує віддалено. Засобом протидії кібертероризму може стати зміцнення та розширення повноважень Міжнародного кримінального суду ООН та/або Міжнародного суду ООН у цій галузі.

7. Проаналізувавши досягнення щодо кіберзахисту в названих країнах європейського регіону, ми виділили ключові моменти, які необхідно включити до української системи захищеного кіберпростору. «Модель забезпечення кібербезпеки» містить такі чотири ключові компоненти: інтеграція + адаптація до загроз + інновації + кіберосвіта = кібербезпека. Така структура може в майбутньому стати основою для нових стратегій і політики кібербезпеки з тим, щоб створити «щит» у кіберпросторі та забезпечити стійкість до сучасних цифрових викликів в Україні.

8. Для забезпечення останнього складника з метою захисту в цифровому середовищі та підвищення обізнаності суспільства пропонуємо створити Національну програму кіберосвіти. Ідея цього проєкту виникла на тлі «кадрового голоду» через війну. Мобілізація до лав ЗСУ, вимушена еміграція спричинили брак працівників і в галузі кіберзахисту. Така програма, переконані, допоможе отримати кожному знання, необхідні для найбільш ефективної роботи в цифровому робочому середовищі. Вона розрахована на спеціалізовані напрямки професій, необхідних для забезпечення функціонування критичних об’єктів держави і матиме відповідні плани, сфокусовані на навчання медичних працівників, фінансистів та економістів, працівників енергетики, науковців, державних службовців і юристів. Програма допоможе кожній професійній групі отримати необхідні знання, що знадобляться для ефективної роботи в цифровому світі. Укладання навчальних

програм з кібербезпеки – комплексний процес, який поєднує базові технічні, юридичні та етичні питання, утілюючи як теоретичний, так і практичний досвід для успішного захисту кіберпростору.

9. Укладені рекомендації щодо реформування українського законодавства, оскільки з огляду на сучасні виклики та відповідно до оновлених стандартів і угод в міжнародній політиці доведена необхідність розширення Національної стратегії кібербезпеки України.

10. Сформульовано особливості трансформації нормативно-правової системи України, оскільки правове регулювання кібербезпеки залишається недостатньо ефективним. Це пояснюємо декількома причинами, по-перше, такі акти часто не враховують специфіки сучасних кібертерористичних загроз, а також діють розрізнено, а фрагментація законодавства створює значні перешкоди у формуванні цілісної державної політики з кібербезпеки. А по-друге, необхідно скасувати положення застарілих законодавчих актів або оновити окремі з них. Це дозволить значно спростити регулювання питань кібербезпеки та активізувати її розвиток в Україні. З політичного аспекту включення положень про кібербезпеку в більш структуроване законодавство є надзвичайно пріоритетним.

11. Обґрунтовано нагальність реформування CERT–UA з тим, щоб основна його функція полягала в координаційному забезпеченні державної політики з кіберзахисту, а розподіл компетенцій був галузевим через підгрупи з робочими назвами (CERT – HC – забезпечення кібербезпеки в галузі охорони здоров'я, CERT – NE – забезпечення кібербезпеки з енергетики, CERT – LR – забезпечення кібербезпеки щодо здійснення правопорядку, правосуддя, тримання під вартою, а також цивільного захисту населення та територій, CERT – ECI – який відповідатиме за кібербезпеку електронних комунікацій та інформаційних послуг тощо).

12. Ініційовано перетворення Антитерористичного Центру (на сьогодні його завдання це – боротьба з фізичними аспектами тероризму), на агенцією з єдиною системою реагування, яка об'єднає обидва аспекти безпеки

(фізичну та кібернетичну). Важливість інтеграції кібертероризму в діяльність Антитерористичного Центру в тому, що це перетворює Україну з переважно оборонною позицією на державу, яка активно формує політику міжнародної безпеки. Розширення функцій центру важливо пов’язати зі стратегічними цілями – членством України в Європейському Союзі та Північноатлантичному альянсі, оскільки Україна, маючи досвід боротьби з гібридними загрозами проти Росії, може надати унікальну інформацію, а також запропонувати методи захисту кіберпростору для тривалого стримування противника країнам – членам цих організацій, що стане вагомим аргументом на користь її інтеграції з цими структурами.

13. Презентовано новітню ідею створення підземної розгалуженої системи керування ядерними станціями з кількома пунктами управління. Для охорони об’єктів запропоновано застосовувати «заморожування» можливості використання апаратної техніки станції військами противника. Такий методологічний підхід може забезпечити «всебічний» захист ядерних установок у кібернетичних вимірах і може зменшити ймовірність несанкціонованого вторгнення та відповідних катастрофічних наслідків. Регулювати таку діяльність пропонуємо галузевому центру CERT – UA з робочою назвою CERT – NE (Група реагування на кіберзлочини України з ядерної енергетики).

14. Виявлено необхідність створення та особливості функціонування новітньої структури на кооперації МАГАТЕ й ENISA. Пропонуємо включити питання управління об'єктами критичної інфраструктури, зокрема атомними електростанціями, до порядку денного міжнародних організацій. Кожна з цих організацій має унікальні компетенції та можливості, які у сукупності здатні створити потужну міжнародну платформу для забезпечення надійного захисту. Синхронізація дій таких організацій сприятиме забезпеченню комплексної безпеки ядерних об'єктів і дасть змогу швидко й злагоджено реагувати на загрози завдяки координації дій обох організацій. Наголосимо, що Україна є найбільш прийнятною для розміщення головного офісу зведеної структури з

огляду на геополітичне розташування та значний досвід у протидії кібератакам будь-якої складності з боку держави-агресора.

15. Спираючись на представлену Концепцію, розроблено концепт «ядерної кібербезпеки», яка має бути закріплена в міжнародній системі правового регулювання міждержавних відносин, оскільки це є стратегічно важливим як для України, так і для країн європейського регіону. Нами сформульовано таке визначення «ядерної кібербезпеки, яку розуміємо як сукупність технічних, організаційних, правових та процедурних заходів, спрямованих на забезпечення захисту ядерних об'єктів, інформаційних систем та мереж управління від кібернетичних загроз і кібератак, з метою недопущення несанкціонованого втручання, яке може призвести до серйозних аварій, загрози навколишньому середовищу, життю і здоров'ю людей, а також порушенню міжнародної безпеки.

16. Проаналізовано поточний стан кібербезпеки eHealth в Україні. Уперше розроблено концепт «кібербезпека eHealth», сформульовано його робоче визначення: кібербезпека eHealth – це забезпечення організації своєчасних доступних та якісних медичних послуг під час використання кіберпростору, що гарантується шляхом виконання особливих вимог щодо захищеності життєво важливої інформації та даних пацієнта (історії хвороб, результати аналізів, діагнози та плани лікування), належної роботи медичних систем і обладнання, збереження безпеки й безперервності роботи в разі надзвичайних ситуацій та дотримання необхідних методів захисту від зовнішніх і внутрішніх кіберзагроз.

17. Доведена пріоритетність розроблення нормативної бази, яка б вичерпно розглядала аспекти кібербезпеки в системі електронної охорони здоров'я, правила та методи систем захисту в закладах охорони здоров'я. З огляду на це підкреслена необхідність введення цих положень до Законів України «Про кібербезпеку» та «Основи законодавства України про охорону здоров'я».

18. Ініційовано та розроблено «Дорожню карту» для України щодо забезпечення кібербезпеки eHealth до 2029 року, яка демонструє розлогий детальний опис кожної дії, яку необхідно реалізувати Україні в реформуванні та покращенні українського досвіду.

19. Сучасний кібертероризм набуває все більш вираженого політичного виміру, трансформуючись із суто технічного явища в потужний інструмент політичного впливу, складник якого виявляється передусім у його ефективності ведення гібридної війни та здійснення геополітичного тиску. Політичний характер кібертероризму особливо яскраво виявляється в його здатності впливати на міжнародні відносини та внутрішньополітичні процеси. Важливим політичним складником сучасного кібертероризму є його симбіоз із інформаційними війнами. Поєднання технічних атак із цілеспрямованими інформаційними кампаніями дозволяє одночасно підривати технологічну інфраструктуру і впливати на суспільну свідомість. Це створює комплексну загрозу для національної безпеки, яка з метою формування нових норм кібербезпеки на рівні міжнародного співробітництва потребує не лише технічних, а й політичних рішень. Україна, маючи унікальний досвід і розуміння природи сучасних загроз, може стати одним із центрів розроблення нової філософії кібербезпеки. Це є особливо актуальним в умовах створення нової архітектури європейської безпеки, де кіберпростір стає одним із ключових фронтів захисту демократичних цінностей.

20. Сучасні виклики кібертероризму потребують не лише актуальних рішень, а й постійного наукового пошуку, оскільки разом із технологіями та геополітичними конфліктами динаміка цифрових загроз еволюціонує. Проведене дослідження вказує на необхідність глибшого політологічного осмислення явища кібертероризму як нового виклику сучасній системі міжнародних відносин. Важливим напрямком має стати вивчення політичних механізмів адаптації державних інституцій до нових викликів. Особливо цікавим є питання балансу між централізацією управління в галузі безпеки та збереженням демократичного контролю. Міжнародний аспект проблеми

потребує переосмислення традиційних підходів до політики безпеки. Кібертероризм, будучи транснаціональним явищем, ставить під сумнів ефективність наявних міжнародних інституцій та механізмів колективної безпеки. У цьому контексті виникає потреба в новій політичній філософії міжнародної кібербезпеки, яка б поєднувала технічні аспекти захисту з політико-правовими механізмами співробітництва. Соціально-політичний вимір проблеми вказує на необхідність глибшого дослідження впливу кібертероризму на громадянське суспільство. Особливого значення набуває вивчення механізмів формування «кіберімунітету» як складової частини загальної політичної культури суспільства. Перспективним напрямком є також дослідження політичних аспектів міжнародної технологічної співпраці. Конкуренція технологічних стандартів, боротьба за цифровий суверенітет та питання регулювання глобальних цифрових платформ стають новими полями геополітичного протистояння, що потребує ретельного політичного аналізу. Отже, подальші дослідження мають сприяти формуванню нової політичної парадигми, яка б адекватно відповідала на виклики кібертероризму, зберігаючи при цьому фундаментальні цінності відкритого суспільства. Це передбачає синтез традиційних політологічних підходів із новітніми технологічними та соціальними реаліями цифрової епохи. Таким чином, подальші дослідження мають бути орієнтовані на поєднання теоретичних інновацій із практичними політичними рішеннями, що дозволить Україні не лише протистояти сучасним загрозам, а й стати активним творцем міжнародної системи кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Джексон П. Напади 11 вересня у США: Що сталося у цей день. *BBC News Україна*. URL: https://www.bbc.com/ukrainian/features-58463114 (date of access: 08.12.2021).
2. September 11, 2001 Terrorist attacks. *George W. Bush Library*. URL: https://www.georgewbushlibrary.gov/research/topic-guides/september-11-2001-terrorist-attacks (date of access: 14.12.2021).
3. Відключення електроенергії в Україні було хакерською атакою. *BBC News Україна*. URL: https://www.bbc.com/ukrainian/news-38585587 (date of access: 11.01.2022).
4. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA patriot act) : Act of 26.10.2001. 107–56. URL: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (date of access: 11.01.2022).
5. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19. № 2. С. 118–129.
6. Корченко О.Г., Бурячок В.Л., Гнатюк С.О. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. *Безпека інформації*. 2013. Т. 19. № 1. С. 40–45.
7. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва. НІСД. 2014. 192 с
8. Корченко О. Г, Паціра Є. В., Гнатюк С. О., Кінзерявий В. М., Казмірчук С. В. Ознаковий принцип формування класифікацій кібератак. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2010. Т. 4. Вип. 146. С. 184–193.
9. Filinovych, V., Sopilko, I., Prudnykova, O. V., Krupnova, A., & Smetanina, N.. Ensuring the functioning of cyberspace in Ukraine: Legal and technical aspects. Sapienza: International Journal of Interdisciplinary Studies. 2024. No5(3), e24055.

10. Корченко О. Г., Казмірчук С. В., Ахметов Б. Б. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія. Київ: ЦП «Компринт», 2017. 435 с.

11. Інформаційна кібербезпека: соціотехнічний аспект : підручник / В. Л. Бурячок та ін. Львів: «Магнолія 2006», 2018. 320 с.

12. Погорецький М.А., Шеломенцев В.П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави*. 2009. № 2. С. 77–81.

13. Denning D.E. Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U. S. House of Representatives. Georgetown University. Georgetown.2000.URL:https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm (date of access: 11.01.2022).

14. Weimann G. Cyberterrorism How Real Is the Threat?. Washington, DC : United states institute of peace. 2004. URL: https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm (date of access: 11.01.2022).

15. De La Vega María Graciela P.P. Ciberterrorismo: Un nuevo desafío para el Derecho Internacional Humanitario. URL: https://tesis.pucp.edu.pe/items/cfad812b-5208-489e-80a4-d0188cd687a8 (date of access: 16.01.2022).

16. Ogunlana S.O. Countering Expansion and Organization of Terrorism in Cyberspace. Walden University. 2018. URL: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=7358&context=dissertations (date of access: 16.02.2022).

17. Sridharan V. Cyber security in power systems. URL: https://repository.gatech.edu/handle/1853/43692 (date of access: 16.02.2022).

18. Lundström B. IT-säkerhet: Största IT-säkerhetshoten mot svenska företag och organisationer idag, samt kontemporära bekämpningsmetoder och verktyg mot dessa IT-säkerhetshot. DIVA. 2016.URL:https://umu.diva-

portal.org/smash/record.jsf?pid=diva2%3A936699&dswid=6717 (date of access: 06.03.2022).

19. Collin B. The Future of Cyberterrorism. *Crime & Justice International Journal*. 1997. Vol. 13 (2). P. 5–26.

20. Бодунова О. М. Історико-правові аспекти виникнення злочинності у сфері інформаційних технологій. *Аналітично-порівняльне правознавство*. 2023. № 1. С. 441–445.

21. Когут Ю. І. Кібертероризм (історія, цілі, об'єкти) : практичний посібник. Київ : Консалтингова компанія «СІДКОН», 2023. 304 с.

22. McGuinness D. *How a cyber attack transformed Estonia. BBC News.* URL: https://www.bbc.com/news/39655415 (date of access: 28.03.2022).

23. Губенко Д. Кібератаку на «Прикарпаттяобленерго» перевіряють у США. URL: https://www.dw.com/uk/після-кібератаки-на-прикарпаттяобленерго-в-сша-переглянуть-захист-енергомереж/a-18964517 (date of access: 28.03.2022).

24. Charvat J. P. I. A. G. Cyber Terrorism: A New Dimension in Battlespace. *Cryptology and Information Security Series. Volume 3: The Virtual Battlefield: Perspectives on Cyber Warfare*. 2009. P. 77–87.

25. Conway M. Cyberterrorism: Hype and Reality. Potomac Books, Inc. 2007. URL: https://doras.dcu.ie/501/1/cybert_hype_reality_2007.pdf (date of access: 11.04.2022).

26. Diorditsa I., Kateryn chuk K., Telestakova A., Kulak N., Nastiuk A. Cyberterrorism as a threat to the cyber security of Ukraine: *A discussion of theoretical aspects. Amazonia Investiga*. 2021. 10(40). P. 73–83. URL: doi: 10.34069/AI/2021.40.04.8 (date of access: 27.04.2022).

27. Clarke R. A. Knake R. Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins Publishers. 2012. 320 p.

28. Lewis J. A. Rethinking Cybersecurity: Strategy, Mass Effect, and States. CSIS. 2018. 46 p.

29. Schmid A. P. Handbook of terrorism prevention and preparedness. ICCT Press Publication. 2021. URL: https://icct.nl/handbook-terrorism-prevention-and-preparedness (date of access: 27.04.2022).

30. Про кіберзлочинність : Конвенція від 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 28.04.2022).

31. Буяджи С. А. Особливості правового регулювання боротьби із кіберзлочинністю у США. *Lex Portus*. 2017. № 2. С. 130–141.

32. Голод К. Інформаційна безпека США: Сучасний стан та уроки для України. *Збірник наукових праць. Геополітика України: історія і сучасність*. 2017. Вип. 2 (19). С. 91–107.

33. Code pénal - Légifrance. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/ (date of access: 29.04.2022).

34. Heimat B. D. I. U. F. *Mit unserem Gesetz zum Schutz kritischer Infrastrukturen machen wir Deutschland krisenfester! Bundesministerium Des Innern Und Für Heimat.* URL: https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2024/11/kabinett-kritis.html (date of access: 02.05.2022).

35. Зінченко О. І. Європейська регіональна система протидії кібертероризму: політичні, інституційні та правові механізми. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія Питання політології*. 2021. № 39. С. 118–122.

36. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 02 квіт. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 09.05.2022).

37. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 09.05.2022).

38. Про затвердження Правил антитерористичної безпеки : Постанова Кабінету Міністрів України від 15.10.2024 № 1172. URL: https://zakon.rada.gov.ua/laws/show/1172-2024-п#Text (дата звернення 11.12.2024).

39. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII (2024) (Україна). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення 11.11.2024).

40. Homburger Z. *The Necessity and Pitfall of Cybersecurity Capacity Building* for *Norm Development in Cyberspace*. *Global Society*. 2019. 33(2). P. 224–242. URL: doi: 10.1080/13600826.2019.1569502 (date of access: 14.10.2022).

41. Марченко О. Кібербезпека та захист інформації: аналіз впливу ризиків та загроз із використанням сучасних ефективних стратегій кіберзахисту. *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2023. № 3. С. 50–59. URL: doi: 10.32782/IT/2023-3-6 (дата звернення: 25.01.2024).

42. Лісовська Ю. П. Кібербезпека: ризики та заходи: навч. посібник. К.: Видавничий дім «Кондор», 2019. 272 с.

43. Андреєв В. І., Хорошко В. О., Чередниченко В. С., Шелест М. Є. Основи інформаційної безпеки. Київ: вид. ДУІКТ, 2009. 292 с.

44. Олійник О. В., Соснін О. В., Шиманський Л. Є. Політико-правові аспекти формування інформаційного суспільства. *Держава і право: Збірник наукових праць*. 2022. № 13. С. 534 – 541.

45. Курій Є. О. Методологія підвищення захищеності об'єктів критичної інфраструктури за рахунок перехресного впровадження стандартів аудиту з кібербезпеки : автореф. дис. … д-ра філософії зі спеціальності: 125. Львів, 2024. 20 с.

46. Давидюк А. В. Методи та засоби підвищення рівня кібербезпеки об’єктів критичної інфраструктури : автореф. дис. … д-ра філософії зі спеціальності: 125. Харків, 2023. 20 с.

47. Гончар С.Ф. Методологія оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури : дис. … доктора техн. наук. Харків. 2020, 319 с.
48. Землянко Г.А. Методи та засоби для забезпечення кібербезпеки системи багатофункційних флотів безпілотних апаратів в умовах комбінованих кібератак : автореф. дис. … д-ра філософії зі спеціальності: 125. Харків, 2024. 20 с.
49. Карпенко А.С. Методи та засоби забезпечення кібербезпеки глобально-розподілених реплікованих систем зберігання даних з контрольованою узгодженістю : автореф. дис. … д-ра філософії. Харків, 2024. 21 с.
50. Мамедова Е.А. Адміністративно-правові засади забезпечення кібербезпеки патрульної поліції в Україні : автореф. дис. … д-ра філософії: 081. Дніпро: НТУ «Дніпровська політехніка», 2024. 20 с.
51. Веселова Л.Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни :10.02.07. Одеса, 2021. 26 с.
52. Тарасюк А. В. Теоретико-правові основи забезпечення кібербезпеки України : автореф. дис. … д-ра юрид. наук: 12.00.07. Київ, 2021. 26 с.
53. Гавриляк В. Б. Державні механізми провадження кібербезпеки в Україні : автореф. дис. … д-ра філософії: 281. Харків, 2021. 18 с.
54. Котух Є. В. Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі : автореф. дис. … д-ра наук: 281. Запоріжжя, 2022. 26 с.
55. Станіславський Т. В. Механізми публічного управління забезпечення кібербезпеки в сучасних умовах : автореф. дис. … канд. наук: 281. Харків, 2020. 17 с.
56. Арсенович Л. А. Механізми формування та забезпечення функціонування системи підготовки фахівців у сфері кібербезпеки органів державної влади України : автореф. дис. … д-ра філософії: 281. Харків, 2021. 19 с.
57. Самойленко О. О. Теорія і методика підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища : автореф. дис. … д-ра пед. наук: 13.00.04. Кропивницький, 2021. 25 с.

58. Бистрова Б. В. Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США : автореф. дис. … канд. пед. наук.13.00.04. Київ, 2018. 22с.
59. Сунгурова С. Р. Інформаційна війна як засіб політичного насилля : дис. … д-ра філософії : 052. Київ, 2024. 19 с.
60. Младьонова А. Д. Інформаційна війна і політика безпеки: політико-правовий вимір : дис. … д-ра філософії: 052 .05. Харків, 2021. 18 с.
61. Таркін В. П. Інформаційні війни у сучасному політичному просторі як феномен XX-XXI ст. : дис. … д-ра філософії : 052. Одеса, 2024. 19 с.
62. Саган О. В. Протидія медіа-інформаційному тероризму як питання національної безпеки України : дис. … канд. політ. наук : 21.01.01. Київ, 2021. 20 с.
63. Жайворонок О. І. Організаційно-правові засади формування та реалізації публічної політики протидії інформаційному тероризму в Україні : дис. … д-ра філософії: Харків, 2021. 21 с.
64. Палій С. А. Формування та реалізація державної політики у сфері інформаційної безпеки у країнах ЄС: досвід для України : дис. … канд. наук з держ. упр. : 281. Харків, 2021. 19 с.
65. Копійка М. В. Політика інформаційної безпеки у сучасних міжнародних відносинах : дис. … д-ра філософії: 291. Київ, 2021. 19 с.
66. Фурсай О. В. Політика інформаційної безпеки Французької Республіки в умовах міжнародно-політичних трансформацій: дис. … д-ра філософії: 291. Київ, 2024. 20 с.
67. Cybersecurity. *ITU*. URL: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (date of access: 11.04.2023).
68. Білявська Ю. В. Використання бенчмаркінгу в операційному процесі туристичного підприємства. *Науковий вісник Полтавського університету економіки і торгівлі. Серія : Економічні науки*. Полтава. 2014. № 2. С. 78–84.
69. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України: аналітична доповідь. Київ : НІСД, 2011. 30 с.

70. Regulation - 2019/881 - EN - EUR-LEX. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj (date of access: 27.12.2024).
71. NIS Directive and national CSIRTs. *ENISA*. December 3, 2024. URL: https://www.enisa.europa.eu/publications/nis-directive-and-national-csirts (date of access: 27.12.2024).
72. National cyber security: framework manual / ed. by A. Klimburg. Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2012. 253 p.
73. Cyber Threats. *ENISA*. September 19, 2024. URL: https://www.enisa.europa.eu/topics/cyber-threats (date of access: 20.12.2023).
74. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). *Bundesamt Für Sicherheit in Der Informationstechnik*. URL: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html (date of access: 09.01.2024).
75. Loi de programmation militaire 2019-2025. Ministère Des Armées. (2022, September 27). URL: https://www.defense.gouv.fr/ministere/dossiers-evenementiels-thematiques-du-ministere-armees-anciens-combattants/loi-programmation-militaire (date of access: 15.01.2024).
76. Data Protection Act 2018:Act. URL:https://www.legislation.gov.uk/ukpga/2018/12/enacted/data.pdf (date of access: 23.01.2024).
77. L_2016194NL.01000101.XM July 19, 2016. URL: https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32016L1148&from=EN (date of access: 05.02.2024).
78. USTAWA z dnia 5 lipca 2018 r. o krajowymsystemiecyberbezpieczeństwa. *Kancelaria Sejmu*. URL:https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf (date of access: 15.02.2024).
79. Christou G. The collective securitisation of cyberspace in the European Union. *West European Politics*. 2018. Vol. чи no. 42(2). P. 278–301. URL: https://doi.org/10.1080/01402382.2018.1510195 (date of access: 27.02.2024).

80. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems: Protocol of 28.01.2003. 189.
81. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) : Protocol of 12.05.2022. 224.
82. Зінченко О. І. Європейська регіональна система протидії кібертероризму: політичні, інституційні та правові механізми. *Вісник ХНУ імені В. Н. Каразіна. Серія : Питання політології.* Харків. 2021. № 39. С. 118–122.
83. Decision No. 7/06 on the countering the use of the internet for terrorist purposes. (2006, December 6). OSCE. https://www.osce.org/mc/23078 (date of access:11.03.2024).
84. Cyber/ICT Security. *OSCE*. URL: https://www.osce.org/cyber-ict-security (date of access: 21.03.2024).
85. European Commission. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. *The European Union Agency for Network and Information Security (ENISA)*.2013. URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (date of access: 08.04.2024).
86. European Commission, he High Representative of the Union for Foreign Affairs and Security Policy (2020). The EU's Cybersecurity Strategy for the Digital Decade. Brussels.
87. Vaillant F. TV5Monde : une cyberattaque inquiétante. *TV5MONDE-Informations*.April 10,2015.URL:https://information.tv5monde.com/international/tv5monde-une-cyberattaque-inquietante-23138 (date of access: 11.04.2024).
88. Тартачний О. Російсько-українська кібервійна: Що та чому стає мішенню хакерів. *SPEKA.media*. 19 листопада, 2024. URL: https://speka.media/rosiisko-ukrayinska-kiberviina-shho-ta-comu-staje-misennyu-xakeriv-9xry6w (дата звернення: 12.12.2024).

89. Parlament – Cyber-Angriff auf den Bundestag. Die Nachrichten. URL: https://www.deutschlandfunk.de/parlament-cyber-angriff-auf-den-bundestag-100.html (date of access: 02.12.2024).

90. США також звинуватили у вірусі NotPetya Росію. *BBC News Україна*. February 16, 2018. URL: https://www.bbc.com/ukrainian/news-43082212 (дата звернення: 16.09.2024).

91. Вірус WannaCry пошкодив комп'ютери у 99 країнах світу. *BBC News Україна*. May 13, 2017. URL: https://www.bbc.com/ukrainian/features-39907984 (дата звернення 16.09.2024).

92. Parliament hit by "sustained" cyber-attack. *BBC News*. June 24, 2017. URL: https://www.bbc.com/news/uk-40394074 (date of access: 17.09.2024).

93. MacAskill E., Syal R. Cyber-attack on UK parliament: Russia is suspected culprit. *The Guardian*.November 27,2017.URL:https://www.theguardian.com/politics/2017/jun/25/cyber-attack-on-uk-parliament-russia-is-suspected-culprit (date of access: 17.09.2024).

94. Kamervragen (Aanhangsel) 2017-2018, nr. 1408 Overheid.nl>Officiële bekendmakingen. (2018, March 12). URL: https://zoek.officielebekendmakingen.nl/ah-tk-20172018-1408.html (date of access: 23.09.2024).

95. Novinky, and Miloslav Fišer. "Kybernetická kanonáda proti Česku pokračuje. Hackeři sestřelili web ČT24."Novinky.2022, April 28.URL:https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-kyberneticka-kanonada-proti-cesku-pokracuje-hackeri-sestrelili-web-ct24-40395336 (date of access: 26.09.2024).

96. Komenda, Panoška, Bulhart, Žofka, Májek, Bartůňková, Dušek, and Ministerstvo zdravotnictví ČR. n.d. *COVID-19: Onemocnění aktuálně MZČR*. URL: https://onemocneni-aktualne.mzcr.cz/covid-19 (date of access: 03.10.2024).

97. Nemocnice Na Rokycansku Po Útoku Hackerů Stále Nefunguje Naplno. *Novinky*. 2018. URL: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-nemocnice-na-

rokycansku-po-utoku-hackeru-stale-nefunguje-naplno-110427 (date of access: 07.10.2024).
98. Un ciberataque bloquea los ordenadores de 13 centros sanitarios en Cataluña. *The Objective*. October 7, 2022. URL: https://theobjective.com/espana/cataluna/2022-10-07/ciberataque-ordenadores-cataluna/ (date of access: 07.10.2024).
99. Sturm S. Darum sind vor allem öffentliche Einrichtungen Ziel von Cyberangriffen. *NoSpamProxy*. May 12, 2020. URL: https://www.nospamproxy.de/de/darum-sind-vor-allem-offentliche-einrichtungen-ziel-von-cyberangriffen/ (date of access: 07.10.2024).
100. Psychotherapie-Zentrum gehackt: Täter veröffentliche tausende Sitzungsprotokolle im Netz. *T-online*. October 28, 2020. URL: https://www.t-online.de/digital/aktuelles/id_88831176/psychotherapie-zentrum-gehackt-taeter-veroeffentliche-tausende-sitzungsprotokolle-im-netz.html (date of access: 07.10.2024).
101. European Cybercrime Centre – EC3. *Europol*. July 22, 2024. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (date of access: 15.10.2024).
102. Joint Cybercrime Action Taskforce (J-CAT). *Europol*. October 1, 2024. URL: https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce (date of access: 24.10.2024).
103. Directive - 2022/2555 - EN - EUR-LEX. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555 (date of access: 24.10.2024).
104. EUCC Certification Scheme. *European Union Cybersecurity Certification*. URL:https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en (date of access: 28.10.2024).
105. Regulation - 2016/679 - EN - gdpr - EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (date of access: 28.10.2024).
106. Nasadyuk A. Захист персональних даних: ризики і загрози нових правил. *PRAVO.UA*. May 21, 2024. URL: https://pravo.ua/zakhyst-personalnykh-danykh-ryzyky-i-zahrozy-novykh-pravyl/ (date of access: 29.10.2024).

107. European Data Protection Board. *EDPB* URL: https://www.edpb.europa.eu/edpb_en (date of access: 04.11.2024).

108. EU and NATO increase information sharing on cyber incidents. *EEAS*. URL: https://www.eeas.europa.eu/node/5253_en (date of access: 07.11.2024).

109. What is Hybrid CoE? *The European Centre of Excellence for Countering Hybrid Threats*. June 26, 2024. URL: https://www.hybridcoe.fi/who-what-and-how/ (date of access: 11.11.2024).

110. Ten countries launch Tallinn Mechanism for cyber assistance to Ukraine. *European Pravda*. December 20, 2023. URL: https://www.eurointegration.com.ua/eng/news/2023/12/20/7175933/ (date of access: 17.10.2024).

111. Tallinn mechanism. *Välisministeerium*. URL: https://vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy/tallinn-mechanism (date of access: 17.10.2024).

112. Талліннський механізм: Україна та міжнародні партнери започаткували новий інструмент співпраці у кіберпросторі. *Кабінет Міністрів України*. URL: https://www.kmu.gov.ua/news/tallinnskyi-mekhanizm-ukraina-ta-mizhnarodni-partnery-zapochatkuvaly-novyi-instrument-spivpratsi-u-kiberprostori (дата звернення:17.10.2024).

113. European Judicial Cybercrime Network (EJCN). *EU CyberNet*. November 1, 2023. URL: https://www.eucybernet.eu/project/european-judicial-cybercrime-network-ejcn/ (date of access: 12.11.2024).

114. European Judicial Cybercrime Network. *Eurojust*. URL: https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network (date of access: 28.11.2024).

115. EuroJust: European Union Agency for Criminal Justice Cooperation. Eurojust. URL: https://www.eurojust.europa.eu/ (date of access: 28.11.2024).

116. Зінченко О. І. Кіберпандемія XXI століття. *Міжнародний науковий журнал «Грааль науки»*. 2021. № 5. С. 71–72.

117. Küberjulgeoleku strateegia komisjon (2008). Küberjulgeoleku strateegia 2008 – 2013. Tallinn: Kaitseministeerium. 2008. URL:https://energiatalgud.ee/sites/default/files/images_sala/e/ea/Kaitseministeerium._Küberjulgeoleku_strateegia_2008_-_2013._Tallinn_2008.pdf (date of access: 09.09.2024).

118. About us. CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. URL: https://ccdcoe.org/about-us/ (date of access: 09.09.2024).

119. Locked shields. URL: https://ccdcoe.org/locked-shields/ (date of access: 09.09.2024).

120. Рада національної безпеки і оборони України. Українська делегація у статусі члена CCDCOE вперше взяла участь у засіданні Керівного комітету Центру. 2023. URL: https://www.rnbo.gov.ua/ua/Diialnist/6372.html (дата звернення 03.01.2024).

121. CCDCOE. Ukraine to be accepted as a Contributing Participant to NATO CCDCOE. Tallinn: Communications at NATO CCDCOE.URL:https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/ (date of access: 03.01.2024).

122. Ensuring the state's cyber security.Majandus Ja Kommunikatsiooniministeerium. URL:https://www.mkm.ee/en/e-state-and-connectivity/cyber-security/ensuring-states-cyber-security (date of access: 04.01.2024).

123. Avaleht RIA. https://ria.ee (date of access: 04.01.2024).

124. Zinchenko O. I. Cyber terrorism: History of Ukraine and current trends. Actual Issues of Modern Science. *European Scientific e-Journal*, 2024. P. 70–79. Ostrava: Tuculart Edition, European Institute for Innovation-Development. doi: 10.47451/soc2024-09-02

125. Ministry of Economic Affairs and Communication. Cyber Security Strategy 2014-2017. ENISA. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (date of access: 04.01.2024).

126. Webmedia. Küberturvalisuse seadus–Riigi teataja. 2018. URL: https://www.riigiteataja.ee/akt/122052018001 (date of access: 05.01.2024).

127. Webmedia. Isikuandmete kaitse seadus–Riigi Teataja. 2023, November 11. URL: https://www.riigiteataja.ee/akt/104012019011?leiaKehtiv (date of access: 14.11.2024).

128. Webmedia. Digitaalallkirja seadus–Riigi teataja. 2004, January 1. URL: https://www.riigiteataja.ee/akt/693656 (date of access: 14.11.2024).

129. Про електронний цифровий підпис. Закон України № 852-IV. 2018. URL: https://zakon.rada.gov.ua/laws/show/852-15#Text (дата звернення: 01.12.2023).

130. Про електронну ідентифікацію та електронні довірчі послуги. Закон України №2155-VIII. 2024. . URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення 20.12.2024).

131. Webmedia. Avaliku teabe seadus–Riigi Teataja. 2014, August 1. URL: https://www.riigiteataja.ee/akt/108072014009 (date of access: 14.11.2024).

132. Küberturvalisuse strateegia. 2019. website. URL: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf (date of access: 14.11.2024).

133. Riigi infosüsteemide osakond. (2020). Küberturvalisuse programm aastateks 2021-2024.

134. Cybersecurity in 2023: Estonia's year of advanced threats. e-Estonia. https://e-estonia.com/2023-estonia-advanced-cybersecurity-threats/

135. Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse strateegia 2024–2030. URL: https://www.mkm.ee/sites/default/files/documents/2024-07/Kyberturvalisuse%20strateegia%202024-2030_labivalt_IT_vaatlik_Eesti.pdf (date of access:16.12.2024).

136. Monitoring cyberspace and impeding incidents. RIA. URL: https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee (date of access: 28.11.2024).

137. Forsvarsministeriet. National strategi for cyber- og informationssikkerhed. København. 2014. URL: https://digst.dk/media/13813/national-strategi-for-cyber-og-informationssikkerhed-2015-2016.pdf (date of access:16.05.2024).

138. Regulering. Trafikstyrelsen. URL:https://www.trafikstyrelsen.dk/arbejdsomraader/cyber/regulering (date of access: 17.12.2024).

139. Civilstyrelsen. LOV nr 436 af 08/05/2018, Digitaliseringsministeriet. Retsinformation. 2018, May 9. URL: https://www.retsinformation.dk/eli/lta/2018/436 (date of access: 04.11.2024).

140. Datatilsynet (Denmark) URL: https://noyb.eu/en/project/dpa/datatilsynet-denmark (date of access: 04.11.2024).

141. Stratégie nationale en Matière de cybersécurité III. 2018. URL:https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-fr-.pdf (date of access: 11.11.2024).

142. Cyber – og informationssikkerhed, åbne data og etik. 2018.URL:https://ida.dk/media/1582/rapport_-_cyber-og_informationssikkerhed_aabne_data_og_etik_-_3_raad_fra_ida.pdf (date of access: 11.11.2024).

143. Key data privacy and Cybersecurity Laws Denmark Global Data Privacy and Cybersecurity Handbook Baker McKenzie Resource Hub. 2024, January. URL: https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/emea/denmark/topics/key-data-privacy-and-cybersecurity-laws (date of access: 11.11.2024).

144. Forsvarsministeriet. Forsvarsministeriet. 2024. URL: https://www.fmn.dk/ (date of access: 11.11.2024).

145. Rigspolitiet Politi. *Forside Politi*.URL:https://politi.dk/om-politiet/virksomheden/rigspolitiet (date of access: 21.11.2024).

146. Key data privacy and Cybersecurity Laws Denmark Global Data Privacy and Cybersecurity Handbook Baker McKenzie Resource Hub. 2024, Januar. URL: https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-

cybersecurity-handbook/emea/denmark/topics/key-data-privacy-and-cybersecurity-laws (date of access: 25.11.2024).

147. Digitaliseringsstyrelsen. (2021). National strategi for cyber- og informationssikkerhed 2022 - 2024.Copenhagen:Finansministeriet.URL: https://fm.dk/media/25359/national-strategi-for-cyber-og-informationssikkerhed_web-a.pdf (date of access: 11.11.2024).

148. DKCERT - Danish Computer Security Incident Response Team. DKCERT - Danish Computer Security Incident Response Team. URL: https://www.cert.dk/en (date of access: 11.11.2024).

149. NORDUnet. (2024, February 16). NORDUnet CERT - NORDUnet. URL: https://nordu.net/network-operations/cert/ (date of access: 14.02.2024).

150. SektorCERTSektorCERT. 2024, July 4. URL: https://sektorcert.dk/ (date of access: 10.09.2024).

151. Säkerhetsskyddslag(2018:585).Sveriges Riksdag. 2018, May.URL:https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-2018585_sfs-2018-585/ (date of access: 14.02.2024).

152. Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänsterSveriges Riksdag. 2018, June 20. URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174/ date of access: 14.02.2024).

153. Lag (2022:482) om elektronisk kommunikation. (2022, May 19). Sveriges Riksdag. URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482/ date of access: 14.02.2024).

154. NCSC. (2024, October 4). URL:https://sakerhetspolisen.se/verksamheten/cybersakerhet/ncsc.html date of access: 04.10.2024).

155. CERT-SE - Sveriges nationella CSIRT. URL: https://www.cert.se/ (date of access: 18.09.2023).

156. FM CERT. (n.d.). FIRST — Forum of Incident Response and Security Teams. URL: https://www.first.org/members/teams/fm_cert date of access: 18.09.2023).

157. BSIG - nichtamtliches Inhaltsverzeichnis. URL: https://www.gesetze-im-internet.de/bsig_2009/ date of access: 18.09.2023).

158. Solix Technologies, Inc. (2024, April 13). DSGVO-Compliance leicht gemacht Datenschutz-Compliance verbessern. URL: https://www.solix.com/de/solutions/gdpr/ (date of access: 18.09.2023).

159. BDSG - nichtamtliches Inhaltsverzeichnis. URL: https://www.gesetze-im-internet.de/bdsg_2018/ (date of access: 18.09.2023).

160. Cyber-Sicherheitsstrategie für Deutschland (2011). Berlin, Germany: Bundesministerium des Innern. URL: https://cyber-peace.org/wp-content/uploads/2013/05/DE_cyberSecurityStrategie.pdf (date of access: 18.09.2023).

161. Bundesamt für Sicherheit in der Informationstechnik. Bundesamt Für Sicherheit in Der Informationstechnik. URL:https://www.bsi.bund.de/DE/Home/home_node.html (date of access: 18.09.2023).

162. CERT-Bund. Bundesamt Für Sicherheit in Der Informationstechnik. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html (date of access: 18.09.2023).

163. Airbus Protect - Safety - Cybersecurity - Sustainability. (2024, October 10). Airbus Protect. URL: https://www.protect.airbus.com/ (date of access: 17.10.2024).

164. Trusted Introducer: Directory: BASF GCERT. (2022, November 21). URL: https://www.trusted-introducer.org/directory/teams/basf-gcert.html (date of access: 17.10.2024).

165. BFK edvconsulting GmbH - Startseite. URL: https://www.bfk.de/en_index.html (date of access: 17.10.2024).

166. Trusted Introducer : Directory : CERT BWI. (2024, January 10). URL: https://www.trusted-introducer.org/directory/teams/cert-bwi.html#teamdetails (date of access: 17.10.2024).

167. Nrw C. CERT NRW: Startseite. Landesbetrieb IT NRW. URL: https://www.cert.nrw.de/ (date of access: 17.10.2024).
168. SaxCert S.S.I.D. (2005, August 17). Startseite - SAX.CERT - sachsen.de. URL: https://www.cert.sachsen.de/ (date of access: 17.10.2024).
169. Trusted Introducer : Directory : Bayern-CERT (DE). (2022, July 15). URL: https://www.trusted-introducer.org/directory/teams/bayern-cert-de.html (date of access: 25.11.2024).
170. CERT der Bundesagentur für Arbeit Bundesagentur für Arbeit. URL: https://www.arbeitsagentur.de/cert (date of access: 25.11.2024).
171. CSIRT-ECB. FIRST — Forum of Incident Response and Security Teams. URL: https://www.first.org/members/teams/csirt-ecb (date of access: 25.11.2024).
172. GmbH, S. (n.d.). S-CERT - Kontaktdaten für Notfälle. Alle Rechte Liegen Beim Autor. URL: https://www.s-cert.de/ (date of access: 25.11.2024).
173. CERTBW. FIRST — Forum of Incident Response and Security Teams. URL: https://www.first.org/members/teams/certbw (date of access: 25.11.2024).
174. Stoltenberg H. (2016, November 23). Cyber-Sicherheitsstrategie 2016. Deutscher Bundestag. URL:https://www.bundestag.de/webarchiv/presse/hib/201611/481582-481582 (date of access: 11.12.2024).
175. Bundeskabinett. Cybersicherheitsstrategie für Deutschland 2021. Berlin,Germany : Bundesministerium des Innern, für Bau und Heimat. 2021.
176. Computer misuse act 1990. (1990). URL: Legislation.gov.uk. https://www.legislation.gov.uk/ukpga/1990/18/section/1/1991-02-01(date of access: 11.12.2024).
177. Data protection act 2018. (2018). Legislation.gov.uk. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents (date of access: 30.11.2024).
178. GDPR. (n.d.). IT Governance - Governance, Risk Management and Compliance for Information Technology. URL: https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation (date of access: 30.11.2024).

179. Cabinet Office (2009). Cyber Security Strategy of the United Kingdom. London : TSO. URL: https://www.gov.uk/government/publications/cyber-security-strategy-of-the-united-kingdom (date of access: 30.11.2023).

180. Cabinet Office, National security and intelligence (2011). The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. London. URL: https://www.gov.uk/government/publications/cyber-security-strategy (date of access: 30.11.2023).

181. Cabinet Office, National security and intelligence, HM Treasury (2021). National Cyber Security Strategy 2016 to 2021. URL: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (date of access: 30.11.2023).

182. National Cyber Strategy 2022 (HTML). (2022, December 15). GOV.UK. URL: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 (date of access: 01.12.2023).

183. National Cyber Security Centre - NCSC.GOV.UK. National Cyber Security Centre. URL: https://www.ncsc.gov.uk/ (date of access: 01.12.2023).

184. ICO. Information Commissioner's Office (ICO). URL: https://ico.org.uk/ (date of access: 01.12.2023).

185. Home. (2023, July 10). www.ofcom.org.uk. URL: https://www.ofcom.org.uk/ (date of access: 01.12.2023).

186. National Security and Defense Council of Ukraine. (2024, October 10). NCCC launches cooperation with the National Cyber Security Centre of the Netherlands to strengthen collective cyber resilience. URL: https://www.rnbo.gov.ua/en/Diialnist/7010.html (date of access: 11.10.2024).

187. Ministry of Security and Justice (2011). The National Cyber Security Strategy (NCSS). URL: https://cyberwar.nl/d/2011_Dutch-NCSS_cyber-security-strategy-uk_tcm92-379999.pdf (date of access: 01.12.2023).

188. Ministerie van Justitie en Veiligheid. (2024, October 14). Home - Cyber Security Raad. URL: https://www.cybersecurityraad.nl/ (date of access: 14.10.2024).

189. Ministerie van Defensie. (2023, January 16). Defence Cyber Command. Cyber Security Defensie.nl. URL: https://english.defensie.nl/topics/cyber-security/cyber-command (date of access: 16.01.2023).

190. Ministry of Security and Justice (2011). The National Cyber Security Strategy (NCSS) 2. URL: https://zoek.officielebekendmakingen.nl/blg-259104.pdf (date of access: 16.01.2023).

191. Ministerie van Justitie en Veiligheid. (2024, July 30). Nederlandse Cybersecurity Agenda geëvalueerd. Nieuwsbericht WODC - Wetenschappelijk Onderzoek- En Datacentrum. URL: https://www.wodc.nl/actueel/nieuws/2021/06/10/nederlandse-cybersecurity-agenda-geevalueerd (date of access: 02.09.2024).

192. Netherlands - Cybersecurity Strategy 2022-2028. (2024, July 29). Digital Skills and Jobs Platform. URL: https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/netherlands-cybersecurity-strategy-2022-2028 ((date of access: 02.09.2024).

193. Ministerie van Algemene Zaken. (2024, May 30). Defence White Paper 2022. Ministry of Defence Government.nl. URL: https://www.government.nl/ministries/ministry-of-defence/defense-white-paper-2022 (date of access: 30.05.2024).

194. wetten.nl - Regeling - Wet beveiliging netwerk- en informatiesystemen - BWBR0041515. (2024, October 1). URL: https://wetten.overheid.nl/BWBR0041515/2024-10-01 (date of access: 01.10.2024).

195. wetten.nl - Regeling - Wet digitale overheid - BWBR0048156. (2023, July 1). URL: https://wetten.overheid.nl/BWBR0048156/2023-07-01 (date of access:02.09.2024).

196. Van Den Bosch, W. S. P. (2024, July 30). New Draft Cybersecurity Act in the Netherlands: What you need to know. Passle. URL: https://biotalk.twobirds.com/post/102jexc/new-draft-cybersecurity-act-in-the-netherlands-what-you-need-to-know (date of access:03.09.2024).

197. Remijnse M. (2024, July 23). Implementing NIS2 directive: 'Cyberbeveiligingswet' • turing law. Turing Law. URL: https://www.turing.law/implementing-nis2-directive-cyberbeveiligingswet/ (date of access:03.09.2024).

198. Nationaal Cyber Security Centrum. (2024, December 3). Home - National Cyber Security Centre. URL: https://english.ncsc.nl/ (date of access: 03.12.2024).

199. Ensie (2014, June 6). Defensie Cyber Expertise Centrum opgericht. 10 Landmacht. URL: https://magazines.defensie.nl/landmacht/2014/05/artikel-cyber (date of access: 03.12.2024)

200. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2021, August 6). The AIVD: Who we are. About AIVD AIVD. URL: https://english.aivd.nl/about-aivd/the-aivd-who-we-are (date of access: 03.12.2024)

201. DCA . URL: https://dutch-cybersecurity-assembly.nl/ (date of access: 03.12.2024)

202. Douzet F. (2014) . Understanding Cyberspace with Geopolitics. Hérodote, 152-153(1), 3-21. URL: https://shs.cairn.info/journal-herodote-2014-1-page-3?lang=en. (date of access: 03.12.2024)Défense et sécurité des systèmes d'information Stratégie de la France (2011).

203. Agence Nationale de la Sécurité des Systèmes d'Information. URL: https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02- (date of access: 18.09.2024).

204. Défense et sécurité des systèmes d'information Stratégie de la France (2011). Agence Nationale de la Sécurité des Systèmes d'Information. URL: https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02- (date of access: 18.09.2024).

205. Stratégie Nationale En Matière De Cybersécurité II. Agence Nationale de la Sécurité des Systèmes d'Information. (2015). URL: https://cybersecurite.public.lu/dam-assets/fr/lu-ncss-2-fr-booklet.pdf (date of access: 18.09.2024).

206. La France et la cybersécurité. *France Diplomatie - Ministère de l'Europe et des Affaires étrangères*. URL: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-

la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/ (date of access: 19.09.2024).

207. Cybersécurité : renforcement par le Gouvernement de la protection des citoyens, des administrations et des entreprises. (n.d.). Ministère De L'Économie Des Finances Et De La Souveraineté Industrielle Et Numérique. https://www.economie.gouv.fr/cybersecurite-renforcement-gouvernement-protection-citoyens-administrations-entreprises (date of access: 19.09.2024)

208. CERT-FR – Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. URL: https://www.cert.ssi.gouv.fr/ (date of access: 18.09.2024).

209. Page d'accueil du ministère des Armées et des Anciens combattants. Ministère Des Armées Et Des Anciens Combattants. URL: https://www.defense.gouv.fr/ (date of access: 19.09.2024).

210. Le commandement de la cyberdéfense (COMCYBER). (2024, September 9). Commandement De La Cyberdéfense. URL: https://www.defense.gouv.fr/comcyber/commandement-cyberdefense-comcyber (date of access: 19.09.2024).

211. Cybersecurity strategy of the Republic of Poland. URL:https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Strategia_Cyberbezpieczeństwa_RP_w_języku_angielskim. (date of access:14.12.2024).

212. Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. (2009). *URL: https://www.iniejawna.pl/pomoce/przyc_pom/z_r_p_o_c.pdf* (date of access:14.12.2024).

213. Wrzosek, M. (n.d.). Cyberpolicy NASK - Polityka ochrony Cyberprzestrzeni RP. Cyberpolicy NASK. URL: https://cyberpolicy.nask.pl/polityka-ochrony-cyberprzestrzeni-rp/#:~:text=Polityka%20Ochrony%20Cyberprzestrzeni%20RP%20z,akceptowalnego%20poziomu%20bezpiecze%C5%84stwa%20cyberprzestrzeni%20pa%C5%84stwa (date of access:14.12.2024).

214. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej (2016). Warszawa: Ministerstwo Cyfryzacji. URL: https://www.gov.pl/attachment/6e104fd5-3e94-4489-b998-78f3ee39474d (date of access:14.12.2024).

215. Strategia cyberbezpieczeństwa przyjęta przez rząd - Ministerstwo Cyfryzacji - Portal Gov.pl. (2017, May 10). Ministerstwo Cyfryzacji. URL: https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-przyjeta-przez-rzad (date of access:14.12.2024).

216. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 - Ministerstwo Cyfryzacji - Portal Gov.pl. (2019, December 30). Ministerstwo Cyfryzacji. URL: https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 (date of access:15.12.2024).

217. Komputerowego, Z.R.N.I.B. CSIRT GOV. CSIRT GOV. URL:https://csirt.gov.pl/ (date of access:15.12.2024).

218. CERT Polska. URL: https://cert.pl/ (date of access:15.12.2024).

219. Sprawozdanie pełnomocnika rządu do spraw cyberbezpieczeństwa (2024). Warszawa : Ministerstwo Cyfryzacji.

220. NASK – Państwowy Instytut Badawczy. (2024, December 1). URL: https://nask.pl/ (date of access:15.12.2024).

221. Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2023 rok (2024). Warszawa: Ministerstwo Cyfryzacji. URL: https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni (date of access:15.12.2024).

222. International Telecommunication Union (2024). Global Cybersecurity Index (GCI). Geneva: Telecommunication Development Bureau. URL: https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx (date of access:15.12.2024).

223. NCSI : Ranking. (2023, 9 червня). URL: https://ncsi.ega.ee/ncsi-index/?archive=1 (date of access: 09.09.2024).

224. Про оборону України, Закон України № 1932-XII (2024) (Україна). URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 02.09.2024).
225. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України", Указ Президента України № 121/2021 (2021) (Україна). URL: https://zakon.rada.gov.ua/laws/show/121/2021#Text (дата звернення:16.09.2023).
226. Про боротьбу з тероризмом, Закон України № 638-IV (2023) (Україна). URL: https://zakon.rada.gov.ua/laws/show/638-15#Text (дата звернення:18.09.2023).
227. Про інформацію, Закон України № 2657-XII (2024) (Україна). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 03.10.2023).
228. Про доступ до публічної інформації, Закон України № 2939-VI (2023) (Україна). URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 05.10.2023).
229. Про електронні комунікації, Закон України № 1089-IX (2024) (Україна). URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 17.10.2023).
230. Про захист інформації в інформаційно-телекомунікаційних системах, Закон України № 80/94-ВР (2024) (Україна). URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 19.10.2023).
231. Про державну таємницю, Закон України № 3855-XII (2024) (Україна). URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 23.10.2023).
232. Про захист персональних даних, Закон України № 2297-VI (2024) (Україна). URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 31.10.2023).
233. Державна служба спеціального зв'язку та захисту інформації України. (2024, December 18). URL: https://cip.gov.ua/ua (дата звернення: 21.11.2023).
234. Рада національної безпеки і оборони України. Рада Національної Безпеки І Оборони України. URL: https://www.rnbo.gov.ua/ (дата звернення: 21.11.2023).

235. Головна сторінка : Служба безпеки України. SSU. URL: https://ssu.gov.ua/ (дата звернення: 21.11.2023).
236. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/ (дата звернення: 21.11.2023).
237. CERT-UA. cert.gov.ua. URL: https://cert.gov.ua/ (date of access:21.11.2023).
238. Укрінформ (2024, 3 вересня). У країна під час повномасштабної війни зазнала більш як 600 кібератак URL: https://www.ukrinform.ua/rubric-society/3901744-ukraina-pid-cas-povnomasstabnoi-vijni-zaznala-bils-ak-600-kiberatak.html (дата звернення: 05.09.2024).
239. SSU. Антитерористичний центр при СБУ. URL: https://ssu.gov.ua/antyterorystychnyi-tsentr-pry-ssu (дата звернення: 23.01.2024).
240. Про електронні документи та електронний документообіг, Закон України № 851-IV (2024) (Україна). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення:14.02.2024).
241. Про Державну службу спеціального зв'язку та захисту інформації України, Закон України № 3475-IV. (2024) (Україна). URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 18.02.2024).
242. Про правовий режим воєнного стану, Закон України № 389-VIII (2024) (Україна). URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 28.02.2024).
243. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, Постанова Кабінету Міністрів України № 518 (2022) (Україна). URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 03.03.2024).
244. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, Постанова Кабінету Міністрів України № 1176. (2020) (Україна). URL: https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text (дата звернення:11.03.2024).

245. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, Постанова Кабінету Міністрів України № 1295. (2022) (Україна). URL: https://zakon.rada.gov.ua/laws/show/1295-2020-п#Text (дата звернення:20.03.2024).

246. Про затвердження Положення про організаційно-технічну модель кіберзахисту, Постанова Кабінету Міністрів України № 1426. (2021) (Україна). URL: https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text (дата звернення: 24.03.2024).

247. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, Постанова Кабінету Міністрів України №299. (2023) (Україна). URL: https://zakon.rada.gov.ua/laws/show/299-2023-п#Text (дата звернення: 23.04.2024).

248. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, Постанова Кабінету Міністрів України № 497. (2023) (Україна). URL: https://zakon.rada.gov.ua/laws/show/497-2023-п#Text (дата звернення:17.05.2024).

249. Про вищу освіту, Закон України № 1556-VII. (2024) (Україна). URL: https://zakon.rada.gov.ua/laws/show/1556-18#Text (дата звернення: 24.05.2024).

250. Про прийняття за основу проекту Закону України про освіту дорослих, Постанова Верховної Ради України № 2874-IX. (2023) (України). URL: https://zakon.rada.gov.ua/laws/show/2874-20#Text (дата звернення: 20.05.2024).

251. Про Національну програму інформатизації, Закон України № 2807-IX. (2022) (Україна). URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення:30.05.2024).

252. Про критичну інфраструктуру, Закон України № 1882-IX. (2024) (Україна). URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення:12.10.2024).

253. Запорізька АЕС: захоплення окупантами, ядерний тероризм. (2022, 3 березня). URL: https://mvs.gov.ua/news/zaporizka-aes-zaxoplennia-okupantami-iadernii-terorizm (дата звернення:12.09.2024).

254. Kro (2023, January 17). Ukrainie pozostał rok. W przeciwnym wypadku nie uda się już uruchomić Zaporoskiej Elektrowni Jądrowej. www.money.pl. URL: https://www.money.pl/gospodarka/ukrainie-pozostal-rok-w-przeciwnym-wypadku-nie-uda-sie-juz-uruchomic-zaporoskiej-elektrowni-jadrowej-6856632575519648a.html (date of access:12.09.2024).

255. Bojanowicz R. (2024, August 18). Eskalacja zagrożeń nuklearnych w Zaporoskiej Elektrowni Atomowej. Grossi wzywa do powściągliwości. Forsal.pl. URL: https://forsal.pl/swiat/ukraina/artykuly/9577554,eskalacja-zagrozen-nuklearnych-w-zaporoskiej-elektrowni-atomowej-gros.html (date of access:12.09.2024).

256. Nowiński A. (2023, June 27). Co, jeśli elektrownia jądrowa w Zaporożu wybuchnie? Jasna opinia ekspertki. naTemat.pl. URL: https://natemat.pl/495614,co-jesli-elektrownia-jadrowa-w-zaporozu-wybuchnie-ekspertka-tlumaczy (date of access:12.09.2024).

257. Osteuropa Z. (2023, August 15). Das Kernkraftwerk Zaporiżžja Zeitschrift OSTEUROPA. Zeitschrift OSTEUROPA. URL: https://zeitschrift-osteuropa.de/blog/das-kernkraftwerk-zaporizzja/ (date of access:12.09.2024).

258. Atomkraftwerke in der Ukraine. (2024, February 20). Bundesamt Für Die Sicherheit Der Nuklearen Entsorgung. URL: https://www.base.bund.de/de/nukleare-sicherheit/internationales/informationen-ukraine/ukraine-akw_inhalt.html (date of access:12.09.2024).

259. Mayer N. (2023, July 7). La centrale nucléaire de Zaporijia pourrait-elle « exploser » et quelles seraient les conséquences ? Futura. URL: https://www.futura-sciences.com/planete/actualites/environnement-centrale-nucleaire-zaporijia-pourrait-elle-exploser-seraient-consequences-97124/ (date of access:12.09.2024).

260. Dell'Anna, A. (2024, April 16). La centrale de Zaporijjia n'explosera probablement pas, mais l'Europe reste sur ses gardes. Euronews. URL:

https://fr.euronews.com/my-europe/2024/04/16/la-centrale-de-zaporijjia-nexplosera-probablement-pas-mais-leurope-reste-sur-ses-gardes (date of access:12.09.2024).

261. Think Tank reports on Russia's war of aggression against Ukraine. (2024, November 13). Consilium. URL: https://www.consilium.europa.eu/en/documents-publications/library/library-blog/posts/think-tank-reports-on-russia-s-war-of-aggression-against-ukraine/ (date of access:13.11.2024).

262. Prospect of nuclear accident 'Dangerously close' at Zaporizhzhia power plant in Ukraine, International Atomic Energy Agency chief warns Security Council Meetings coverage and press releases. (2024, April 15). URL: https://press.un.org/en/2024/sc15662.doc.htm (date of access:12.09.2024).

263. Explosionen auf der Krim - Gezielter Angriff aus der Ukraine? (2022, August14). URL: https://www.merkur.de/politik/militaer-ticker-ukraine-news-krieg-russland-zr-91717005.html (date of access:12.09.2024).

264. Zaporizhzhia - Rapport de l'AIEA : quels sont les risques liés à la centrale nucléaire en Ukraine occupée par la Russie ? BBC News Afrique. (2022, September 8). URL:https://www.bbc.com/afrique/monde-62821675 (date of access:12.09.2024).

265. Зінченко О. І. (2024). Кібертероризм в енергетичному секторі України та забезпечення кібербезпеки. *Кібербезпека енергетики : Матеріали науково-практ. конф.,* Київ, 52–55.

266. International Atomic Energy Agency (IAEA). Official web site of the IAEA. URL: https://www.iaea.org/ (date of access: 21.10.2024).

267. Анна (2024, 6 вересня). Що таке шифрування і як воно працює- IT News. IT News. URL: https://it-news.com.ua/statti/shyfruvannia-yak-zakhystyty-svoi-dani-u-tsyfrovu-epokhu.html (дата звернення: 21.10.2024).

268. Zero Trust: багаторівнева модель безпеки для сучасного бізнесу - Cloud. (2022, 18 травня). Cloud. URL: https://cloud.smart-it.com/news-post/zero-trust-bagatorivneva-model-bezpeky-dlya-suchasnogo-biznesu/ (date of access: 21.10.2024).

269. Back in BlackEnergy: 2014 targeted attacks in Ukraine and Poland. (2014, September 22). URL: https://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/ (date of access: 21.10.2024).

270. УНІАН (2016, 12 січня). УНІАН редакція. УНІАН. URL: https://www.unian.ua/society/1234268-eksperti-rozpovili-yaku-tehnologiyu-vikoristovuvali-hakeri-pri-napadi-na-ukrajinski-oblenergo-ta-zmi.html (дата звернення: 26.12.2024).

271. Червоненко В. (2016, 6 січня). Чи була кібератака на обленерго? BBC News Україна. URL:https://www.bbc.com/ukrainian/society/2016/01/160106_cyber_attacks_electricity_ukraine_vc (дата звернення: 26.12.2024).

272. Vukmanovic P. O., Jewkes S. (2017, January 18). Ukraine's power outage was a cyber attack - Ukrenergo. Reuters. URL: https://www.reuters.com/article/world/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BB/ (date of access: 26.12.2024).

273. Війна Росії проти України: хронологія кібератак. Європ. Союз, 2022. URL:https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf (дата звернення: 26.12.2024).

274. Аналітичний звіт Держспецзв'язку за результатами дослідження загроз, 2023. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=60201 (дата звернення: 26.12.2024).

275. Кіберзахист енергосектору: у 2022 році заблоковано понад 1,5 млн спроб атакувати галузь Міністерство енергетики України. (2023, 30 червня). URL: https://www.mev.gov.ua/novyna/kiberzakhyst-enerhosektoru-u-2022-rotsi-zablokovano-ponad-15-mln-sprob-atakuvaty-haluz (дата звернення: 04.11.2024).

276. Правда Е. (2024, 4 листопада). Кількість кібератак у 2023 році зросла на 16% – Держспецзв'язку. Економічна Правда. URL: https://epravda.com.ua/news/2024/01/31/709355 (дата звернення: 04.11.2024).

277. Паталяк Є. (2024, 17 вересня). Захист критичної інфраструктури. Wezom. URL: https://wezom.com.ua/ua/blog/zahist-kritichnoyi-infrastrukturi (дата звернення:17.09.2024).

278. Polska energetyka wystawiona na ataki hakerskie. (2022, 10 Marzec). elektro.info. URL: https://www.elektro.info.pl/artykul/najnowsze/185359,polska-energetyka-wystawiona-na-ataki-hakerskie (date of access: 08.05.2024).

279. Co zrobić, aby polska energetyka była cyberbezpieczna? (2023, Listopada 14). URL: https://www.energetyka-rozproszona.pl/artykuly/co-zrobic-aby-polska-energetyka-byla-cyberbezpieczna/ (date of access: 08.05.2024).

280. Cordis C. (2023, July 21). Czy hakerzy naprawdę mogą wyłączyć sieć energetyczną? CORDIS European Commission. URL: https://cordis.europa.eu/article/id/444373-could-hackers-really-take-down-the-power-grid/pl (date of access: 08.05.2024).

281. Kaleta N. (2024, May 13). Cyberataki w 2023 roku w Polsce i na świecie. Simplicity. URL: https://simplicity-poland.pl/blog/polska-i-swiat-w-2023-roku-najgrozniejsze-cyberataki/(date of access: 28.05.2024).

282. SWRWissen. (2024, December 10). Wie sicher sind erneuerbare Energien vor Hackern? SWR. URL: https://www.swr.de/wissen/cybergefahr-bei-erneuerbaren-energien-durch-hacker-100.html (date of access: 28.05.2024).

283. Kondruss B. (2024, March 17). Bedeutende Cyberangriffe auf die Energiewirtschaft 2023. KonBriefing Research. URL: https://konbriefing.com/de-topics/cyber-angriffe-2023-ind-energiewirtschaft.html#Res370841 (date of access: 28.05.2024).

284. Sektor CERT (2023). The attack against Danish, CLEAR critical infrastructure.

285. Mäder L. (2023, November 14). Cyberangriff auf Dänemark: Spur führt nach Russland. Neue Zürcher Zeitung. URL: https://www.nzz.ch/technologie/mehrere-hackerangriffen-nahmen-die-energieversorgung-daenemarks-ins-visier-eine-spur-fuehrt-nach-russland-ld.1765449 (date of access: 28.05.2024).

286. Reuters (2023, June 27). Siemens and UCLA say data compromised in MOVEit data breach. Reuters. URL: https://www.reuters.com/technology/siemens-energy-no-critical-data-was-compromised-after-moveit-data-breach-2023-06-27/ (date of access: 28.05.2024).

287. Egon N. (2023, August 30). Cyberattaque à Engie : fuite des données de milliers de clients. Economie Matin. URL: https://www.economiematin.fr/engie-les-donnees-de-110-000-clients-ont-fuite-a-cause-dune-cyberattaque (date of access: 28.05.2024).

288. Redactie. (2023, December 7). Aqualectra herstelt na cyberaanval - Curacao.nu. Curacao.nu. URL: https://curacao.nu/aqualectra-herstelt-na-cyberaanval/ (date of access:19.09.2024).

289. Eckstein P., Hr A. J. (2024, August 13). Cyberangriffe aus dem Ausland 2023 stark gestiegen. tagesschau.de. URL: https://www.tagesschau.de/inland/cyberangriffe-anstieg-bka-100.html (date of access: 02.09.2024).

290. Про внесення змін до деяких законодавчих актів України щодо вдосконалення системи управління сферою охорони здоров'я та забезпечення медичного обслуговування населення, Закон України № 1962-IX (2021) (Україна). URL: https://zakon.rada.gov.ua/laws/show/1962-20#Text (дата звернення:19.09.2024).

291. Е-здоров'я. *Міністерство Охорони Здоров'я*. URL: https://moz.gov.ua/uk/news/ehealth (дата звернення: 19.09.2024).

292. The Global Digital Health Partnership (GDHP). (2024, December 9). Global Digital Health Partnership. Global Digital Health Partnership. URL: https://gdhp.health/ (date of access: 23.12.2024).

293. Україна приєдналась до Глобального цифрового партнерства у сфері охорони здоров’я. (2018, 7 вересня). URL: https://moz.gov.ua/uk/ukraina-priednalas-do-globalnogo-cifrovogo-partnerstva-u-sferi-ohoroni-zdorovja (дата звернення:19.09.2024).

294. Cybersecurity Workstream (2024). Guidance for Medical Device Cybersecurity (GMDC). GDHP. URL: https://gdhp.health/wp-content/uploads/2024/10/GDHP-Guidance-for-Medical-Device-Cybersecurity_final.pdf (date of access: 30.09.2024).

295. Europe 2020 – for a healthier EU. (n.d.). Public Health. URL: https://health.ec.europa.eu/other-pages/basic-page/europe-2020-healthier-eu_en (date of access: 30.09.2024).

296. Electronic cross-border health services. (2024, April 24). Public Health. URL: https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en (date of access: 30.09.2024).

297. Publications Office of the European Union. (2024). 2024 digital decade ehealth indicator study : final report. Publications Office of the EU. URL: https://op.europa.eu/en/publication-detail/-/publication/c04f6162-3833-11ef-b441-01aa75ed71a1/language-en (date of access: 30.09.2024).

298. EU4Health programme 2021-2027 – a vision for a healthier European Union. (2024, September 20). Public Health. URL: https://health.ec.europa.eu/funding/eu4health-programme-2021-2027-vision-healthier-european-union_en (date of access: 30.09.2024).

299. Checking-up on Health: Ransomware accounts for 54% of cybersecurity threats ENISA. (2023, July 5). URL: https://www.enisa.europa.eu/news/checking-up-on-health-ransomware-accounts-for-54-of-cybersecurity-threats (date of access: 30.09.2024).

300. EuroHealthNet. (2024, August 27). Improving health equity in Europe: priorities for the 2024-2029 policy landscape - EuroHealthNet. URL: https://eurohealthnet.eu/improving-health-equity-in-europe-priorities-for-the-2024-2029-policy-landscape/ (date of access: 30.09.2024).

301. Cyber Risk GmbH. (n.d.). The European Health Data Space (EHDS). URL: https://www.european-health-data-space.com/ (date of access: 30.09.2024).

302. EHealth Security Experts Group. (n.d.). Resilience and CIIP Portal. URL: https://resilience.enisa.europa.eu/ehealth-security (date of access: 30.09.2024).

303. Parfonova I., Zinchenko O. Cybersecurity enchasement in the field of eHealth system development in Ukraine. Медичні Перспективи. 2024. Vol. 29, no. 4. P. 247–256.

304. EHealth Security. URL: https://www.ehealthgroup.ch/ehealth-security ((date of access: 09.10.2024).
305. Andero (2023, April 6). Estonia and Sweden to join forces to drive innovation in healthcare. Invest in Estonia. URL: https://investinestonia.com/estonia-and-sweden-to-join-forces-to-drive-innovation-in-healthcare/ (date of access: 09.10.2024).
306. Zhou W. You can change the system: How Estonia has built the most advanced eHealth system in the world – Memotext. URL: https://www.memotext.com/you-can-change-the-system-how-estonia-has-built-the-most-advanced-ehealth-system-in-the-world (date of access: 09.10.2024).
307. Nath B. (2022, December 26). Woman died after a ransomware attack encrypted hospital services. techdator. URL: https://techdatoral.pages.dev/posts/woman-died-after-a-ransomware-attack-encrypted-hospital-services/ (date of access: 09.10.2024).
308. Eddy M., Perlroth N. (2020, September 19). Cyber attack suspected in German woman's death. The New York Times. URL: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html (date of access: 09.10.2024).
309. Ralston W. (2020, November 11). The untold story of a cyberattack, a hospital and a dying woman. WIRED. URL: https://www.wired.com/story/ransomware-hospital-death-germany/ (date of access: 09.10.2024).
310. Cybersikkerhed og kompetencer i fokus i nyt projekt. (2024, February 19). VPT. URL: https://vpt.dk/administration/cybersikkerhed-og-kompetencer-i-fokus-i-nyt-projekt (date of access: 09.10.2024).
311. Sikorska M. (2024, June 4). 5 najgroźniejszych ataków ransomware w Polsce. Czy Twoja firma na pewno jest bezpieczna? Grandmetric: Network & Security. URL: https://www.grandmetric.com/pl/5-najgrozniejszych-atakow-ransomware-w-polsce/ (date of access: 09.10.2024).
312. Okręgowa Izba Lekarska w Warszawie - OIL WWA. URL: https://izba-lekarska.pl/ (date of access: 09.10.2024).

313. Stahie S. (2023, February 2). Killnet Attacks European Hospitals, including UMCG in the Netherlands. Hot For Security. URL: https://www.bitdefender.com/en-us/blog/hotforsecurity/killnet-attacks-european-hospitals-including-umcg-in-the-netherlands (date of access: 09.10.2024).

314. Ministerie van Volksgezondheid, Welzijn en Sport. (2021, November 2). Services and institutions. Ministry of Health, Welfare and Sport Government.nl. URL: https://www.government.nl/ministries/ministry-of-health-welfare-and-sport/services-and-institutions (date of access: 09.10.2024).

315. Le Dossier Médical Partagé (DMP) en pratique. (2024, November 25). URL: https://www.ameli.fr/medecin/sante-prevention/dmp-et-mon-espace-sante/dossier-medical-partage/dmp-en-pratique (date of access: 14.10.2024).

316. Agence du Numérique en Santé. (n.d.). La transformation numérique de notre système de santé commence ici, pour vous et avec vous ! Agence Du Numérique En Santé. URL: https://esante.gouv.fr/ (date of access: 14.10.2024).

317. Kerkour T. (2022). "Les cyberattaques contre les établissements de santé ont doublé en 2021." Le Figaro. URL: https://www.lefigaro.fr/secteur/high-tech/les-cyberattaques-contre-les-etablissements-de-sante-ont-double-en-2021-20220215 (date of access: 14.10.2024).

318. Afp Le P. A. (2021). "Cyberattaque à l'hôpital de Dax : reprise «très progressive», «aucune rançon» payée." leparisien.fr. URL: https://www.leparisien.fr/faits-divers/cyberattaque-a-lhopital-de-dax-reprise-tres-progressive-aucune-rancon-payee-11-02-2021-KICTQBN3D5GNNJS6GRFAVZMCKU.php. (date of access: 14.10.2024).

319. Echos L. (2022). "L'hôpital de Versailles victime d'une cyberattaque." Les Echos. URL: https://www.lesechos.fr/pme-regions/ile-de-france/lhopital-de-versailles-victime-dune-cyberattaque-1885808#:~:text=L'%C3%A9tablissement%20hospitalier%20de%20%20Versailles%2C%20dans%20les%20Yvelines%2C%20est,le%20coup%20de%20cette%20cyberattaque (date of access: 14.10.2024).

320. “Victime d’une attaque informatique, l’hôpital de Villefranche-sur-Saône contraint de déprogrammer des opérations.”. (2021). leparisien.fr, URL: https://www.leparisien.fr/faits-divers/rhone-lhopital-de-villefranche-victime-dune-attaque-informatique-15-02-2021-ZNCTT6EKABCLLMLHK26VHSTNK4.php. (date of access: 14.10.2024).

321. Portail-Ie. (2023, April 17). Retour sur les grandes cyberattaques en France en 2022 : quelles résolutions pour 2023 ? Portail De L’IE. URL: https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2023/retour-sur-les-grandes-cyberattaques-en-france-en-2022-quelles-resolutions-pour-2023/ (date of access: 14.10.2024).

322. French Healthcare. (2023, September 15). Expertise française E-Santé - Expertise French Healthcare. URL: https://frenchhealthcare.fr/expertises/e-health/ (date of access: 14.10.2024).

323. Agence du Numérique en Santé. (2023, December 6). Lancement de la Feuille de route du numérique en santé 2023-2027. Agence Du Numérique En Santé. URL: https://esante.gouv.fr/actualites/lancement-de-la-feuille-de-route-du-numerique-en-sante-2023-2027 (date of access: 25.09.2024).

324. Whitehouse, Giest, Dumortier, Artmann. (2010). eHealth Strategies: Country Brief: Wales. E-book. European Commission.

325. NSW Government. (2016). eHealth Strategy for NSW Health 2016-2026: A digitally enabled and integrated health system delivering patient-centred health experiences and quality health outcomes. E-book.NSW Government.

326. The Scottish Government. (2023, February 24). Health and social care: data strategy. URL: https://www.gov.scot/publications/data-strategy-health-social-care-2/ (date of access:12.09.2024).

327. HSC. (2022). Cyber Security Strategy HSC Northern Ireland 2022-2026.E-book.

328. Healthcare UK. (2019). DigitalHealth.

329. Palmer D. (2021, May 14). Ransomware: How the NHS learned the lessons of WannaCry to protect hospitals from attack. ZDNET. URL:

https://www.zdnet.com/article/ransomware-how-the-nhs-learned-the-lessons-of-wannacry-to-protect-hospitals-from-attack/ (date of access:12.09.2024).

330. Collier R. (2017). NHS ransomware attack spreads worldwide. URL: CMAJ. 5, 189(22):E786-E787. doi: 10.1503/cmaj.1095434 (date of access:16.09.2024).

331. Smart W. (2018). Lessons Learned Review of the WannaCryRansomware Cyber Attack. E-book.GOV.UK.

332. British hospital group declares ‘major incident’ following cyberattack. (2024, November 26). The Record From Recorded Future News. URL: https://therecord.media/england-hospitals-cyberattack-nhs-wirral (date of access: 03.09.2024).

333. Arishti Info Labs. (2022, May 1). Ransomware attack on Irish healthcare system. Blog. URL: https://arishti.com/blog/ransomware-attack-on-irish-healthcare-system (date of access: 03.09.2024).

334. Cyber security strategy for health and adult social care to 2030 - NHS England Digital. (2023, August 1). NHS England Digital. URL: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/cyber-security-strategy-for-health-and-adult-social-care-to-2030 (date of access: 07.09.2024).

335. E-hälsa. (2023, December 15). Socialstyrelsen. URL: https://www.socialstyrelsen.se/kunskapsstod-och-regler/omraden/e-halsa/ (date of access: 03.09.2024).

336. Про схвалення Концепції реформи фінансування системи охорони здоров'я, Розпорядження Кабінету Міністрів України № 1013-р (2016) (Україна). URL: https://zakon.rada.gov.ua/laws/show/1013-2016-p#Text (дата звернення: 23.12.2024).

337. Перші медичні заклади долучилися до пілоту системи eHealth. (2017, 6 вересня). URL: https://moz.gov.ua/uk/pershi-medichni-zakladi-doluchilisja-do-pilotu-sistemi-ehealth (дата звернення:17.09.2024).

338. Online A. (2020, 16 жовтня). Digital Med 2020: виклики та розвиток eHealth в Україні. Аптека Online. URL: https://www.apteka.ua/article/568312 (дата звернення:17.10.2024).

339. e-Health в Україні: що це і як працює? (2022, 5 серпня). Громадський Простір. URL: https://www.prostir.ua/?news=e-health-v-ukrajini-scho-tse-i-yak-pratsyuje (дата звернення:17.12.2024).

340. Укрінформ (2020). Кабмін затвердив Концепцію розвитку електронної системи охорони здоров'я. URL: https://www.ukrinform.ua/rubric-society/3162532-kabmin-zatverdiv-koncepciu-rozvitku-elektronnoi-sistemi-ohoroni-zdorova.html (дата звернення: 18.12.2024).

341. Левченко А. (2022, 1 лютого). Заступниця міністра охорони здоров'я Карчевич: "Зараз електронні медзаписи покривають більше 80% форм паперової документації". Інтерфакс. URL: https://interfax.com.ua/news/interview/795328.html (дата звернення: 20.12.2024).

342. Міністерство охорони здоров'я України. (2022). "План Відновлення Системи Охорони Здоров'я України Від Наслідків Війни На 2022 - 2032 Роки.". Урядовий портал. URL: https://moz.gov.ua/uploads/ckeditor/Новини/21-07-2022-Draft-Ukraine%20HC%20System%20Recovery%20Plan-2022-2032_UKR.pdf. (дата звернення:18.09.2024).

343. Serafini, A. G., & Serafini, A. G. (2024, October 18). Firewall e Sistemi IAM. SGSI e conformità NIS2. Cips Legal. URL: https://www.cipslegal.it/nis2/atti-documenti-nis2/firewall-e-sistemi-iam-sgsi-e-conformita-nis2/ (date of access:18.12.2024).

344. Jayaraman, N. (2023, December 15). IDS and IPS: Understanding Similarities and Differences. Cybersecurity Exchange. URL: https://www.eccouncil.org/cybersecurity-exchange/network-security/ids-and-ips-differences/ (date of access: 12.12.2024).

345. Compliancy Group. (2023, August 9). VPN in Healthcare Healthcare Data Protection. URL: https://compliancy-group.com/using-vpn-for-healthcare-data-protection/ (date of access:11.11.2024).

346. Охорона здоров'я Ukraine U.S. Agency for International Development. (2024, October 15). U.S. Agency For International Development. URL: https://www.usaid.gov/uk/ukraine/health (дата звернення: 08.12.2024).

347. USAID. (2022). Проект USAID «Підтримка реформи охорони здоров'я».” Press release. USAID. URL: https://moz.gov.ua/uploads/8/44830-nl_feb_23_ukr_final.pdf (date of access: 08.12.2024).

348. Country Development Cooperation Strategy - Ukraine Ukraine U.S. Agency for International Development. (2024, Janury 9). U.S. Agency For International Development. URL: https://www.usaid.gov/ukraine/country-development-cooperation-strategy-ukraine (date of access:11.11.2024).

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 11:48:33 20.06.2025

Назва файлу з підписом: ЗІНЧЕНКО_ДИСЕРТАЦІЯ 052.pdf.asice
Розмір файлу з підписом: 2.0 МБ

Перевірені файли:
Назва файлу без підпису: ЗІНЧЕНКО_ДИСЕРТАЦІЯ 052.pdf
Розмір файлу без підпису: 2.7 МБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: Зінченко Олександра Ігорівна
П.І.Б.: Зінченко Олександра Ігорівна
Країна: Україна
РНОКПП: 3589202643
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 11:48:20 20.06.2025
Сертифікат виданий: "Дія". Кваліфікований надавач електронних довірчих послуг
Серійний номер: 382367105294AF970400000010C057005744F703
Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301
Алгоритм підпису: ДСТУ 4145
Тип підпису: Кваліфікований
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований

Версія від: 2025.02.05 13:00