SOCIAL AND BEHAVIORAL SCIENCES

DOI https://doi.org/10.51647/kelm.2023.1.20

DECYZJE POLITYCZNE DOTYCZĄCE CYBERBEZPIECZEŃSTWA W KRAJACH EUROPEJSKICH

Yuliia Zavhorodnia
kandydat nauk politycznych, docent,
docent Katedry Teorii Politycznych
Narodowego Uniwersytetu "Odeska Akademia Prawnicza"
(Odessa, Ukraina)
ORCID ID: 0000-0003-3500-8638
julija020890@gmail.com

Adnotacja. Kraje europejskie wykazują ewolucję postrzegania cyberbezpieczeństwa, potrzeby ochrony infrastruktury organów zarządzających i wolę polityczną w celu przyjęcia odpowiednich przepisów w życiu publicznym. Już w świecie, w którym ma miejsce globalna cyberwojna i lokalna wojna w Ukrainie, doświadczenie systemu cyberobrony w Europie jest ważnym elementem dalszej powojennej działalności krajów.

Wiele procesów modernizacji działalności zarządczej jest opóźnionych, a tematem pierwszego planu jest zakończenie lokalnej konfrontacji na terytorium Ukrainy. Ponieważ zakończenie tej wojny oznaczałoby zmniejszenie poziomu cyberataków i potrzebę powojennej odbudowy oraz stabilizację wszystkich procesów polityczno-zarządczych. Niemniej jednak procesu cyberbezpieczeństwa nie można odłożyć na powojenną półkę, to skuteczna komunikacja, która jest dostępna za pośrednictwem przestrzeni informacyjnej, pozwoli szybko i skutecznie ustabilizować porządek światowy po wojnie w Ukrainie.

Słowa kluczowe: cyberbezpieczeństwo, cyberobrona, konsolidacja, Estonia, Finlandia, Niemcy.

POLITICAL DECISIONS ON CYBER SECURITY IN EUROPEAN COUNTRIES

Yulia Zavhorodnya
Candidate of Political Sciences, Associate Professor,
Associate Professor at the Department of Political Theories
National University "Odesa Law Academy" (Odesa, Ukraine)
ORCID ID: 0000-0003-3500-8638
julija020890@gmail.com

Abstract. European countries demonstrate the evolution of the perception of cyber security, the need to protect the infrastructure of governing bodies and the political will to adopt relevant standards in public life. Already in a world where there is a global cyber war and a local war in Ukraine, the experience of the cyber defense system in Europe is an important component for the further post-war activities of the countries.

Many processes related to the modernization of administrative activities are being postponed, and the topic of the first plan is the end of local confrontation on the territory of Ukraine. Since the end of this war will mean a decrease in the level of cyberattacks and the need for post-war reconstruction and stabilization of all political and administrative processes. However, the process of cyber security cannot be put on the post-war shelf, it is effective communication that is available through the information space that will allow to quickly and effectively stabilize the world order after the war in Ukraine.

Key words: cyber security, cyber protection, consolidation, Estonia, Finland, Germany.

ПОЛІТИЧНІ РІШЕННЯ ЩОДО КІБЕРБЕЗПЕКИ В ЄВРОПЕЙСЬКИХ КРАЇНАХ

Юлія Завгородня
кандидат політичних наук, доцент,
доцент кафедри політичних теорій
Національного університету «Одеська юридична академія»
(Одеса, Україна)
ORCID ID: 0000-0003-3500-8638
julija020890@gmail.com

Анотація. Європейські країни демонструють еволюцію сприйняття кібербезпеки, потреби щодо захисту інфраструктури органів управління та політичну волю для прийняття відповідних нормативів у суспільному житті. Уже в світі де відбувається глобальна кібервійна та локальна війна в Україні досвід системи кіберзахисту у Європі є важливою складовою для подальшої післявоєнної діяльності країн.

Багато процесів щодо модернізації управлінської діяльності відкладаються, а темою першого плану є закінчення локального протистояння на території України. Оскільки, закінчення цієї війни буде означати зменшення рівня кібератак та потреба у повоєнній відбудові та стабілізація усіх політико-управлінських процесів. Проте, процес кібербезпеки не можливо відкласти на післявоєнну поличку, саме ефективна комунікація, яка доступна через інформаційний простір, дозволить швидко та ефективно стабілізувати світовий порядок після війни в Україні.

Ключові слова: кібербезпека, кіберзахист, консолідація, Естонія, Фінляндія, Німеччина.

Вступ. Сучасний світ створює систему захисту кібепростору, яка діє на національному рівні, так і на наддержавному рівні. Підтвердженням цьому є діяльність НАТО у сфері кібербезпеки учасників Альянсу, створення міжнародних організацій, які координують діяльність учасників щодо об'єднання та міждержавна підтримка в регіональних коаліціях країн.

Уніфікація інформаційного простору в світі, потребує консолідованого рішення, щодо кіберзахисту у світі, проте світ і досі боїться обмежень державного управління та укорінення глобалізації управління в світі, а тому часто користується індивідуалістським підходом. Проте, у сфері кібербезпеки індивідуалістський підхід робить вразливою систему захисту, оскільки можливості окремих країн різні, пріоритети різні, забезпеченість кадрами різна. Троте, глобальні втрати від кібератак в економічному аспекті змінюють вектор цінностей окремих країн та переформатовають сучасне світосприйняття. Спільна методика щодо захисту критичної інформаційної інфраструктури шлях до вдосконалення інформаційної політики.

Аналіз окремих європейських країн дозволить узагальнити уявлення про систему цінностей у кібербезпеці, кіберборотьбі в політичній площині, оскільки захисті процеси від кіберконфліктів переформатовають уявлення про систему управління, взаємовідносин та кібератак на політичних діячів. Окрім того, впливові суб'єкти політики формують власні соціальні інформаційні сторінки, передвиборчі сторінки, формують ряд аккаунтів для так званого «хейту» щодо діяльності та висловлювань представників політичних партій, груп чи окремих політичних діячів.

Загалом, європейські країни у своїй діяльності демонструють єдність в багатьох аспектах політики, по різним вразливим питанням, а тому формування системи захисту у кіберпросторі не є виключенням. Проте, розвиток інформаційної інфраструктури лише набуває обертів та переформатовує політичну реальність світу. Адже інформаційні технології задають нові тренди для війни, яка містить небезпеку глобальних потрясінь.

Враховуючи специфіку актуальності розвитку сучасних протистоянь у кіберпросторі виникає необхідність консолідації зусиль щодо боротьби з негативними наслідками для вразливих суб'єктів, тому ***метою*** статі стало вивчення особливостей кіберборотьби окремими країнами європейського союзу, котрі мають політичний досвід, щодо кіберзлочинів та кібератак, який оприлюднений для публічного ознайомлення.

Основна частина. Для досягнення поставленої мети необхідно виконати ряд ***завдань,*** які сприятимуть отриманню, якісних висновків, а саме: проаналізувати існуючу систему кіберборотьби у Фінляндії; проаналізувати існуючу систему кіберборотьби у Естонії; проаналізувати існуючу систему кіберборотьби у Німеччині; виокремити специфіку визначених країн, їх особливості та недоліки; узагальнити ефективні механізми щодо впливу на кіберпротиборство; визначити перспективи удосконалення політичного протиборства у кіберплощині країнами європейського союзу.

Оцінюючи мету та завдання обраної тематики дослідження, варто акцентувати увагу на потребі політичної згуртованості демократичних режимів у сфері кіберборотьби. Оскільки, межі політичного кібервпливу не визначені, суб'єкти не персоналізовані, наслідки не прогнозовані в повному обсязі, тому удосконалювати систему кіберзнань та кіберпротидії потрібно постійно усім країнам світу, навіть тим, які мають найвищі показники у розвитку. Військова агресія росії на території України демонструє збільшення кібервпливу на країни, які активно публічно намагаються допомагати Україні. Так, за даними звіту компанії Check Point в першій половині 2022 року кількість кібератак збільшилась на 42% (Security Spectrum Services LLP., 2022). Разом з тим, світові втрати у зв'язку з кіберзлочинністю у 2021 році дослідники оцінюють у 5,5 трильйонів євро. В загальному аспекті Європі кібератаки обходяться приблизно 180 - 290 мільярдів євро щороку (Security Spectrum Services LLP., 2022).

Тому, питання щодо ціннісного фактору кібербезпеки у сучасному європейському просторі, та й у світі загалом, є досить актуальним, оскільки, сформує механізм для ефективної боротьби з шкідливими кіберпроцесами в кіберпросторі.

Матеріал і методи досліджень. Для деталізації актуалізованого напрямку було досліджено нормативну складову кібербезпеки інформаційно розвинутих країн у Європі, які демонструють передові технології по відношенню до системи кіберзахисту та кіберборотьби в сучасному світі. Окрім того, важливу роль відіграє аналіз науковцями розвитку кібербезпеки, як поштовху до подальших змін у процесах державного управління. Тому, робота в напрямку аналізу окремих європейських країн відбувалась за допомогою аналізу статистичних даних, та праць зарубіжних та вітчизняних авторів, а саме: Завгородньої Ю., Майгре М., Кавин С., Зінич Л., Добржанська О., Демцов А. та ін.

З метою отримання якісних результатів дослідження було використано загальнонаукові методи, а саме: системний метод (сприяв узагальненню розуміння кібербезпеки в політичних процесах), футурологічний метод (допоміг визначити вектор для майбутньої співпраці у напрямку кібербезпеки країн Європи), конфліктологічні теорії розвитку суспільства (визначили глобалізацію процесів протиборства через кіберпростір), метод біхевіоризму (сприяв здійсненню аналізу поведінки суб'єктів політики у європейських країнах щодо кіберзахисту).

Також, важливу роль у дослідженні відіграв метод статистичних даних, який математичними вирахуванням продемонстрував логіку економічної та конфліктогеннної небезпеки кіберпротиборства у сучасному світі, низькому рівню захищеності навіть економічно розвинутих країн, оскільки саме кібреатаки є глобалізованим компонентом.

Разом з тим, метод прийняття політичних рішень досить важливий для вирішення прогалин у кібербезпеці сучасного європейського світу, проте досвід кібернетично розвинутих країн задає тренди для запозичення та об'єднання в проблемі безпеки у кіберпросторі. Адже, сучасна політика демонструє внутрішню індивідуальність країн та глобальну систему захисту, яка зможе протистояти викликам сучасного світу, технологій та рішень. Адже, швидкість, якість та обґрунтованість політичних рішень в сучасному світі є запорукою успішної їх реалізації.

Важливо роль у дослідженні відіграв метод компоративістики, який допоміг виявити споріднені явища кібербезпеки та їх дієвість у протидії. Зрозуміло, що з таким показниками щодо економічних втрат Європи щороку від кіберзлочинів можемо дійти висновку, що потрібно продовжувати аналізувати, якісні показники, щоб декларувати їх в політичних рішеннях.

Окрім того, приділено увагу кібернетичному методу, який маючи не політичну сутність, вдало пояснює політичні процеси, які діють із запізненням, тому у структурі кібернетичної системи виокремлюють керуючий та керований об'єкти, прямі зв'язки, по яким здійснюються команди управління, та зворотні зв'язки, по котрих рухається інформація щодо виконання команд управління, аналіз котрої сприяє можливому коригуванню команди управління. Таке уявлення про кіберзв'язки демонструє наявність систематизованих ланцюгів для політичної конфронтації позицій в кіберпросторі, що сприятиме розумінню елемента захисту та форм протидії.

Результати та їх обговорення. Сучасна система міжнародних відносин допомагає скоординувати виклики та проблеми сучасного світу. Основною проблемою у сфері міжнародних конфліктів є кібербезпека, оскільки є най вразливішою для сильних держав, які мають міжнародний авторитет.

Так, старший науковий співробітник та керівник напрямку кібербезпеки в CEPS Initiative Лоренцо Пупілло зазначив, що «сучасна війна сформована зростаючими явищами міжнародних кібератак на державній арені. Стійкість – це ключ до такої загрози. Хоча багато комп'ютерів відреагували завдяки декільком процедурам та програмам, мільйони інших були атаковані. Це свідчить про необхідність підвищення обізнаності про кіберзагрози» (Пупілло, 2017).

Окрім того, Л. Пупілло вважає, що « ЄС, як нормативна супердержава, повинен взяти на себе ініціативу у визначенні нових норм захисту цивільного використання Інтернету» (Пупілло, 2017).

Враховуючи специфіку кіберпростору та можливість протидії кіберконфліктам в європейських країнах існує думка, щодо уніфікації законодавства в кібербезпеці європейських країн, оскільки боротись з забезпеченням захисту інформації в кіберпросторі дуже складно, а тому така тенденція може слугувати до консолідації демократичних країн в не залежності від економічного рівня розвитку до підтримки балансу в кіберсередовищі.

На думку Тьєррі Бретона «комп'ютери, телефони, побутова техніка, пристрої віртуальної допомоги, автомобілі, іграшки... кожен із цих сотень мільйонів підключених продуктів є потенційною точкою входу для кібератаки, і тим не менш, сьогодні на більшість апаратних і програмних продуктів не поширюються будь-які зобов'язання щодо кібербезпеки»(Interfax-Україна, 2022).

Тому, Єврокомісія бажає сформувати таке законодавство для ЄС, щоб створити уніфіковані вимоги для продуктів, котрі містять цифрові елементи протягом усього їхнього життєвого циклу, адже існуюча небезпека приносить великі економічні втрати для світу. Так, кожні 11 секунд у світі відбувається кібератака, що у 2021 році проявилася в еквіваленті 5,5 трлн євро(Interfax-Україна, 2022).

У зв'язку з цим, кіберсфера та кібербезпека стали важливим аспектом зовнішньої політики та політики безпеки для Фінляндії. Оскільки, кіберзагрози не поважають національних кордонів, тому у європейських країн виникає розуміння необхідності зміцнення міжнародного співробітництва у сфері кібербезпеки. МЗС координує даний напрямок діяльності. Основною метою національної стратегії кібербезпеки Фінляндії є реагування на кіберзагрози, посилення загальної безпеки суспільства та забезпечення безперебійного функціонування кіберсфери.

У рамках законодавчо затвердженої Стратегії регламентовано десять цілей, реалізація яких надає Фінляндії можливість на національному рівні контролювати навмисні та ненавмисні несприятливі наслідки кіберсфери, а також реагувати на них і відновлюватися після них. Комітет безпеки контролює реалізацію стратегії кібербезпеки Фінляндії (Finland´s Cyber security Strategy, 2013).

Для Фінляндії, особливо ЄС, є центральним гравцем у питаннях кібербезпеки. ЄС сформулював низку спільних політик щодо кібернетичних питань, серед яких Висновки Ради щодо кібердипломатії, ухвалені Радою Європейського Союзу в лютому 2015 року. Тому, визначаючи національні цілі захисту в кіберпросторі Фінляндія розуміє цінність співпраці в даному напрямку роботи для більшості цивілізованих країн.

Хоча, Фінляндія отримала корону країни з найнижчим показником кібернебезпеки в усьому світі за період з 2018 по 2022 роки. Зацікавившись безпекою цифрових кочівників, експерти Reboot Digital PR Services

проаналізували статистику кібербезпеки, включно з випадковими завантаженнями, фішинговими сайтами, сайтами розміщення шкідливого програмного забезпечення та скомпрометованими комп'ютерами, щоб створити індекс кібернебезпеки.

Тому, за допомогою дослідження стало відомо, що Фінляндія отримала корону найбільш кіберзахищеної країни в світі з показником кібернебезпеки 12,6 зі 100, очолюючи рейтинги в Європі та в усьому світі. Але цей показник захищеності не достатньо високий для безпеки країни та Європи в цілому.

Тому, уже сьогодні органи державного управління Фінляндії повідомляють про потребу забезпечувати захист кіберпростору в більших об'ємах, що випливає з потреб у кадровому потенціалі та освіченості громадян.

Чудовим зразком найбільш прогресивних європейських країн в безпековому плані, щодо кіберпростору є Естонія, котра входить в топ 5 країн за рівнем кіберзахисту. Звичайно, цьому слугували виклики, які стояли перед цією країною під час її розвитку. Ще у 2007 році відбулись кібератаки російських хакерів на кіберпростір Естонії, тому удосконалення та цифровізація держави розпочалась з надійної системи захисту, яка сприяла подальшим системним діям, котрі вивели цю європейську країну на високий рівень інформаційно-безпекового розвитку.

Звичайно, що центральними діями Естонії є прийняття на національному рівні важливих рішень, таких як Стратегія кібербезпеки, котра визначила державні органи що є точками контакту і відповідають на державному рівні за координацію і організацію постійного підвищення кваліфікації і навчання в сфері кіберзахисту. Окрім того, після атак 2007 року був сформований КІБЕРЦЕНТР, «схвалений НАТО (так атаки на Естонію стали хорошим шансом для неї, але й НАТО також почав сприймати кіберсферу на серйозному рівні)» (Майгре, 2021).

Естонія пройшла довгий шлях становлення органів управління кіберзахистом, проте продемонструвала ефективність та якість прийнятих рішень. «До 2011 р. координацію політики держави в області кібербезпеки забезпечувало Міністерство оборони Естонії, а з 2011 р. відповідальність за координацію політики в області кібербезпеки Естонії перейшла від Міністерства оборони до Міністерства з економічних питань та комунікацій. Міністерство оборони є координаційним органом для кібернетичної оборони в загальній системі національної оборони. Відповідно, розробка і впровадження політики інформаційної безпеки належить до компетенції саме Міністерства з економічних питань та комунікацій, зокрема до його структурних підрозділів, таких як Департамент державних інформаційних систем та Естонський центр інформатики (Кавин, 2020). У червні 2011 р. Естонський центр інформатики був трансформований в Управління інформаційних систем Естонії (Estonian Information Systems Autority (EISA)). В Управління інформаційних систем Естонії входять ряд структурних підрозділів, які комплексно забезпечують кібербезпеку держави, зокрема: Департамент із захисту критичних інформаційних інфраструктур (Critical Information Infrastructure Protection (CIIP)), Центр обміну документами (About document exchange centre (DEC)), Інфраструктура відкритих ключів (Public Key Infrastructure (PKI)), IT-інфраструктура (IT-infrastructure). Інфраструктура відкритих ключів забезпечує безпеку цифрову аутентифікацію і цифрові підписи. IT-інфраструктура забезпечує доступність основних інформаційних послуг держави навіть у разі форс-мажорних обставин» (Кавин, 2020).

Основними напрямками подальшого удосконалення системи кібербезпеки Естонії є створення державних підрозділів з кібер поліції, а також Центрів реагування на інциденти у кіберпросторі, основна робота яких направлена на боротьбу з кіберзлочинами. Разом з тим, підвищується міра відповідальності за адміністративні та кримінальні злочини у галузі інформаційних правопорушень.

Окрім того, варто приділити увагу Німеччині, яка також чітко реагує на виклики сучасності та координує свою діяльність прагматично щодо кіберзахисту цієї країни та держав котрих вона підтримує.

Відносно Стратегії кібербезпеки ФРН федеральний уряд застосовує заходи на базі існуєчих структур до відповідних загроз за такими напрямками як «захист найважливіших інформаційних інфраструктур (в центрі уваги кібербезпеки є захист інформаційних структур, які містять цінність державну); IT–системи безпеки ФРН (захист інфраструктур містить потребу у надійності IT–систем громадян, а також малих та середніх підприємств, тому, користувачі потребують інформацію, яка відповідала б їхнім потребам і не суперечила сама собі про ризики, які пов'язані з IT–системами і самостійно застосовувати заходи безпеки, щодо безпеки свідомої поведінки у кіберпросторі); посилення IT–безпеки в публічному управлінні (публічне управління ще сильніше захистить свої IT–системи, державні установи повинні бути зразком відносно захисту даних, тому основою електронного обміну даними і вербальної комунікації буде загальна, універсальна і надійна сітьова інфраструктура Федеральної адміністрації)» (Добржанська О., Демцов А., 2011).

Окрім того, в Німеччині сформовано національний Центр кіберзахисту, який націлений на виконання заходів щодо безпеки кіберпростору, розвиваючи цей напрямок Німеччина, як і інші прогресивні та цифро візовані країни приходить до висновків щодо потреби міжнародної координації зусиль по кіберзахисту. Тому, коли в Україні розпочалось повномасштабне вторгнення агресора однією із форм підтримки, яку надала Німеччина для України – це матеріальна підтримка для кіберзахисту України. Оскільки повалення інформаційної критичної інфраструктури – це суспільний хаос та паніка, порушення балансу управлінської системи, дестабілізація процесів взаємовідносин між органами управління та суспільством, тому цей напрямок потрібно було захищати поряд з усіма іншими критично важливими об'єктами держави.

Загальна концепція діяльності Федерального відомства з забезпеченні безпеки інформаційної техніки у сучасних умовах координує свою діяльність зі структурами НАТО і ЄС для виконання наступних функцій: «оцінка ризику впровадження інформаційних технологій, перевірка надійності існуючих інформаційно-технічних засобів, котрі використовуються у сфері діяльності федеральних органів влади; розробка критеріїв, методів і випробувальних засобів для оцінки ступеня захищеності національних комунікаційних систем;

створення, перевірка надійності, випробування і впровадження в експлуатацію криптографічного матеріалу для інформаційного обміну (приміром, шифрування секретних документів) на федеральному рівні та на об'єктах економічних і підприємствах, пов'язаних зі сферою національної безпеки; перевірка ступеня захищеності, сертифікація інформаційно- технічних систем і видача відповідних сертифікатів; видача дозволів на впровадження інформаційних систем на важливих державних об'єктах; здійснення спеціальних заходів безпеки інформаційного обміну в державних органах, поліції тощо; підтримання контактів з метою консультування федеральних відомств, правоохоронних органів, відомств з охорони Конституції (в інформаційно-технічній сфері), а також керівників підприємств і організацій (для протидії економічному шпигунству)» (Корсун К., 2017).

Враховуючи специфіку кібернетичної сфери держава та економіка мають створити чіткий стратегічний та організаційний базис з метою посилення інтеграції в кіберпростір на основі інтенсивного обміну інформацією громадян різних країн.

Формування наддержавної системи захисту кіберпростору в Європі розпочинається з прийняття Конвенції про кіберзлочинність в 2001 році Радою Європи, а пізніше прийнято додатковий протокол до Конвенції у 2003 році, який націлений на боротьбу розповсюдження інформації расистського та ксенофобського характеру. В сучасному аспекті розвитку подій політичних, міжнародних, глобальних виникає потреба гнучкого мислення щодо подолання атак у різних формах прояву та стимулює сучасних фахівців до практичного пошуку дієвих механізмів. Проте, сфера прийняття управлінських рішень обмежує фахівців сфери ІТ в рамках культури дій та методів впливу.

Україна у своїх діях завжди рівняється на стратегічному рівні на європейських колег. Однак, в умовах війни українська держава стає бажаним партнером, який має великий досвід боротьби з кіберагресором. Оскільки, українські фахівці в кіберпросторі налаштувались на попереджувальні заходи, які допомагали боротися з атаками та отримувати хороші відгуки партнерів про досягнені результати. Практичний досвід є важливою складовою для подальшого удосконалення та розвитку системи кібербезпеки на глобальному рівні.

Тому, Україна уже підписала Меморандуми щодо співпраці з окремими європейськими країнами, такими як: Фінляндія, Німеччина. Окрім того, Україна ділиться розробками програми Дія, яка зарекомендувала себе якісними показниками та відгуками. Сьогодні політичні рішення європейських країн прямо чи опосередковано пов’язані з військовими подіями на території української держави. Тому, усі політичні рішення у європейських країнах, пов’язані з кібернетичним простором, можуть приймаються на підставі отриманого досвіду у кіберборотьбі війни в Україні.

Разом з тим, політична система європейських країн постійно страждає від окремих видів кібернападів, що потребує безперервного контролю за інформаційно-ресурсним забезпеченням країн Європи та їх громадян.

Висновки. Мабуть, найважливішим кроком, який можна зробити в будь-якій сучасній європейській країні, - це переконатися, що вона працює над ініціюванням і вихованням культури обізнаності щодо питань кібербезпеки. Сьогодні для громадян уже недостатньо добре просто думати про кібербезпеку як про проблему, якою повинен займатися ІТ-відділ. Проте, у 2023 році усвідомлення загроз і вжиття основних запобіжних заходів для забезпечення безпеки мають стати основною частиною завдань для діяльності глобальних суб’єктів політики.

Аналізуючи окремі країни Європи бачимо, що Фінляндія є найбільш кіберзахищеною країною для віддаленої роботи, Естонія найбільш цифровізованою країною та центром кібернетичного захисту НАТО, Німеччина прагматично діє до викликів сучасності у кіберпросторі та в оремих випадках вдало справляється з проблемами кіберзагроз. Проте, усі ці європейські країни мають єдине розуміння щодо потреби спільних концепцій захисту та безпеки в кіберпросторі. Оскільки, політичні конфлікти та плюралізм суспільних проблем створюють небезпеку глобального хаосу в інформаційній системі та цифровізованому просторі людей, який є зручною, швидкою та дієвою процедурою, тому безперервне спостереження за політичними процесами, їх розвитком та можливими атаками від прийнятих політичних рішень, можливо сформувати вдалі механізми протидії та попередження в кіберпросторі.

Разом з тим, існуючі дані про атаки та їх подолання в кіберпросторі продемонстрували, що чотири з десяти країн із найбезпечнішими мережами знаходяться саме в Європі. Тому, продовження наднаціонального рівня співпраці щодо кіберпростору та координації спільних дій щодо форм та методів кіберзахисту є запорукою збільшення показників безпеки кіберпростору та стабілізації просторових меж в окремих європейських країнах та загалом у світовому порядку сучасності.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від Відомості Верховної Ради, 2017, № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Початок роботи нового постачальника послуг кібербезпеки для партнерів у азіатсько-тихоокеанському регіоні. *Security Spectrum Services LLP.* 2022. URL: https://pages.checkpoint.com/cyber-attack-2022-trends.html
3. Кібербезпека в ЄС: життя в рамках парадоксу прогресу. Відкриваючи Україну Європі. *Пупілло.* 2017. URL: https://ukraine-office.eu/cybersecurity-in-the-eu-living-within-a-paradox-of-progress/
4. Єврокомісія запропонувала ухвалити закон про кіберстійкість цифрових продуктів. *Interfax-Україна*. 2022. URL: https://ua.interfax.com.ua/news/general/859165.html
5. Finland's cyber security strategy. Government Resolution. 2013. URL: https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

6. Майгре М. Віртуальний фронт. Як Естонія стала гуру з кіберзахисту і чому може повчитися в неї Україна. *Фокус.* 2021. URL: https://focus.ua/uk/opinions/484496-virtualnyy-front-kak-estoniya-stala-guru-po-kiberzashchite-i-chemu-mozhet-pouchitsya-u-nee-ukraina
7. Кавин С. Нормативно-правові механізми забезпечення кібербезпеки в країнах Балтії. *Підприємство, господарство і Право.* №12. 2020. URL: http://pgp-journal.kiev.ua/archive/2020/12/56.pdf
8. Зінич Л. Інформаційна безпека Естонії: досвід для України. *Збірник наукових статей.* 2020. URL: http://lib.pnu.edu.ua:8080/bitstream/123456789/8674/1/2088-Article%20Text-4373-1-10-20200219.pdf
9. Десять найбільш захищених країн світу у кіберпросторі 2018-2022 років. 2022. URL: https://www.helsinkitimes.fi/images/2022/8-Aug/cs_graph.png
10. Добржанська О.Л., Демцов А.А. Кібербезпека як феномен міжнародних відносин на прикладі федеративної республіки Німеччини. *Міжнародна інформаційна безпека: сучасні конфепції та практика.* 2011. URL: http://apir.iir.edu.ua/index.php/apmv/article/view/2126/1889
11. Корсун К. Як із кібербезпекою на Заході: досвід Німеччини. *Укрінформ.* 2017. URL: https://www.ukrinform.ua/rubric-technology/2233793-ak-iz-kiberbezpekou-na-zahodi-dosvid-nimeccini.html

References:

1. Zakon Ukrainy (2017) «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» [About the main principles of ensuring cyber security of Ukraine] vid Vidomosti Verkhovnoi Rady, № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian]
2. Pochatok roboty novoho postachalnyka posluh kiberbezpeky dlia partneriv u aziatsko-tykhookeanskomu rehioni.[Start of work of a new provider of cyber security services for partners in the Asia-Pacific region] Security Spectrum Services LLP. (2022) URL: https://pages.checkpoint.com/cyber-attack-2022-trends.html[in Ukrainian]
3. Kiberbezpeka v YeS: zhyttia v ramkakh paradoksu prohresu. [Cybersecurity in the EU: living within the paradox of progress] Vidkryvaiuchy Ukrainu Yevropi. Pupillo. (2017). URL: https://ukraine-office.eu/cybersecurity-in-the-eu-living-within-a-paradox-of-progress/ [in Ukrainian]
4. Yevrokomisiia zaproponuvala ukhvalyty zakon pro kiberstiikist tsyfrovykh produktiv.[The European Commission proposed to adopt a law on the cyber resistance of digital products] Interfax-Ukraine. (2022). URL: https://ua.interfax.com.ua/news/general/859165.html [in Ukrainian]
5. Finland's cyber security strategy. Government Resolution. (2013). URL: https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf[in English]
6. Maihre M. (2021)Virtualnyi front. Yak Estoniia stala huru z kiberzakhystu i chomu mozhe povchytysia v nei Ukraina. [Virtual front. How Estonia became a cyber defense guru and why Ukraine can learn from it.] Fokus. URL: https://focus.ua/uk/opinions/484496-virtualnyy-front-kak-estoniya-stala-guru-po-kiberzashchite-i-chemu-mozhet-pouchitsya-u-nee-ukraina [in Ukrainian]
7. Kavyn S. (2020) Normatyvno-pravovi mekhanizmy zabezpechennia kiberbezpeky v krainakh Baltii. [Regulatory and legal mechanisms for ensuring cyber security in the Baltic States] Pidpryiemstvo, hospodarstvo i Pravo. №12. URL: http://pgp-journal.kiev.ua/archive/2020/12/56.pdf [in Ukrainian]
8. Zinych L.(2020) Informatsiina bezpeka Estonii: dosvid dlia Ukrainy. [Information security of Estonia: experience for Ukraine] Zbirnyk naukovykh statei. 2020. URL: http://lib.pnu.edu.ua:8080/bitstream/123456789/8674/1/2088-Article%20Text-4373-1-10-20200219.pdf [in Ukrainian]
9. Desiat naibilsh zakhyshchenykh krain svitu u kiberprostori 2018-2022 rokiv.[The ten most protected countries in the world in cyberspace 2018-2022] (2022). URL: https://www.helsinkitimes.fi/images/2022/8-Aug/cs_graph.png[in Ukrainian]
10. Dobrzhanska O.L., Demtsov A.A. (2011) Kiberbezpeka yak fenomen mizhnarodnykh vidnosyn na prykladi federatyvnoi respubliky Nimechchyny.[Cyber security as a phenomenon of international relations on the example of the Federal Republic of Germany] Mizhnarodna informatsiina bezpeka: suchasni konfeptsii ta praktyka. URL: http://apir.iir.edu.ua/index.php/apmv/article/view/2126/1889[in Ukrainian]
11. Korsun K. (2017) Yak iz kiberbezpekoiu na Zakhodi: dosvid Nimechchyny.[How to deal with cyber security in the West: the experience of Germany] Ukrinform. URL: https://www.ukrinform.ua/rubric-technology/2233793-ak-iz-kiberbezpekou-na-zahodi-dosvid-nimeccini.html[in Ukrainian]