Cybersecurity System as a Component of National Security

UDC: 004.056:355.45 DOI: https://doi.org/10.15421/172496

Kret Olga
Ph.D., Assoc Prof., https://orcid.org/0000-0003-1736-3863, olga.kret@rshu.edu.ua
Kret Roman
Ph.D., Assoc Prof., https://orcid.org/0000-0001-6208-5837, roman.kret@rshu.edu.ua
Kundeus Oksana
Ph.D., Assoc Prof., https://orcid.org/0000-0002-1162-3858, oksana.kundeus@rshu.edu.ua
Rivne State University of the Humanities (Rivne, Ukraine)

Abstract

The relevance of this research is driven by the development of information technologies, which is accompanied by an increase in the number and complexity of cyber threats. The modern world is increasingly dependent on digital systems, making states vulnerable to cyberattacks on critical infrastructure. The growing number of attacks on key national assets, such as energy systems, banking institutions, and communication networks, underscores the necessity of robust cybersecurity. Cyberattacks, which can cause significant economic and social consequences, are becoming tools of pressure, highlighting the importance of cybersecurity in ensuring national stability.

The aim of this study is to identify the fundamental principles and elements of a cybersecurity system as a component of a state's national security, to assess its relevance and effectiveness based on the analysis of modern cyber threats, and to justify ways to improve state cybersecurity policies by considering international experience and specific examples.

The results of the study indicate the need for a comprehensive approach to building a cybersecurity system. Protection from cyber threats should encompass not only technological but also legal and organizational aspects. International cooperation is particularly critical, as threats in cyberspace do not respect national borders. The experience of leading countries shows that effective combat against cyberattacks requires the involvement of both the public sector and private business. Examples include initiatives by the United States and EU countries, which are developing infrastructure and collaborating on the international level.

Conclusions emphasize that cybersecurity is a key element of any state's national security strategy. Effective protection in cyberspace is possible only through close cooperation between the state, businesses, and international organizations. Continuous updates of security measures, along with personnel training and raising citizens' awareness of cyber threats, are critically important components of a successful cybersecurity strategy.

Keywords: cybersecurity, national security, cyberattacks, critical infrastructure, international cooperation, state policy, digital technologies, cyber threats, cyber defense, information systems

Система кібербезпеки як складова національної безпеки держави

Крет Ольга, Крет Роман, Кундеус Оксана
Рівненський державний гуманітарний університет (Рівне, Україна)

Анотація

Актуальність цього дослідження зумовлена розвитком інформаційних технологій, що супроводжується збільшенням кількості та складності кіберзагроз. Сучасний світ дедалі більше залежить від цифрових систем, що робить держави вразливими до кібернападів на критичну інфраструктуру. Зростання кількості атак на об'єкти державної важливості, такі як енергетичні системи, банківські установи та комунікаційні мережі, підтверджує необхідність надійного кіберзахисту. Кібератаки, що здатні викликати серйозні економічні та соціальні наслідки, стають інструментом тиску, що підвищує значимість теми кібербезпеки для забезпечення національної стабільності.

Метою даного дослідження є визначення основних принципів та елементів системи кібербезпеки як складової національної безпеки держави, вивчення її актуальності та ефективності на основі аналізу сучасних кіберзагроз, а також обґрунтування шляхів удосконалення державної політики у сфері кіберзахисту з урахуванням міжнародного досвіду та конкретних прикладів.

Результати дослідження свідчать про необхідність комплексного підходу до побудови системи кібербезпеки. Захист від кіберзагроз має охоплювати не лише технологічні, але й правові та організаційні аспекти. Зокрема, критичним є міжнародне співробітництво, оскільки загрози в кіберпросторі не мають державних кордонів. Досвід провідних країн свідчить, що для ефективної боротьби з кібератаками необхідно залучати як державний сектор, так і приватний бізнес. Прикладом можуть слугувати ініціативи США та країн ЄС, які розвивають інфраструктуру та співпрацюють на міжнародному рівні.

Висновки підкреслюють, що кібербезпека є ключовим елементом стратегії національної безпеки будь-якої держави. Ефективний захист у кіберпросторі можливий лише за умов тісної співпраці між державою, бізнесом та міжнародними організаціями. Постійне оновлення засобів захисту, а також навчання персоналу та підвищення обізнаності громадян щодо кіберзагроз є критично важливими складовими успішної стратегії кібербезпеки.

Ключові слова: кібербезпека, національна безпека, кібератаки, критична інфраструктура, міжнародне співробітництво, державна політика, цифрові технології, кіберзагрози, кіберзахист, інформаційні системи

Стаття надійшла / Article arrived: 15.07.2024 Схвалено до друку / Accepted: 17.10.2024

Вступ.

У сучасному світі цифрові технології стали невід'ємною частиною функціонування державних інститутів, економічних систем та повсякденного життя громадян. Зростаюча залежність від інформаційних систем та мереж робить держави вразливими до нових загроз у кіберпросторі, де кібератаки можуть стати інструментом політичного, економічного та військового тиску. Захист критичних інформаційних інфраструктур, забезпечення безпеки даних та протидія кібератакам стають пріоритетними завданнями кожної держави, що прагне зберегти стабільність та безпеку на національному рівні.

З кожним роком масштаби кіберзагроз лише зростають. Наприклад, кібератака на Colonial Pipeline у 2021 році, що спричинила зупинку постачання пального в США, показала, наскільки вразливою може бути інфраструктура держави до цифрових загроз. Це доводить, що навіть розвинені країни можуть стати жертвами кібернападів, які мають серйозні економічні та соціальні наслідки. Іншим прикладом є атака вірусу NotPetya у 2017 році (Шеремет, 2017), яка зачепила кілька країн, включно з Україною, де в результаті були паралізовані робота банківської системи, енергетичні об'єкти та державні установи. Це підкреслює глобальний характер кіберзагроз, які можуть охоплювати як державні, так і приватні структури. У цьому контексті система кібербезпеки стає важливою складовою загальної стратегії національної безпеки держави, забезпечуючи захист її критичних ресурсів та інтересів у цифровому просторі.

Актуальність обраної тематики зумовлена стрімким розвитком технологій, збільшенням кількості та масштабів кібератак, а також впливом цих загроз на національну безпеку. У наш час кіберзагрози більше не обмежуються викраденням даних чи порушенням роботи окремих підприємств. Вони мають потенціал завдати серйозної шкоди національній інфраструктурі, економіці та навіть вплинути на політичну ситуацію в державі. Прикладом масштабної загрози є атака на енергосистему України в грудні 2015 року, яка спричинила відключення електроенергії для сотень тисяч людей. Ця атака була спрямована на критичну інфраструктуру, що підкреслює важливість захисту таких об'єктів у рамках національної стратегії кібербезпеки (Відключення електроенергії, 2016).

Іншим прикладом є втручання у вибори у США в 2016 році, де кібероперації, спрямовані на маніпуляцію громадською думкою через соціальні медіа та злом інформаційних систем, продемонстрували, як цифрові загрози можуть впливати на демократичні процеси. Такі події показують, що питання кібербезпеки виходять за межі технічних аспектів та охоплюють національну стабільність, політичну незалежність та суспільну довіру. Усе це робить дослідження системи кібербезпеки як складової національної безпеки надзвичайно важливим. Сучасні реалії вимагають комплексного підходу до формування ефективної стратегії кіберзахисту, яка охоплює технологічні, правові та організаційні аспекти.

Метою даного дослідження є визначення основних принципів та елементів системи кібербезпеки як складової національної безпеки держави, вивчення її актуальності та ефективності на основі аналізу сучасних кіберзагроз, а також обґрунтування шляхів удосконалення державної політики у сфері кіберзахисту з урахуванням міжнародного досвіду та конкретних прикладів. Для досягнення поставленої мети, у дослідженні використовуються методи аналізу, синтезу, порівняння досвіду у сфері кібербезпеки, метод індукції та дедукції, описовий метод та метод узагальнення а також методи системного та структурного аналізу для вивчення кібербезпеки як складової національної безпеки.

Аналіз попередніх досліджень і публікацій з кібербезпеки як складової національної безпеки охоплює різні аспекти кіберзахисту та загроз для національних систем безпеки.

Тетяна Сліпченко у своїй праці "Кібербезпека як складова системи захисту національної безпеки: європейський досвід" розглядає законодавче регулювання кібербезпеки в Україні та пропонує вдосконалення правової бази, незалежний аудит безпеки й міжнародне співробітництво (Сліпченко, 2020).

Ольга Вакулік з колегами у статті "Cybersecurity as a component of the national security of the state" підкреслюють роль українських державних органів у боротьбі з кіберзагрозами, наголошуючи на недостатній співпраці між державними та приватними структурами (Vakulyk, Petrenko, Kuzmenko, Pochtovyi, & Orlovskyi, 2020).

Карлос Солар у своїй роботі "Cybersecurity and cyber defence in the emerging democracies" аналізує кібербезпеку в нових демократіях, звертаючи увагу на баланс між національними інтересами і демократичними принципами (Solar, 2020).

Міріам Данн Кавелті та Андреас Венгер у статті "Cyber security meets security politics" досліджують вплив глобальних кіберзагроз на політичні процеси та національну безпеку, наголошуючи на необхідності міжнародного співробітництва (Dunn Cavelty, & Wenger, 2019).

Володимир Ліпкан і Ігор Діордіца у своїй праці "Національна система кібербезпеки" висвітлюють потребу в уніфікованій моделі кібербезпеки для ефективного захисту держави (Ліпкан, & Діордіца, 2017).

Володимир Ємельянов і Ганна Бондар у статті "Кібербезпека як складова національної безпеки" акцентують на захисті критичної інфраструктури

та необхідності впровадження нових стандартів кібербезпеки (Ємельянов, & Бондар, 2019).

Ці праці підкреслюють важливість співпраці між державними, приватними структурами та міжнародними партнерами для ефективної протидії кіберзагрозам.

Результати дослідження.

Кібербезпека є фундаментальною складовою національної безпеки, яка відіграє важливу роль у захисті державних інтересів в умовах глобалізації та стрімкого розвитку інформаційних технологій. Визначення кібербезпеки охоплює широкий спектр аспектів, що стосуються захисту інформаційних систем, кіберпростору, а також забезпечення конфіденційності, цілісності та доступності даних. Кібербезпека визначається як система заходів, спрямованих на захист від кіберзагроз, які можуть бути спрямовані як на державні установи, так і на приватні інституції, критичну інфраструктуру та суспільство в цілому. Згідно з визначенням, кібербезпека передбачає управління ризиками, пов'язаними з використанням цифрових технологій, та захист інформаційного середовища від несанкціонованого доступу, кібернападів та інших загроз (Сліпченко, 2020).

Зв'язок між кібербезпекою та національною безпекою є очевидним і критичним. У сучасному світі національна безпека залежить не лише від фізичного захисту кордонів, але й від захисту кіберпростору, оскільки більшість державних функцій і комунікацій здійснюються за допомогою інформаційних технологій. Кіберзагрози можуть підривати функціонування державних інститутів, впливати на політичну стабільність і безпосередньо загрожувати національній безпеці. У такому контексті кібербезпека стає невід'ємною частиною національної стратегії безпеки, що охоплює як оборонні, так і наступальні аспекти кібердій. Це передбачає не лише захист державних ресурсів, але й активну протидію зовнішнім загрозам та кібертероризму (Vakulyk, Petrenko, Kuzmenko, Pochtovyi, & Orlovskyi, 2020). Кіберзагрози мають значний вплив на державні інститути, економіку та суспільну стабільність.

Кібербезпека стала однією з ключових сфер у сучасному інформаційному суспільстві. Визначення цього терміну варіюється серед науковців та організацій, проте всі вони сходяться на важливості його ролі в захисті інформаційного простору. О. А. Баранов надає два визначення кібербезпеки. Перш за все, він розглядає її як інформаційну безпеку в контексті використання комп'ютерних систем та телекомунікаційних мереж. Альтернативно, він визначає кібербезпеку як захищеність критично важливих інтересів особи, суспільства та держави в умовах використання цих технологій, спрямовану на мінімізацію шкоди від неповного, несвоєчасного та недостовірного використання інформації, негативного інформаційного впливу, а також несанкціонованого розповсюдження даних (Баранов, 2014).

За твердженням О. М. Степко, кібербезпеку варто розуміти як стан захищеності важливих інтересів особи, суспільства та держави, що спрямований на зменшення шкоди, спричиненої недостовірною, неповною або несвоєчасною інформацією, негативними інформаційними впливами, а також несанкціонованим використанням інформаційних технологій (Степко, 2014).

В. М. Фурашев характеризує кібербезпеку як здатність окремих осіб, спільнот та урядів запобігати та пом'якшувати негативні наслідки або маніпуляції з інформацією, будь то навмисні чи ненавмисні (Фурашев, 2012).

Д. Несрін та Л. А. Радомська підкреслюють, що кібербезпека охоплює захист цілісності комп'ютерних систем, включаючи обладнання, програмне забезпечення та дані, зокрема особисту інформацію, від можливих загроз і атак, що можуть виникати під час різних бізнес-процесів (Несрін, & Радомська, 2021). Зважаючи на різні підходи до визначення, можна констатувати, що кібербезпека охоплює захист інформації, технологій та інтересів різних суб'єктів від різноманітних загроз у кіберпросторі.

Вплив кіберзагроз на державні інститути, економіку та суспільну стабільність є значним. Сучасні кібератаки можуть паралізувати державні системи та викликати серйозні збої в економіці. Після кібератак в Естонії у 2007 році багато країн усвідомили важливість кібербезпеки для національної безпеки. Невідомий та невидимий супротивник може завдати шкоди без прямого військового втручання, що робить кібербезпеку пріоритетом для державних стратегій безпеки. Також, атака вірусу "Petya" у 2017 році паралізувала роботу численних українських державних установ, банків і приватних компаній, що показує вразливість держави перед кіберзагрозами. Такі атаки можуть не тільки знищити важливі дані, але й дестабілізувати політичну ситуацію, створюючи недовіру до уряду з боку населення. Це підкреслює важливість створення національної системи кібербезпеки, яка повинна інтегрувати як державні, так і приватні сектори у боротьбі з кіберзагрозами (Ліпкан, & Діордіца, 2017).

У світі спостерігається тенденція до підвищення уваги до кібербезпеки з боку міжнародних організацій. Провідні країни світу вже розробили стратегії кібербезпеки, які включають не тільки захист інформаційних систем, але й заходи щодо попередження кібершпигунства та кібертероризму (Ліпкан, & Діордіца, 2017). Кіберзагрози мають багатогранний вплив на різні сфери державного та суспільного життя, так, кібератаки можуть призвести до витоку конфіденційної інформації, порушення роботи урядових систем та підриву довіри громадян до державних установ. Кіберзлочинність завдає значних

фінансових збитків компаніям та державі. Атаки на фінансові установи, промислові підприємства та інші економічно важливі об'єкти можуть призвести до економічної нестабільності. Поширення дезінформації та маніпуляція громадською думкою через кіберпростір можуть викликати соціальні напруження, політичну нестабільність та підривати демократичні процеси. У зв'язку з цим, забезпечення кібербезпеки є критично важливим для захисту національних інтересів та підтримки стабільності держави. Кібербезпека є ключовим елементом національної безпеки в інформаційному суспільстві. Захист від кіберзагроз вимагає комплексного підходу, що включає міжнародну співпрацю, розвиток законодавчої бази та впровадження передових технологій.

Ключовим документом у цій сфері є Конвенція Ради Європи про кіберзлочинність, ратифікована в 2005 році (Конвенція про кіберзлочинність, 2005). Її метою є підвищення ефективності кримінальних розслідувань та судового переслідування, пов'язаних з комп'ютерними системами та даними, шляхом спрощення процедури збору електронних доказів. Частина дослідників виступає за прийняття на рівні ООН універсального міжнародно-правового акта, подібного до Конвенції проти кіберзлочинності, для врегулювання питань міжнародної співпраці у боротьбі з кіберзагрозами. Однак інші фахівці вважають, що механізмів, передбачених Конвенцією Ради Європи 2001 року, достатньо для ефективної протидії кіберзлочинності. Ці механізми спрямовані на вдосконалення кримінальних розслідувань, судового переслідування та полегшення збору електронних доказів (Саєнко, Савела, & Тополянський, 2021).

Європейський Союз впровадив низку правових актів для боротьби з кіберзлочинністю, зокрема Директиву ЄС про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (2016 рік) та Директиву ЄС щодо боротьби з шахрайством та іншими фінансовими злочинами в Інтернеті (2017 рік). Особлива увага в ЄС приділяється своєчасному виявленню та швидкому реагуванню на кіберінциденти й атаки на електронні інформаційні ресурси. Директива ЄС про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу, ухвалена в 2016 році, стала важливим кроком у зміцненні кібербезпеки всередині Європейського Союзу.

Основною метою цієї директиви було встановлення єдиних стандартів безпеки для мережевих та інформаційних систем у державах-членах ЄС. Вона зобов'язала країни створити національні органи, відповідальні за кібербезпеку, та визначити конкретні сектори, критично залежні від інформаційних систем, включаючи енергетику, транспорт, банківську сферу, охорону здоров'я та водопостачання. Директива також запровадила вимогу до операторів основних послуг та провайдерів цифрових послуг повідомляти про серйозні інциденти в своїй інфраструктурі, що дозволяє швидко реагувати на загрози. Одним з аспектів директиви є стимулювання міжнародного співробітництва в сфері кібербезпеки та обмін інформацією між державами-членами для забезпечення колективної кібербезпеки на рівні ЄС. (Про заходи, 2016).

Директива Європейського Союзу щодо боротьби з шахрайством та іншими фінансовими злочинами в Інтернеті, ухвалена в 2017 році, спрямована на боротьбу з кіберзлочинністю, пов'язаною з фінансовими операціями в цифровому просторі. Вона встановлює правову основу для запобігання та протидії фінансовим злочинам в Інтернеті, включаючи крадіжки даних, незаконне використання платіжних засобів, фішинг та інші форми онлайн-шахрайства. Основна увага цієї директиви зосереджена на захисті електронних транзакцій та платіжних систем від кіберзлочинців. Директива також вимагає від держав-членів забезпечити жорстке покарання за кіберзлочини, пов'язані з фінансовими операціями, та стимулювати міжнародну співпрацю для швидкого реагування на загрози в цій сфері. Особливий акцент робиться на забезпеченні безпеки особистих даних користувачів під час фінансових операцій і вдосконаленні механізмів обміну інформацією між країнами щодо кіберзагроз. (Про боротьбу, 2017).

В умовах глобального протистояння та мілітаризації кіберпростору, США залишаються провідною силою у формулюванні та впровадженні кібербезпекової стратегії. Вони підкреслюють важливість національної безпеки через кіберзахист. Стратегія кібербезпеки, опублікована урядом США, визначає кібербезпеку як комплекс заходів для захисту комп'ютерних систем від несанкціонованого доступу. Важливим аспектом є регулювання безпеки на національному рівні, включаючи застосування санкцій та стратегічні партнерства з іншими країнами для спільної боротьби проти кіберзагроз. США активно співпрацюють з країнами-партнерами, такими як Україна, у сфері вдосконалення кібербезпеки.

Нормативні документи, що визначають ключові принципи національної безпеки та оборони, такі як Доктрина інформаційної безпеки та Стратегічний оборонний бюлетень, підкреслюють важливість міжнародної співпраці. Розвиток партнерських відносин з іноземними цивільними та військовими організаціями сприяє обороноздатності та державній безпеці. Це стимулює вітчизняних фахівців до вдосконалення національної моделі державного управління у сфері кібербезпеки на основі вивчення міжнародного досвіду.

Досвід Сполучених Штатів у сфері інформаційної безпеки вважається показовим. США є одним із піонерів у впровадженні електронного урядування

та розробці систем захисту інформаційних ресурсів і національного інформаційного суверенітету. У країні діє кілька ключових установ, які займаються забезпеченням інформаційної безпеки: Агентство національної безпеки (АНБ), Національне управління кібербезпеки, Федеральне бюро розслідувань (ФБР) та Центральне розвідувальне управління (ЦРУ). АНБ, зокрема, активно співпрацює з приватним сектором та науковими установами для протидії загрозам у недержавних комп'ютерних мережах. Президент США відіграє ключову роль у регулюванні сфери кібербезпеки, визначаючи стратегічні напрямки та політики.

Після Другої світової війни, у відповідь на радянську пропаганду, США почали формувати законодавчі основи інформаційної безпеки. З того часу було прийнято комплекс федеральних та штатних законів, які забезпечують захист інформаційного простору країни. Основні з них: Закон "Про охорону особистих таємниць", Закон "Про таємницю", Закон "Про висвітлення діяльності уряду", Закон "Про право на фінансову таємницю", Закон "Про доступ до інформації про діяльність ЦРУ", Закон "Про безпеку комп'ютерних систем" та інші. Ці закони покладають основу для інформаційної безпеки в країні та визначають методи захисту інформації від несанкціонованого доступу та кібератак. (Яковлєв, 2020).

Система кібербезпеки в сучасних країнах є складним комплексом технологічних, організаційних та законодавчих заходів. Вона спрямована на захист національних інтересів у кіберпросторі, захист критичної інфраструктури та інформаційних ресурсів від різноманітних кіберзагроз. Досвід США у цій сфері демонструє важливість комплексного підходу, міжнародної співпраці та постійного вдосконалення законодавчої бази. Для країн, що розвивають власні системи кібербезпеки, вивчення та адаптація такого досвіду є критично важливими для забезпечення національної безпеки та суверенітету в цифрову епоху. Міжнародне співробітництво у сфері кібербезпеки потребує гармонізації кримінального законодавства, розробки нових елементів міжнародного партнерства та підтримки договорів і моделей, таких як Типовий закон ООН про комп'ютерні злочини. Незважаючи на наявність усталених міжнародних конвенцій і постійних зусиль, динамічний характер кіберзагроз потребує безперервної адаптації правової бази та скоординованих дій для ефективної протидії та запобігання кіберзлочинності на глобальному рівні.

З розвитком інформаційних технологій та глобалізацією мережі Інтернет зловмисники отримали безпрецедентні можливості для здійснення атак на державні установи, критичну інфраструктуру та громадян. Ці загрози можуть мати різні форми, але всі вони потенційно здатні завдати значної шкоди як на економічному, так і на політичному рівні. Одним із найпоширеніших видів кіберзагроз є кібершпигунство. Воно полягає у несанкціонованому доступі до конфіденційної інформації з метою її викрадення або використання у власних інтересах. Зловмисники можуть бути як хакерами, так і організованими групами, часто підтримуваними іноземними державами. Викрадена інформація може включати державні таємниці, військові плани, технологічні розробки або персональні дані громадян.

Наприклад, у 2015 році була виявлена масштабна кампанія кібершпигунства, спрямована на урядові установи різних країн, з метою викрадення дипломатичної інформації та стратегічних планів. Кібертероризм є ще одним серйозним викликом. Він передбачає використання комп'ютерних та мережевих технологій для здійснення терористичних актів або сприяння їм. Метою кібертерористів є посіяти паніку, дестабілізувати суспільство або завдати шкоди критичній інфраструктурі. Наприклад, атаки на системи управління міським транспортом можуть призвести до хаосу на дорогах, а втручання в роботу медичних закладів – до загрози життю пацієнтів. Кібертероризм особливо небезпечний тим, що дозволяє зловмисникам діяти анонімно та з будь-якої точки світу. Атаки на критичну інфраструктуру є однією з найбільш руйнівних форм кіберзагроз. (Стівенс, & Бертон, 2023).

Кіберзагрози стають все складнішими і різноманітнішими. У дослідженні 10Guards були виділені основні типи атак 2021 року. Фішинг – одна з найпоширеніших загроз, яка включає spear-phishing, whaling, smishing, vishing, і email phishing. Програми-вимагачі (ransomware) блокують доступ до даних і вимагають викуп. Шкідливе ПЗ (malware) шкодить пристроям та краде інформацію. Витік даних часто спричиняється через погано захищені системи. DDoS-атаки перевантажують сервери, а атаки "Людина посередині" перехоплюють комунікації. Інші загрози включають SQL-ін'єкції, експлойти нульового дня та атаки брутфорс. Організації повинні бути готові до цих загроз, впроваджуючи захисні заходи. (Найпопулярніші види кібератак, 2021).

Атака на українську енергосистему 2015 року залишила понад 200 тисяч людей без електроенергії, підкресливши вразливість інфраструктури. (BBC News Україна, 2017). Вірус NotPetya 2017 року вразив тисячі комп'ютерів, зокрема в Україні, спричинивши значні збитки (Бабель, 2020). Атака на Colonial Pipeline у 2021 році зупинила постачання палива на східне узбережжя США, викликавши паніку і дефіцит (Як хакери зупинили, 2021). Втручання у вибори США 2016 та 2020 років показало, що кіберзагрози можуть мати політичні наслідки. Наслідки кібератак для національної безпеки включають економічні втрати, гуманітарні кризи, загрози життю громадян, та ослаблення обороноздатності. Соціальні наслідки можуть включати поширення дезінформації, паніку і

суспільні заворушення (Сливка, 2022). Для ефективної протидії кіберзагрозам необхідний комплексний підхід. Держави повинні інвестувати у розвиток національних систем кібербезпеки, створювати спеціалізовані органи та підрозділи, що відповідають за захист критичної інфраструктури та державних установ. Необхідно удосконалювати законодавчу базу, встановлюючи чіткі правила та норми поведінки в кіберпросторі. Міжнародна співпраця є ключовим елементом у боротьбі з кіберзлочинністю. Оскільки зловмисники діють глобально, без взаємодії між державами, правоохоронними органами та міжнародними організаціями ефективна протидія неможлива. Необхідно розробляти спільні стандарти безпеки, обмінюватися інформацією та досвідом, проводити спільні навчання та операції.

Важливим є також підвищення обізнаності громадян та приватного сектора про кіберзагрози. Проведення освітніх програм, тренінгів та кампаній з кібергігієни допоможе знизити ризик успішних атак, які часто використовують людський фактор як найслабшу ланку в системі безпеки. У підсумку, кіберзагрози є невід'ємною частиною сучасного світу і становлять серйозну загрозу для національної безпеки. Їхній вплив може бути руйнівним, але за умови правильного підходу та співпраці можливо ефективно протидіяти цим викликам. Забезпечення кібербезпеки має стати пріоритетом для держав, бізнесу та суспільства, адже від цього залежить наше спільне майбутнє у цифрову епоху. (Вдовенко, Живило, Черноног, & Докіль, 2022).

Висновки.

Кібербезпека в умовах глобалізації та інформаційного суспільства виступає ключовим елементом національної безпеки будь-якої держави. З огляду на все більшу залежність державних установ, економічних систем та повсякденного життя громадян від цифрових технологій, кіберзагрози стають одним із головних викликів для стабільності та безпеки держави. Кіберзагрози, такі як кібератаки на критичну інфраструктуру, витоки даних, кібершпигунство та кібертероризм, мають глобальний характер і можуть завдати серйозних економічних та соціальних наслідків. Як свідчать приклади масштабних атак на інфраструктури України, США та інших країн, навіть найбільш розвинені держави вразливі до таких загроз.

Одним з найважливіших аспектів боротьби з кіберзагрозами є міжнародне співробітництво, яке забезпечує обмін інформацією, досвідом та технологіями. Досвід провідних країн у цій сфері свідчить, що ефективна кібербезпека можлива лише завдяки глобальній координації та інтеграції зусиль.

Наприклад, США, які є одним з лідерів у галузі кіберзахисту, створили розгалужену мережу державних установ, таких як Агентство національної безпеки (АНБ) та Національне управління кібербезпеки, які активно співпрацюють із приватним сектором та міжнародними партнерами для виявлення та нейтралізації кіберзагроз. Інші країни також активно впроваджують власні стратегії кібербезпеки. У Європейському Союзі була прийнята Директива про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем, яка передбачає створення єдиних стандартів для держав-членів ЄС у питаннях кібербезпеки. Директива зобов'язує країни створювати національні органи кібербезпеки, визначати сектори критичної інфраструктури та налагоджувати систему повідомлень про інциденти для швидкого реагування на загрози. Важливим є те, що ЄС активно стимулює обмін інформацією між країнами-членами для колективної безпеки кіберпростору.

Міжнародне співробітництво з НАТО є одним з основних напрямків посилення кіберзахисту для багатьох країн, зокрема України. Створення платформ, таких як Платформа Україна – НАТО з протидії гібридній війні, та Цільовий фонд для розвитку кібербезпеки сприяє підвищенню здатності країн реагувати на кіберзагрози та впроваджувати новітні технології для захисту національної інфраструктури. Важливим елементом є участь України в міжнародних навчаннях та операціях, які дозволяють обмінюватися передовими практиками та розробляти спільні заходи протидії загрозам.

Слід зазначити, що міжнародні організації, такі як ООН, також визнають важливість створення глобальних стандартів кібербезпеки. Рішення Групи урядових експертів з міжнародної інформаційної безпеки ООН у 2015 році заклали підґрунтя для застосування міжнародного права до кіберпростору, підкреслюючи необхідність розробки міжнародних норм та правил для регулювання кіберпростору, що є особливо актуальним для країн, які стикаються з систематичними кібератаками. Окрім державних ініціатив, важливу роль відіграє приватний сектор. Багато міжнародних компаній співпрацюють з урядами та міжнародними організаціями у питаннях кібербезпеки. Приватні корпорації займаються розробкою новітніх технологічних рішень, які дозволяють підвищити рівень захисту інформаційних систем та мінімізувати наслідки кіберзагроз. Україна, яка стикається з постійними кібератаками, особливо з боку Росії, активно зміцнює свою національну систему кібербезпеки, впроваджуючи міжнародні стандарти та розвиваючи співпрацю з міжнародними партнерами.

Прийняття Закону України «Про основні засади забезпечення кібербезпеки України» у 2017 році стало важливим кроком у формуванні національної стратегії кіберзахисту. Україна також активно співпрацює з НАТО та ЄС для зміцнення своїх кіберзахисних можливостей. Важливими є освітні програми, які допомагають підвищувати обізнаність

населення та організацій про ризики кіберзагроз. Отже, кібербезпека стає пріоритетом для державної політики кожної країни. Для ефективної протидії кіберзагрозам необхідний комплексний підхід, який включає не лише технологічні рішення, але й правові, організаційні та освітні ініціативи. Міжнародне співробітництво є ключовим фактором у боротьбі з кіберзагрозами, адже лише через спільні зусилля можливо забезпечити стійкий захист національних інтересів у цифровому просторі.

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

Баранов, О. А. (2014). Про тлумачення та визначення поняття "Кібербезпека". *Правова інформатика*, 2(42), 54-62. Відновлено з https://ippi.org.ua/sites/default/files/14boavpk.pdf

Вдовенко, С., Живило, Є., Черноног, О., & Докіль, В. (2022). Аналіз особливостей функціонування системи кібероборони. Нормативно-правові аспекти. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*, 74, 52-72. https://doi.org/10.17721/2519-481X/2022/74-06

Відключення електроенергії в Україні було хакерською атакою. (2016). *BBC News Україна*. Відновлено з https://www.bbc.com/ukrainian/news-38585587#:~:text=Компанія%20з%20кібербезпеки%20Information%20Systems%20Securit%20Partners%20(ISSP),2015%20році.%20Тоді%20це%20зачепило%20225%20тис.%20людей

Ємельянов, В., & Бондар, Г. (2019). Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. *Публічне управління та регіональний розвиток*, 5, 493-523. https://doi.org/10.34132/pard2019.05.02

Конвенція про кіберзлочинність. (2005). *Конвенція Ради Європи*. Відновлено з https://zakon.rada.gov.ua/laws/show/994_575#Text

Ліпкан, В., & Діордіца, І. (2017). Національна система кібербезпеки як складова частина системи забезпечення національної безпеки україни. *Інформаційне право*, 5, 174-180. Відновлено з http://pgp-journal.kiev.ua/archive/2017/5/40.pdf

Найпопулярніші види кібератак у 2021. (2021). Відновлено з https://10guards.com/ua/articles/the-most-common-types-of-cyber-attacks-in-2021/

Несрін, Д., & Радомська, Л. А. (2021). *Сучасний стан кібербезпеки в Україні*. Вінницький національний технічний університет. Відновлено з https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/37987/90562.pdf?sequence=2&isAllowed=y

Про боротьбу з шахрайством, спрямованим проти фінансових інтересів Союзу, кримінально-правовими засобами. № 2017/1371. (2017, Липень 5). *Директива Європейського Парламенту та Ради*. Відновлено з https://zakon.rada.gov.ua/laws/show/984_008-17#Text

Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. № 2016/1148. (2016, Липень 6). *Директива Європейського Парламенту та Ради*. Відновлено з https://zakon.rada.gov.ua/laws/show/984_013-16#Text

Саєнко, М. І., Савела, Є. А., & Тополянський, Ю. Ю. (2021). Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського національного університету. Серія: Право*, 64, 386-391. https://doi.org/10.24144/2307-3322.2021.64.71

Сливка, М. М. (2022). Міжнародне співробітництво у сфері забезпечення кібербезпеки України. *Юридичний науковий електронний журнал*, 10, 489-491. https://doi.org/10.32782/2524-0374/2022-10/121

Сліпченко, Т. (2020). Кібербезпека як складова системи захисту національної безпеки: європейський досвід. *Актуальні проблеми правознавства*, 1(1), 128-133. https://doi.org/10.35774/app2020.01.128

Степко, О. М. (2014). Аналіз головних складових інформаційної безпеки держави. *Інститут міжнародних відносин Національного авіаційного університету. Політологія*, 1(3), 90-99. Відновлено з https://jrnl.nau.edu.ua/index.php/IMV/article/view/3214

Стівенс, Д. Т., & Бертон, Д. Дж. (2023). НАТО і стратегічна конкуренція в кіберпросторі. *НАТО REVIEW, думки, аналіз і обговорення питань безпеки*. Відновлено з https://www.nato.int/docu/review/uk/articles/2023/06/06/nato-strategchna-konkurentsya-v-kberprostor/index.html

Фурашев, В. М. (2012). Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*, 2(5), 162-174. Відновлено з https://ippi.org.ua/sites/default/files/12fvmsvv.pdf

Шеремет, А. (2020, Жовтень 19). *Мін'юст США назвав росіян, які стоять за вірусом NotPetya. У 2017 році він завдав Україні збитків на $500 мільйонів*. Відновлено з http://surl.li/rllqbf

Як хакери зупинили трубопровід у США та до чого це призведе - BBC News Україна. (2021). *BBC News Україна*. Відновлено з https://www.bbc.com/ukrainian/features-57069276

Яковлєв, П. О. (2020). Досвід державного регулювання забезпечення інформаційної безпеки зарубіжних держав (на прикладі Сполучених штатів Америки, Канади, Німеччини, Франції). *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО»*, 30, 106-113. https://doi.org/10.26565/2075-1834-2020-30-13

Dunn Cavelty, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 41(1), 5-32. https://doi.org/10.1080/13523260.2019.1678855

Solar, C. (2020). Cybersecurity and cyber defence in the emerging democracies. *Journal of Cyber Policy*, 5(3), 392-412. https://doi.org/10.1080/23738871.2020.1820546

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). Cybersecurity as a Component of the National Security of the State. *Journal of Security and Sustainability Issues*, 9(3), 775-784. https://doi.org/10.9770/jssi.2020.9.3(4)

REFERENCES

Baranov, O. A. (2014). On the interpretation and definition of the concept of "Cybersecurity". *Legal Informatics*, 2(42), 54-62. Retrieved from https://ippi.org.ua/sites/default/files/14boavpk.pdf

Convention on Cybercrime. (2005). *Council of Europe Convention*. Retrieved from https://zakon.rada.gov.ua/laws/show/994_575#Text

Dunn Cavelty, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 41(1), 5-32. https://doi.org/10.1080/13523260.2019.1678855

Emelyanov, V., & Bondar, G. (2019). Cybersecurity as a component of national security and cyber protection of critical infrastructure of Ukraine. *Public Administration and Regional Development*, 5, 493-523. https://doi.org/10.34132/pard2019.05.02

Furashev, V. M. (2012). Cyberspace and information space, cybersecurity and information security: essence, definition, differences. *Information and Law*, 2(5), 162-174. Retrieved from https://ippi.org.ua/sites/default/files/12fvmsvv.pdf

How hackers stopped a pipeline in the US and what it will lead to - BBC News Ukraine. (2021). *BBC News Ukraine*. Retrieved from https://www.bbc.com/ukrainian/features-57069276

Lipkan, V., & Diorditsa, I. (2017). National Cybersecurity System as a Component of the National Security System of Ukraine. *Information Law*, 5, 174-180. Retrieved from http://pgp-journal.kiev.ua/archive/2017/5/40.pdf

Nesrin, D., & Radomska, L. A. (2021). *Current State of Cybersecurity in Ukraine*. Vinnytsia National Technical University. Retrieved from https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/37987/90562.pdf?sequence=2&isAllowed=y

On measures for a high common level of security of network and information systems across the Union. No. 2016/1148. (2016, July 6). *Directive of the European Parliament and of the Council*. Retrieved from https://zakon.rada.gov.ua/laws/show/984_013-16#Text

On the fight against fraud to the Union's financial interests by criminal law. No. 2017/1371. (2017, July 5). *Directive of the European Parliament and of the Council*. Retrieved from https://zakon.rada.gov.ua/laws/show/984_008-17#Text

Saenko, M. I., Savela, E. A., & Topolyansky, Y. Y. (2021). International experience in combating cybercrime and cyberfraud. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 64, 386-391. https://doi.org/10.24144/2307-3322.2021.64.71

Sheremet, A. (2020, October 19). *The US Department of Justice named the Russians behind the NotPetya virus. In 2017, it caused $500 million in losses to Ukraine*. Retrieved from http://surl.li/rllqbf

Slipchenko, T. (2020). Cybersecurity as a component of the national security protection system: European experience. *Current Problems of Law*, 1(1), 128-133. https://doi.org/10.35774/app2020.01.128

Slyvka, M. M. (2022). International cooperation in the field of ensuring cybersecurity of Ukraine. *Legal Scientific Electronic Journal*, 10, 489-491. https://doi.org/10.32782/2524-0374/2022-10/121

Solar, C. (2020). Cybersecurity and cyber defence in the emerging democracies. *Journal of Cyber Policy*, 5(3), 392-412. https://doi.org/10.1080/23738871.2020.1820546

Stepko, O. M. (2014). Analysis of the Main Components of State Information Security. *Institute of International Relations of the National Aviation University. Political Science*, 1(3), 90-99. Retrieved from https://jrnl.nau.edu.ua/index.php/IMV/article/view/3214

Stevens, D. T., & Burton, D. J. (2023). NATO and Strategic Competition in Cyberspace. *NATO REVIEW, Opinions, Analysis and Discussion of Security Issues*. Retrieved from https://www.nato.int/docu/review/uk/articles/2023/06/06/nato-strategchna-konkurentsya-v-kberprostor/index.html

The Most Popular Types of Cyberattacks in 2021. (2021). Retrieved from https://10guards.com/ua/articles/the-most-common-types-of-cyber-attacks-in-2021/

The power outage in Ukraine was a hacker attack. (2016). *BBC News Ukraine*. Retrieved from https://www.bbc.com/ukrainian/news-38585587#:~:text=Company%20with%20cybersecurity%20Information%20Systems%20Securit%20Partners%20(ISSP),2015%20years.%20Then%20it%20affected%20225%20thousands%20of%20people

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). Cybersecurity as a Component of the National Security of the State. *Journal of Security and Sustainability Issues*, 9(3), 775-784. https://doi.org/10.9770/jssi.2020.9.3(4)

Vdovenko, S., Zhivylo, E., Chernogo, O., & Dokil, V. (2022). Analysis of the features of the functioning of the cyber defense system. Regulatory and legal aspects. *Collection of scientific papers of the Military Institute of the Taras Shevchenko National University of Kyiv*, 74, 52-72. https://doi.org/10.17721/2519-481X/2022/74-06

Yakovlev, P. O. (2020). Experience of state regulation of information security of foreign states (using the example of the United States of America, Canada, Germany, France). *Bulletin of the V. N. Karazin Kharkiv National University. Series "PRAVO"*, 30, 106-113. https://doi.org/10.26565/2075-1834-2020-30-13