УДК: 351.862

https://doi.org/10.52058/3041-1254-2025-11(21)-691-704

Зарубенко Артур Олександрович Начальник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, PhD (доктор філософії) з технічних наук, https://orcid.org/0000-0002-7616-6416

Дєгтяр Олег Андрійович головний науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, доктор наук з державного управління, професор, https://orcid.org/0000-0001-6413-3580

МІЖНАРОДНІ ТА УКРАЇНСЬКІ ДЕРЖАВНІ МЕХАНІЗМИ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ

Анотація. У статті досліджуються сучасні підходи до правового регулювання кібербезпеки на національному та міжнародному рівнях. Особливу увагу приділено аналізу державних механізмів, які забезпечують ефективний захист кіберпростору, враховуючи глобальні виклики та загрози у сфері інформаційної безпеки. Розглядаються ключові міжнародні нормативно-правові акти, що регулюють питання кібербезпеки, зокрема Будапештська конвенція про кіберзлочинність, рекомендації Європейського Союзу, ООН та інших міжнародних організацій.

У контексті українського законодавства досліджуються основні нормативно-правові акти, такі як Закон України "Про основні засади забезпечення кібербезпеки України", а також підзаконні акти, що регламентують діяльність державних органів у цій сфері. Окремо акцентується увага на ролі Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції та інших інституцій, залучених до забезпечення кібербезпеки.

У статті також порівнюються українські механізми правового регулювання з міжнародними практиками, визначаються їхні сильні та слабкі сторони. Особливу увагу приділено питанням гармонізації українського законодавства з європейськими стандартами у сфері кібербезпеки, а також викликам, пов'язаним із впровадженням цих стандартів.

Автори аналізують сучасні тенденції розвитку правового регулювання кібербезпеки, зокрема зростання уваги до захисту критичної інфраструктури, персональних даних та протидії кіберзлочинності. У статті пропонуються рекомендації щодо вдосконалення нормативно-правової бази України у сфері

кібербезпеки з урахуванням міжнародного досвіду та необхідності адаптації до нових кіберзагроз.

Особливу увагу приділено основним державним органам, які відповідають за реалізацію політики у сфері кібербезпеки. Серед них виділяються Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція, Міністерство оборони України, розвідувальні органи та Національний банк України. У статті здійснено аналіз законодавчої бази, що є фундаментом для забезпечення кіберзахисту держави. Основним документом у цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України», а також інші нормативні акти, які регулюють правові та організаційні аспекти боротьби з кіберзлочинністю та забезпечення захисту критичної інфраструктури.

Також розглянуто актуальні програми та стратегії реформування, зокрема «План заходів з реалізації Концепції реформування Державної служби спеціального зв'язку та захисту інформації України на 2024–2025 роки». Цей план передбачає низку заходів, спрямованих на модернізацію національної системи кібербезпеки, розвиток центрів реагування на кіберінциденти, а також підготовку висококваліфікованих фахівців у цій галузі.

Результати дослідження можуть бути корисними для науковців, практиків, а також для представників державних органів, залучених до формування політики у сфері кібербезпеки.

Ключові слова: кібербезпека, правове регулювання, національна безпека, кіберзагрози, державне управління, міжнародні стандарти, критична інфраструктура.

Zarubenko Artur Oleksandrovych Head of Scientific center of communication and information technologies, Kruty Heroes Military Institute of Telecommunications and Information Technologies, PhD (Doctor of Philosophy) of Technical Sciences, https://orcid.org/0000-0002-7616-6416

Diegtiar Oleg Andriyovych chief researcher, Scientific center of communication and information technologies, Kruty Heroes Military Institute of Telecommunications and Information Technologies, doctor of sciences in public administration, professor, https://orcid.org/0000-0001-6413-3580

INTERNATIONAL AND UKRAINIAN STATE MECHANISMS OF LEGAL REGULATION OF CYBERSECURITY

Abstract. The article explores modern approaches to legal regulation of cybersecurity at both national and international levels. Special attention is given to analyzing state mechanisms that ensure effective protection of cyberspace, considering

global challenges and threats in the field of information security. Key international regulations addressing cybersecurity issues are examined, including the Budapest Convention on Cybercrime, as well as recommendations from the European Union, the United Nations, and other international organizations.

In the context of Ukrainian legislation, the main regulatory acts are investigated, such as the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine," along with subordinate legislations regulating the activities of state bodies in this field. The article specifically highlights the roles of the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Police, and other institutions involved in ensuring cybersecurity.

Additionally, the article compares Ukrainian legal regulation mechanisms with international practices, identifying their strengths and weaknesses. It places particular emphasis on harmonizing Ukrainian legislation with European standards in the field of cybersecurity, as well as the challenges associated with implementing these standards.

The authors analyze current trends in the development of legal regulation of cybersecurity, particularly the increasing focus on protecting critical infrastructure, personal data, and combating cybercrime. Recommendations are offered for improving Ukraine's regulatory framework in the field of cybersecurity, considering international experience and the need to adapt to new cyber threats.

Special attention is given to the main state bodies responsible for implementing cybersecurity policy. These include the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Police, the Ministry of Defense of Ukraine, intelligence agencies, and the National Bank of Ukraine. The article analyzes the legislative framework that serves as the foundation for ensuring the country's cyber defense. The primary document in this area is the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine," along with other regulations that govern the legal and organizational aspects of combating cybercrime and protecting critical infrastructure.

Relevant reform programs and strategies are also examined, including the "Action Plan for Implementing the Concept of Reforming the State Service of Special Communications and Information Protection of Ukraine for 2024–2025." This plan outlines a series of measures aimed at modernizing the national cybersecurity system, developing centers for responding to cyber incidents, and training highly qualified specialists in this field.

The research findings may be beneficial for scholars, practitioners, and representatives of state bodies involved in formulating cybersecurity policy.

Keywords: cybersecurity, legal regulation, national security, cyber threats, public administration, international standards, critical infrastructure.

Постановка проблеми. У сучасних умовах стрімкого розвитку інформаційних технологій кібербезпека набуває критичного значення для держав, орга-

нізацій та окремих громадян. Зростання кількості кіберзагроз, атак на критичну інфраструктуру, викрадення персональних даних та фінансових ресурсів створює серйозні виклики для забезпечення стабільності та безпеки інформаційного простору. Особливо актуальною ця проблема є для України, яка, перебуваючи в умовах гібридної війни, стикається із постійними спробами порушення функціонування державних систем, зокрема через кібератаки з боку ворожих сил.

Попри наявність нормативно-правової бази та створення спеціалізованих державних органів, таких як Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України та інші, залишається низка невирішених питань. Серед них – недостатній рівень координації між інституціями, обмежені ресурси для модернізації кіберінфраструктури, недостатня кількість кваліфікованих кадрів та низький рівень адаптації до міжнародних стандартів у сфері кіберзахисту.

Крім того, існує необхідність удосконалення механізмів правового регулювання кібербезпеки, що включає гармонізацію українського законодавства з європейськими та міжнародними нормами. Забезпечення ефективного захисту критичної інфраструктури, розробка дієвих стратегій протидії кіберзлочинності, а також формування культури кібербезпеки серед населення є ключовими завданнями, які потребують комплексного підходу.

Таким чином, проблема правового регулювання кібербезпеки є багатогранною і потребує системного аналізу, спрямованого на вдосконалення законодавчої бази, підвищення ефективності роботи державних органів та інтеграцію міжнародного досвіду задля забезпечення стійкості українського кіберпростору.

Аналіз останніх досліджень і публікацій. Проблематика кібербезпеки та її нормативно-правового регулювання отримала широке висвітлення як у вітчизняних, так і зарубіжних наукових та правових джерелах. Основу досліджень становлять ключові законодавчі акти України, зокрема Закон «Про основні засади забезпечення кібербезпеки України» [1], Закон «Про захист інформації в інформаційно-комунікаційних системах» [2], Закон «Про захист персональних даних» [3], Стратегія кібербезпеки України (2021) [4] та План заходів на 2025 рік з реалізації Стратегії кібербезпеки України [5].

Важливий внесок у формування теоретико-правових основ зроблено у працях таких дослідників, як Б. Кормич [6], А. Марущак [7], А. Семенченко [8], В. Плескач [9] та інших, які розглядали організаційно-правові аспекти забезпечення кіберзахисту. У сфері державного управління значну увагу приділено роботам О. Потія [8], Д. Мялковського [8] та С. Кравченка [10], які акцентували на необхідності інституційного розвитку та реформування системи кібербезпеки.

Зарубіжний досвід детально аналізується у дослідженнях, що стосуються виконання міжнародних угод, таких як Будапештська конвенція про кіберзлочинність [11], резолюції ООН [15], директиви ЄС NIS та NIS2 [12], а також у практиках НАТО та ENISA, спрямованих на розвиток систем реагування на кіберінциденти.

Наукові статті Ю. Яковенка [16], Ю. Деркаченка [16], В. Гавриляка [17] та Ю. Третяка [18] зосереджені на аналізі викликів інтеграції України до європейського кіберпростору, співпраці з міжнародними організаціями та перспектив державного управління у цій сфері.

Проте, попри значні напрацювання у законодавчому регулюванні, науковці наголошують на потребі вдосконалення правових механізмів, посилення координації між суб'єктами кібербезпеки та впровадження новітніх підходів до захисту критичної інфраструктури.

Мета статті - Метою статті є аналіз сучасного стану нормативно-правового забезпечення кібербезпеки в Україні, визначення ключових проблем та викликів у цій сфері, а також формулювання пропозицій щодо вдосконалення правових механізмів для забезпечення ефективного захисту інформаційного простору. Особлива увага приділяється інтеграції міжнародного досвіду, адаптації українського законодавства до європейських стандартів, а також розробці інноваційних підходів до захисту критичної інфраструктури та координації дій між суб'єктами системи кібербезпеки.

Виклад основного матеріалу. Національна система кібербезпеки України є комплексною структурою, яка об'єднує організаційні суб'єкти, а також правові, технічні та управлінські заходи, спрямовані на забезпечення захисту національних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури. Вона інтегрує політичні, науково-технічні, правові, оборонні, криптографічні та організаційно-управлінські інструменти, які дозволяють ефективно протидіяти кіберзагрозам. Система включає в себе не лише заходи з попередження та виявлення кібератак, але й оперативне реагування на інциденти, а також забезпечення захисту інформації від несанкціонованого доступу.

На рівні інституцій визначено основних суб'єктів, відповідальних за функціонування системи кібербезпеки. До них належать Державна служба спеціального зв'язку та захисту інформації України, Національна поліція, Служба безпеки України, Міністерство оборони України, Генеральний штаб, розвідувальні органи та Національний банк України. Ці установи займаються реалізацією державної політики у сфері кіберзахисту, протидією кіберзлочинам, захистом критичної інфраструктури та запобіганням кібертероризму.

Діяльність національної системи кібербезпеки базується на постійному вдосконаленні нормативно-правової бази, гармонізації із міжнародними стандартами Європейського Союзу та НАТО, підготовці фахівців, створенні та розвитку центрів швидкого реагування на кіберінциденти, а також на тісній співпраці між державними структурами та приватним сектором. Значну роль у координації цих процесів відіграє Державний центр кіберзахисту [19], який відповідає за функціонування національної мережі реагування на комп'ютерні інциденти (CERT-UA) та здійснює аудит кіберзахисту об'єктів критичної інфраструктури.

У червні 2025 року в Україні було відкрито Кіберцентр UA30 [20], що став важливим елементом посилення національної системи кібербезпеки. Цей сучасний центр було створено за ініціативи Міністерства цифрової трансформації України у співпраці з міжнародними організаціями та стратегічними партнерами, з метою посилення спроможностей держави у протидії кіберзагрозам.

Кіберцентр UA30 є важливим компонентом системи цифрового захисту України, створеним для протидії зростанню кількості кібератак, які спрямовані на державні установи, об'єкти критичної інфраструктури та персональні дані громадян. Його робота охоплює низку ключових напрямів, які забезпечують комплексний підхід до кіберзахисту:

Реагування на інциденти – здійснення моніторингу, виявлення та оперативної нейтралізації кібератак у режимі реального часу.

Аналіз загроз – вивчення векторів атак, прогнозування потенційних ризиків і кіберзагроз.

Підготовка кадрів – створення навчальних платформ для підвищення кваліфікації українських фахівців у сфері кібербезпеки.

Захист громадян – популяризація принципів кібергігієни та впровадження заходів для захисту персональних даних.

Технічна інфраструктура UA30 включає сучасне обладнання, зокрема серверні комплекси, аналітичні системи, інструменти для виявлення атак, а також платформи для моделювання та симуляції кіберзагроз. Основні напрями діяльності центру спрямовані на:

забезпечення захисту національних цифрових реєстрів і критично важливих об'єктів;

координацію роботи із Службою безпеки України, Державною службою спеціального зв’язку та захисту інформації України, а також CERT-UA;

підтримку інформаційної та цифрової безпеки в умовах гібридної війни.

Інноваційний підхід до роботи Кіберцентру UA30 дозволяє ефективно реагувати на сучасні виклики у сфері кіберзахисту та зміцнювати обороноздатність держави в цифровому просторі.

Стратегічна роль Кіберцентру UA30 виходить за межі суто технологічного спрямування. Він функціонує як багатофункціональна платформа, яка об’єднує зусилля державних установ, приватного сектору та громадського суспільства для зміцнення кібербезпеки країни.

У сучасних умовах, коли кіберзагрози стають рівнозначними традиційним воєнним викликам, створення таких інноваційних центрів є не лише важливим етапом розвитку, але й основою для забезпечення цифрового суверенітету та стабільності держави.

Протягом останніх років в Україні було розроблено та впроваджено низку нормативно-правових актів, які формують законодавчу базу для кіберзахисту. Особлива увага приділяється адаптації національного законодавства до

міжнародних стандартів, що є важливим кроком для інтеграції України до європейського безпекового простору.

Основним законодавчим актом у цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України». Документ визначає правові та організаційні основи функціонування національної системи кібербезпеки, формулює ключові напрями державної політики та встановлює механізми взаємодії між державними органами, бізнесом і громадськими організаціями для захисту кіберпростору.

Закон закріплює такі основні положення:

визначення суб'єктів національної системи кібербезпеки, до яких належать органи виконавчої влади, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації, Національна поліція, Міністерство оборони та інші уповноважені структури;

принципи забезпечення кібербезпеки, серед яких верховенство права, пріоритет захисту прав людини, інтеграція заходів безпеки та партнерська співпраця з приватним сектором і міжнародними організаціями;

механізми координації дій державних органів з метою запобігання, виявлення та нейтралізації кібератак;

зобов'язання державних структур щодо впровадження заходів для захисту інформаційних систем, зменшення ризиків несанкціонованого доступу до даних та забезпечення відновлення систем після інцидентів.

Особлива увага приділяється захисту критичної інформаційної інфраструктури, яка є стратегічно важливою для національної безпеки. У цьому контексті закон передбачає проведення аудитів, моніторинг, звітність та розвиток державно-приватного партнерства для посилення стійкості цифрового середовища. Закон «Про основні засади забезпечення кібербезпеки України» є концептуальною основою для створення сучасної системи кіберзахисту, на базі якої розробляються підзаконні акти, державні стратегії та спеціалізовані програми.

Рішення РНБО України від 14 травня 2021 року «Про Стратегію кібербезпеки України», затверджене Указом Президента від 26 серпня 2021 року № 447/2021, визначає стратегічний курс держави у сфері кіберзахисту.

У Стратегії кібербезпека визначається як один із пріоритетів національної безпеки. Документ передбачає створення ефективної системи реагування на кіберзагрози, зміцнення кіберстійкості та інтеграцію України до стандартів ЄС і НАТО. Серед основних викликів, на яких акцентується увага, виділяються: зростання значення кіберпростору як нової арени протистояння, загроза кібервійськових дій, активність держав-агресорів та використання кіберінструментів у інформаційно-психологічних операціях.

Стратегія визначає такі ключові завдання: формування системи кібероборони; протидія кіберзлочинності; забезпечення кіберстійкості; розвиток кадрового та науково-технічного потенціалу; зміцнення координації між державними структурами; активна співпраця з міжнародними партнерами.

До основних заходів, передбачених Стратегією, належать створення Національного координаційного центру кібербезпеки при РНБО, розвиток системи управління кіберінцидентами, впровадження оцінки ризиків, проведення аудитів інформаційної безпеки, реалізація науково-дослідних програм, удосконалення системи підготовки фахівців та стимулювання державно-приватного партнерства.

Проте реалізація Стратегії стикається з низкою проблем, серед яких недостатня координація між установами, обмеженість фінансових ресурсів і кадрового забезпечення, а також відсутність чітких показників виконання. У документі зазначається, що попередня Стратегія 2016 року була реалізована лише частково (менше ніж на 40 %) через нестачу ресурсів та інституційної підтримки.

Стратегія 2021 року враховує попередні помилки, інтегрує міжнародні стандарти та пропонує більш чіткі механізми управління кібербезпекою, що дозволяє ефективніше реагувати на сучасні виклики.

Розпорядження Кабінету Міністрів України № 204-р «Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України», ухвалене 7 березня 2025 року, визначає детальний перелік кроків та заходів, спрямованих на практичне впровадження положень Стратегії кібербезпеки протягом зазначеного періоду.

Документ охоплює широкий спектр напрямів, серед яких модернізація інфраструктури кіберзахисту державних органів, впровадження систем для виявлення вразливостей та реагування на кіберінциденти, розвиток кадрового потенціалу через навчання і сертифікацію, удосконалення законодавчої бази, створення систем моніторингу та аудиту, а також посилення співпраці з приватним сектором і громадянським суспільством. У плані передбачено конкретну черговість виконання заходів, часові рамки, відповідальних виконавців, необхідні ресурси та критерії оцінки успішності.

Особливу увагу приділено розвитку Національного центру резервування державних інформаційних ресурсів, розгортанню систем швидкого реагування на інциденти (CSIRT), забезпеченню кібергігієни серед працівників державних установ, а також вдосконаленню механізмів безпечного доступу державних органів до мережі Інтернет.

Цей нормативний акт відіграє ключову роль у переході від загальних стратегічних завдань до їх практичного виконання, оскільки деталізує операційні кроки, визначає відповідальних за реалізацію та забезпечує контроль за виконанням заходів.

Серед важливих документів у сфері кібербезпеки варто також виділити «План заходів з реалізації Концепції реформування Державної служби спеціального зв'язку та захисту інформації України на 2024–2025 роки». Цей документ спрямований на вдосконалення організаційної структури та функціональних можливостей Держспецзв'язку, адаптуючи її діяльність до сучасних викликів у сфері кіберзахисту та інформаційної безпеки.

План заходів визначає три основні стратегічні цілі:

Зміцнення захисту державних інформаційних ресурсів шляхом впровадження новітніх технологій криптографічного захисту, багатофакторної автентифікації та управління доступом;

Зниження ризиків несанкціонованого доступу до конфіденційної інформації через модернізацію систем моніторингу та аудиту кіберінцидентів;

Розвиток національної інфраструктури кіберзахисту, включно зі створенням резервних центрів обробки даних, оновленням державних реєстрів та активізацією співпраці з міжнародними партнерами.

Документ передбачає низку конкретних заходів, таких як цифрова трансформація ключових сервісів Держспецзв'язку, впровадження системи управління ризиками відповідно до міжнародних стандартів ISO/IEC 27001, створення механізмів реагування на кіберінциденти (CERT-UA), а також підготовка фахівців з кіберзахисту за сучасними навчальними програмами.

Важливим аспектом є забезпечення стійкості державного сектору до кібератак. План передбачає модернізацію мережевої інфраструктури, впровадження технологій «Zero Trust», посилення кібергігієни серед працівників державних органів та створення національної системи раннього виявлення кіберзагроз.

Реалізація зазначеного плану спрямована на створення комплексної системи управління кіберризиками, яка відповідає міжнародним стандартам та забезпечує стабільну роботу державних органів навіть в умовах гібридних загроз. Активний розвиток цифрових технологій у державному управлінні та впровадження електронних сервісів формують нові вимоги до захисту хмарних середовищ, які набувають популярності серед державних установ і приватних компаній.

У цьому контексті важливу роль відіграють рекомендації міжнародних експертів, зокрема компанії KPMG, які акцентують увагу на необхідності комплексного підходу до кібербезпеки. Серед основних інструментів вони виділяють багатофакторну автентифікацію, яка зменшує ризики несанкціонованого доступу; шифрування даних як під час їх зберігання, так і передачі; а також впровадження сучасних технологій для управління доступом і контролю.

Застосування таких заходів дозволяє значно підвищити захищеність хмарних інфраструктур та забезпечити збереження конфіденційної інформації в умовах зростаючих кіберзагроз.

Адаптація українського законодавства до європейських директив NIS (2016) та NIS2 (2022) є важливим кроком у зміцненні національної системи кібербезпеки. Директива NIS заклала основу для створення спільних стандартів кіберзахисту серед держав-членів ЄС, тоді як NIS2 суттєво розширила вимоги до захисту критичної інформаційної інфраструктури, розробки стратегій реагування та підвищення відповідальності операторів ключових послуг. Імплементація цих норм в Україні сприяє не лише підвищенню рівня захисту державних і приватних ресурсів, а й інтеграції країни до європейської системи кіберстійкості.

Україна активно розвиває міжнародну співпрацю у сфері кібербезпеки, беручи участь у спільних програмах та навчаннях з ЄС, НАТО, Європейським агентством з мережевої та інформаційної безпеки (ENISA), ООН, ОБСЄ та Інтерполом. Це дає змогу отримати доступ до передових методик боротьби з кіберзагрозами, обмінюватися досвідом і впроваджувати сучасні технологічні рішення у національну практику.

Міжнародні стандарти також відіграють важливу роль у побудові ефективної архітектури кіберзахисту. Наприклад, стандарт ISO/IEC 27001 пропонує універсальні принципи управління інформаційною безпекою, які охоплюють процеси оцінки ризиків, моніторинг кіберзагроз, планування заходів реагування та постійне вдосконалення систем захисту.

Спільні навчання та тренінги з міжнародними партнерами відіграють ключову роль у підвищенні ефективності кіберзахисту. Такі заходи сприяють: Підвищенню професійного рівня фахівців через практичні симуляції кібератак. Наприклад, участь України у найбільших навчаннях НАТО з кібероборони — Cyber Coalition, які відбулися в Таллінні наприкінці листопада – початку грудня 2021 року. Сценарії навчань включали атаки на критично важливу інфраструктуру, такі як енергетичні підстанції, системи водопостачання та комунікації. Це дозволило українським експертам оцінити свою готовність до реагування у змішаних умовах (онлайн і офлайн), налагодити взаємодію з партнерами та розробити оперативні алгоритми дій [21].

Ознайомленню з найкращими міжнародними практиками у сфері кібербезпеки. Зокрема, участь України у щорічних змаганнях НАТО з кіберзахисту — Locked Shields, які проходять в Естонії. У рамках цих тренінгів українські спеціалісти отримали можливість вивчити підходи інших країн до реагування на кіберзагрози, цифрової криміналістики, використання інструментів для виявлення атак і адаптації захисних систем. Цей досвід допоміг удосконалити власні протоколи реагування [22].

Налагодженню взаємодії між державним і приватним секторами. У листопаді 2024 року Україна провела стратегічні командно-штабні навчання та практичні змагання з кібербезпеки для балканських країн — Cyber Resilience Strategies та Regional Cyber Shield (CTF). У заходах брали участь представники державних органів, приватних компаній, технологічних стартапів і неурядових

організацій із кількох країн регіону. Навчання включали моделювання масштабних кібератак на енергетичний і телекомунікаційний сектори, що супроводжувалися порушенням комунікаційних каналів. Це сприяло зміцненню співпраці між державними установами та приватним сектором у сфері обміну інформацією та спільного реагування.

Водночас міжнародна співпраця та проведення навчань стикаються з певними викликами:

Різниця в законодавстві країн. Юридичні підходи до класифікації кіберзлочинів, обмеження доступу до даних або їх обміну можуть ускладнювати проведення спільних навчань і взаємодію в кризових ситуаціях.

Ризик залежності від зовнішніх партнерів. Використання технологій або програмного забезпечення, яке контролюється іншими країнами чи корпораціями, може створювати ризики для цифрового суверенітету. Якщо законодавство або інфраструктура країни не адаптовані до таких умов, це може призвести до залежності державних даних або ключових ресурсів від зовнішніх суб'єктів.

Україна має міцну нормативно-правову базу для кіберзахисту, але для ефективної протидії сучасним загрозам необхідно її вдосконалення. Основними пріоритетами є:

Захист критичної інфраструктури через впровадження принципів «zero trust» та проведення регулярних аудитів безпеки.

Розвиток кадрового потенціалу, включаючи підтримку навчальних програм, сертифікацію фахівців і участь у міжнародних тренінгах.

Зміцнення державно-приватного партнерства через обмін інформацією, спільні проєкти та стандарти безпеки.

Інтеграція в міжнародні ініціативи, участь у директивах, програмах альянсів та глобальних проєктах із кібербезпеки для використання накопиченого досвіду та передових стандартів.

Висновки. Сфера кібербезпеки в Україні перебуває на етапі активного становлення, що супроводжується гармонізацією національного законодавства з європейськими стандартами та інтеграцією у глобальний безпековий простір. Законодавчі акти, такі як Закон України «Про основні засади забезпечення кібербезпеки України», а також Стратегія кібербезпеки та відповідні програми її реалізації, формують основу для захисту критично важливих об'єктів інфраструктури та створення ефективної системи кіберзахисту.

Подальший розвиток у цій сфері залежить від зміцнення інституційної спроможності, оновлення технічних засобів, підвищення кваліфікації фахівців та розширення міжнародної співпраці. Ці заходи сприятимуть підвищенню ефективності державної політики у сфері кібербезпеки та забезпеченню надійного захисту національних інтересів у цифровому середовищі.

Література:

1. Про основні засади забезпечення кібербезпеки України. Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Про захист інформації в інформаційно-комунікаційних системах. Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

3. Про захист персональних даних. Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17

4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". Указ Президента України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text

5. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України. Розпорядження Кабінету Міністрів України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text

6. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: дис. … д-ра юрид. наук. 12.00.07. Харків, 2004.

7. Марущак А.І. Пріоритети розвитку інформаційного права України. Інформація і право. 2011.

8. Потій О., Семенченко А., Бакалинський О., Мялковський Д. Публічне управління інституціональним розвитком у сфері кіберзахисту. Науковий вісник: Державне управління. 2021. № 3(9). С. 136–162. DOI: 10.32689/2618-0065-2021-3(9)-136-162.

9. Семенченко А.І., Плескач В.Л., Заярний О.А., Плескач М.В. Організаційно-правові механізми державного управління забезпеченням кібербезпеки та кіберзахисту України: сутність, стан та перспективи розвитку. 2020.

10. Кравченко С.О. Державно-управлінські реформи: теоретико-методологічне обґрунтування та напрями впровадження : монографія. Київ : НАДУ, 2008. 296 с.

11. Конвенція про кіберзлочинність. Будапешт. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/994_575#Text

12. Directive (EU) 2022/2555 of the European Parliament (NIS2). 2022. [Електронний ресурс]. Режимдоступу:https://eur-lex.europa.eu/legalcontent/en/TXT/?uri=CELEX%3A32022L 2555

13. Cybersecurity of Critical Infrastructure in Ukrainian Legislation and in Directive (EU) 2022/2555. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/375323482_Cybersecurity_of_Critical_Infrastructure_in_Ukrainian_Legislation_and_in_Directive_EU_20222555

14. ISO/IEC 27001:2022. [Електронний ресурс]. Режим доступу: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

15. Резолюція Генеральної Асамблеї ООН A/RES/70/237. 2015. [Електронний ресурс]. Режим доступу: https://undocs.org/Home/Mobile?FinalSymbol=A%2Fres%2F70%2F237& Language=E&DeviceType=Desktop&LangRequested=False

16. Яковенко Ю.Л., Деркаченко Ю.В., Кухтик С.В., Березовський Д.О. Шляхи удосконалення системи кібербезпеки в Україні. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. 2021. № 1. DOI: 10.54929/pmtl-issue1-2021-13.

17. Гавриляк В.Б. Стратегія кібербезпеки ЄС (2021) на цифрове десятиліття: перспективи для України. Вісник Національної академії державного управління при Президентові України. Серія: Державне управління. 2021. № 1. С. 46–52.

18. Третяк Ю. Система суб'єктів адміністративно-правового забезпечення кібербезпеки. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2024. Т. 11. № 2 (42). С. 197–205.

19. Державний центр кіберзахисту. [Електронний ресурс]. Режим доступу: https://scpc.gov.ua/uk

20. Кіберцентр UA30. [Електронний ресурс]. Режим доступу: https://inspect.in.ua/vukrayini-vidkryly-kiberczentr-ua30-novu-forteczyu-na-czyfrovomu-fronti/

21. Ukrainian cyber experts lend skills to NATO's largest-ever digital warfare drills in Estonia. [Електронний ресурс]. Режим доступу: Ukraine joins in NATO's biggest cyber defense drills to fortify cooperation against shared threats / The New Voice of Ukraine

22. Ukraine to participate in large-scale NATO cyber defense exercises . [Електронний ресурс]. Режим доступу: Ukraine to participate in large-scale NATO cyber defense exercises

References:

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the Basic Principles of Ensuring Cybersecurity of Ukraine]. Zakon Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

2. Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh [On the Protection of Information in Information and Communication Systems]. Zakon Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text [in Ukrainian].

3. Pro zakhyst personalnykh danykh [On the Protection of Personal Data]. Zakon Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17 [in Ukrainian].

4. Pro rishennia RNBO Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy" [On the Decision of the NSDC of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"]. Ukaz Prezydenta Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].

5. Pro zatverdzhennia planu zakhodiv na 2025 rik z realizatsii Stratehii kiberbezpeky Ukrainy [On Approval of the Action Plan for 2025 for the Implementation of the Cybersecurity Strategy of Ukraine]. Resolution of the Cabinet of Ministers of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text [in Ukrainian].

6. Kormych, B.A. (2004). Orhanizatsiino-pravovi osnovy polityky informatsiinoi bezpeky Ukrainy [Organizational and Legal Foundations of Ukraine's Information Security Policy]. Doctoral dissertation, Kharkiv. [in Ukrainian].

7. Marushchak, A.I. (2011). Priorytety rozvytku informatsiinoho prava Ukrainy [Priorities of the Development of Information Law in Ukraine]. Informatsiia i pravo. [in Ukrainian].

8. Potii, O., Semenchenko, A., Bakalynskyi, O., & Mialkovskyi, D. (2021). Publichne upravlinnia instytutsionalnym rozvytkom u sferi kiberzakhystu [Public Administration of Institutional Development in the Field of Cybersecurity]. Naukovyi visnyk: Derzhavne upravlinnia, 3(9), 136–162. https://doi.org/10.32689/2618-0065-2021-3(9)-136-162 [in Ukrainian].

9. Semenchenko, A.I., Pleskach, V.L., Zaiarnyi, O.A., & Pleskach, M.V. (2020). Orhanizatsiino-pravovi mekhanizmy derzhavnoho upravlinnia zabezpechenniam kiberbezpeky ta kiberzakhystu Ukrainy: sutnist, stan ta perspektyvy rozvytku [Organizational and Legal Mechanisms of Public Administration in Ensuring Cybersecurity and Cyber Defense of Ukraine: Essence, State and Prospects for Development]. [in Ukrainian].

10. Kravchenko, S.O. (2008). Derzhavno-upravlinski reformy: teoretyko-metodolohichne obgruntuvannia ta napriamy vprovadzhennia [Public Administration Reforms: Theoretical and Methodological Justification and Directions for Implementation]. Kyiv: NADU. [in Ukrainian].

11. Konventsiia pro kiberzlochynnist [Convention on Cybercrime]. Budapest. Retrieved from https://zakon.rada.gov.ua/laws/show/994_575#Text [in Ukrainian].

12. Directive (EU) 2022/2555 of the European Parliament (NIS2). (2022). Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555 [in EU].

13. Cybersecurity of Critical Infrastructure in Ukrainian Legislation and in Directive (EU) 2022/2555. (2023). Retrieved from https://www.researchgate.net/publication/375323482_Cyber security_of_Critical_Infrastructure_in_Ukrainian_Legislation_and_in_Directive_EU_20222555 [in EU].

14. ISO/IEC 27001:2022. (2022). Retrieved from https://www.iso.org/obp/ui/en/#iso:std:isoiec:27001:ed-3:v1:en [in EU].

15. UN General Assembly. (2015). Resolution A/RES/70/237. Retrieved from https://undocs.org/Home/Mobile?FinalSymbol=A%2Fres%2F70%2F237&Language=E&DeviceTy pe=Desktop&LangRequested=False [in EU].

16. Yakovenko, Yu.L., Derkachenko, Yu.V., Kukhtyk, S.V., & Berezovskyi, D.O. (2021). Shliakhy udoskonalennia systemy kiberbezpeky v Ukraini [Ways to Improve the Cybersecurity System in Ukraine]. Problemy suchasnykh transformatsii. Seriia: pravo, publichne upravlinnia ta administruvannia, 1. https://doi.org/10.54929/pmtl-issue1-2021-13 [in Ukrainian].

17. Havryliak, V.B. (2021). Stratehiia kiberbezpeky YeS (2021) na tsyfrove desiatylittia: perspektyvy dlia Ukrainy [EU Cybersecurity Strategy (2021) for the Digital Decade: Prospects for Ukraine]. Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy. Seriia: Derzhavne upravlinnia, 1, 46–52 [in Ukrainian].

18. Tretiak, Yu. (2024). Systema subiektiv administratyvno-pravovoho zabezpechennia kiberbezpeky [System of Subjects of Administrative and Legal Support of Cybersecurity]. Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Seriia: Yurydychni nauky, 11(2), 197–205 [in Ukrainian].

19. Derzhavnyi tsentr kiberzakhystu [State Cyber Defense Center]. Retrieved from https://scpc.gov.ua/uk [in Ukrainian].

20. Kibercentr UA30 [Cyber Center UA30]. Retrieved from https://inspect.in.ua/v-ukrayinividkryly-kiberczentr-ua30-novu-forteczyu-na-czyfrovomu-fronti/ [in Ukrainian].

21. Ukrainian cyber experts lend skills to NATO's largest-ever digital warfare drills in Estonia. Retrieved from Ukraine joins in NATO's biggest cyber defense drills to fortify cooperation against shared threats / The New Voice of Ukraine [in EU].

22. Ukraine to participate in large-scale NATO cyber defense exercises. Retrieved from Ukraine to participate in large-scale NATO cyber defense exercises [in EU].