УДК 004.056.5:343.326

ГОРУН О.Ю., головний науковий співробітник Українського науково-дослідного Інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-0447-1729.

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

Анотація. *Стаття присвячена аналізу правового забезпечення національної системи кібербезпеки. Аналізуються прийняті за період незалежності України законодавчі акти у сфері забезпечення кібербезпеки. Розглядаються ключові етапи формування національної системи кібербезпеки. Досліджується законодавчий досвід ЄС та НАТО у сфері забезпечення кібербезпеки. Звертається увага на заходи Стратегії кібербезпеки України, які сьогодні залишаються нереалізованими. Визначаються основні напрямки правового забезпечення формування національної системи кібербезпеки.*

Ключові слова*: законодавство, кібербезпека, національна система кібербезпеки, об'єкти критичної інфраструктури, правове забезпечення.*

Summary. *The article is devoted to the legal support of the national cyber security system. Contains an analysis of legislative acts adopted during the period of Ukraine's independence in the field of cyber security. The key stages of the formation of the national cyber security system are considered. The legislative experience of the EU and NATO in the field of ensuring cyber security is studied. Measures of the Cybersecurity Strategy of Ukraine, which remain unimplemented today, are analyzed. The main directions of legal support for the formation of the national cyber security system are defined.*

Keywords: *legislation, cyber security, national cyber security system, critical infrastructure objects, legal support.*

Постановка проблеми. Стратегія кібербезпеки України проголошує, що "Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі" [1]. Цей пріоритет зумовлює потребу розробки, впровадження та удосконалення правових основ забезпечення національної системи кібербезпеки для протидії кіберзагрозам.

За роки реалізації попередньої Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.16 р. № 96, було докладено значних зусиль до становлення та розвитку національної системи кібербезпеки. Водночас визнається: "відсутність належної державної підтримки розвитку її інституційного забезпечення, недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського законодавства" [1].

Результати аналізу наукових публікацій. Правове забезпечення національної системи кібербезпеки досліджували у своїх роботах О. Алексеєва [2], О. Довгань [3], Д. Доронін, І. Діордіца [4], Ю. Когут [5], С. Кондратов [6], В. Ліпкан [4], О. Суходоля [6], П. Рогов [7], Н. Ткачук [8] та ін.

Водночас, залишаються недостатньо вивченими правові засади функціонування національної системи кібербезпеки в умовах воєнного стану, особливо після повномасштабного збройного вторгнення рф. Важливим є врахування попереднього досвіду побудови такої системи на національному та міжнародному рівні. Корисним в контексті формування цієї системи є відповідний законодавчий досвід ЄС та НАТО. Під цим кутом зору заслуговують на увагу Стратегія кібербезпеки ЄС на цифрове десятиліття, стратегії кібербезпеки країн-членів НАТО. Викладені обставини зумовлюють актуальність цієї статті.

Метою статті є удосконалення правового забезпечення національної системи кібербезпеки на підставі аналізу чинного законодавства з питань забезпечення кібербезпеки України, а також стратегічних документів ЄС та НАТО з цих питань.

Виклад основного матеріалу. Як вже зазначалося, серед передумов та чинників, які формують кіберзагрози, привертає увагу недосконалість нормативно-правової бази у сфері кібербезпеки, повільна імплементація стандартів ЄС і НАТО з питань кібербезпеки, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері. Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації цієї Стратегії кібербезпеки України [1].

Ще до повномасштабного збройного вторгнення рф Україна зробила низку кроків, спрямованих на формування національної системи кібербезпеки. Верховна Рада України ухвалила низку законодавчих актів з питань захисту об'єктів критичної інфраструктури.

Одним із перших нормативних актів у цій царині є прийнятий ще у 1994 році Закон України "Про захист інформації в інформаційно-комунікаційних системах", який регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах [9].

На початку 2000-х років відбулися зміни у формуванні національної системи кібербезпеки, пов'язані із нагальною потребою захисту державних інформаційних ресурсів. Протягом 2002 – 2006 років Урядом України затверджено:

– Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах (Постанова Кабінету Міністрів України від 07.09.22 р. № 1772) [10].

– Порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури (Постанова Кабінету Міністрів України від 22.07.22 р. № 821) [11].

– Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджені, зміст яких визначає загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (Постанова Кабінету Міністрів України від 29.03.06 р. № 373) [12].

Після розпочатої у 2014 році агресії російської федерації проти України простежуються динамічні інституційні зміни, спрямовані на формування системи об'єктів критичної інфраструктури держави.

Так, Постановою Кабінету Міністрів України від 23.08.16 р. № 563 затверджено Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави [13], яким регламентовано механізм створення переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави.

Важливим етапом інституалізації національної системи кібербезпеки стало прийняття Закону України "Про основні засади забезпечення кібербезпеки України", який визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [1]. Ст. 8 цього Закону визначає зміст національної системи кібербезпеки як "…сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури" [14]. Можна погоджуватися з судженням О. Довганя та І. Дороніна, які вважають: "попри деякі неоднозначні формулювання у тексті законодавчого акту і можливі питання з його практичним застосуванням, слід зазначити, що період формування національного законодавства у сфері кібербезпеки розпочатий, а основний акт спеціального законодавства, що започатковує відповідну систему законодавства, ухвалений" [3, с. 99].

У подальшому у період 2019 – 2020 рр. з метою реалізації цього Закону та формування відповідного масиву нормативно-правових актів, що складатимуть безпосереднє законодавство у сфері забезпечення кібербезпеки, Кабінетом Міністрів України затверджено:

– Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (Постанова Кабінету Міністрів України від 19.06.19 р. № 518) [15];

– Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки та визначила відповідальним за функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (Постанова Кабінету Міністрів України від 23.12.20 р. № 1295) [16].

Важлива методологічна та організаційна основа формування національної системи забезпечення кібербезпеки міститься у Порядку віднесення об'єктів до критичної інфраструктури (Постанова Кабінету Міністрів України від 09.10.20 р. № 1109 [17], який був розроблений з урахуванням вимог законодавства ЄС (Директива ЄС 2016/1148). Цей нормативний акт доповнює Порядок формування переліку об'єктів критичної інформаційної інфраструктури (Постанова Кабінету Міністрів України від 09.10.20 р. № 943), який визначає механізм формування національного та секторальних переліків об'єктів критичної інформаційної інфраструктури [18].

Значну роль в інституалізації національної системи кібербезпеки відіграє Постанова Кабінету Міністрів України якою затверджено "Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератак" від 23.12.20 р. № 1295 [19].

З метою забезпечення функціонування національної системи кібербезпеки Постановою Кабінету Міністрів України затверджено "Положення про організаційно-технічну модель кіберзахисту, зміст якої охоплює комплекс заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем" від 29.12.21 р. № 1426 [21].

Найбільш важливою з точки зору визначення пріоритетів кібербезпеки та формування цілей та етапів національної системи кібербезпеки є Стратегія кібербезпеки України [1]. Стратегія визначає стратегічні цілі, серед яких виділяється формування нової якості національної системи кібербезпеки, її розбудова на засадах стримування, кіберстійкості та взаємодії, а серед проблем згадується недостатня убезпеченість від кіберзагроз об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів.

Наприкінці 2021 р. був прийнятий важливий Закон України "Про критичну інфраструктуру", який визначає правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури. За цим Законом національна система захисту критичної інфраструктури визначається як "сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури" (ст. 1 цього Закону) [21].

Після повномасштабної агресії рф проти України з 2022 року змінився фокус державної політики у сфері кібербезпеки у напрямку посилення протидії кібератакам, кіберінцидентам та іншим гібридним загрозам з боку рф, чия деструктивна активність у кіберпросторі створює реальну загрозу національній інформаційній інфраструктурі.

Період протягом 2022 року – 2023-го року охарактеризувався повноцінною активізацією процесів реформування інституційного забезпечення національної системи кібербезпеки.

Лише у 2022 році Президентом України та Кабінетом Міністрів України ухвалено низку актів, спрямованих на забезпечення безпеки об'єктів критичної інфраструктури, посилення їх кіберзахисту, а саме:

– Стратегія забезпечення державної безпеки (Указ Президента України від 16.02.22 р. № 56/2022) зафіксувала перелік основних загроз національній системі кібербезпеки (пп. 7, 9, 11, 15, 19, 20) та основних цілей, напрямів та завдань державної політики у сфері державної безпеки (Розділ 3), серед яких пріоритетними є: завершення створення, подальший розвиток і посилення спроможності національної системи кібербезпеки; оптимізація координації її суб'єктів з метою ефективної протидії кіберзагрозам у сучасному безпековому середовищі; створення ефективної системи обміну інформацією між суб'єктами забезпечення державної безпеки та запровадження дієвих механізмів доступу суб'єктів забезпечення державної безпеки до державних електронних інформаційних ресурсів та автоматизованих інформаційних і довідкових систем, реєстрів, банків (баз) даних [22].

– Порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури (Постанова Кабінету Міністрів України від 22.07.22 р. № 821) [23], метою якого є встановлення відповідності стану захищеності об'єкта критичної інфраструктури вимогам законодавства, достовірності наданої інформації визначеним суб'єктам національної системи захисту критичної інфраструктури, надання методичної допомоги операторам об'єктів критичної інфраструктури в удосконаленні системи захисту критичної інфраструктури;

– Регламент обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури (Постанова Кабінету Міністрів України від 14.10.22 р. № 1174) [24], яким визначено механізм інформаційного реверсу між суб'єктами, залученими до захисту критичної інфраструктури з метою забезпечення її захисту та стійкості.

Повномасштабне збройне вторгнення виявило низку проблем забезпечення захисту критичної інфраструктури в умовах воєнного стану.

З метою їх розв'язання відповідно до законів України "Про основні засади забезпечення кібербезпеки України" (частина третя статті 6 цього Закону), "Про критичну інфраструктуру" (частина п'ята статті 11 цього Закону) Урядом України протягом 2023 року затверджено:

– Порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, що визначає механізм організації та проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та вимоги до його проведення (Постанова Кабінету Міністрів України від 24.03.23 р. № 257) [25], який розроблено на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО із залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій;

– Порядок ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього (Постанова Кабінету Міністрів України від 28.04.23 р. № 415) [26], який забезпечує включення, оброблення, виключення, захист, відображення та надання інформації про найбільш важливу для життєдіяльності суспільства та держави критичну інфраструктуру, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості, здійснюється моніторинг їх дотримання;

– Порядок розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури (Постанова Кабінету Міністрів України від 04.08.23 р. № 818) [27], який визначає вимоги до розроблення оператором критичної інфраструктури паспорта безпеки на об'єкт критичної інфраструктури та його складових, а також механізм його погодження секторальними і функціональними органами у сфері захисту критичної інфраструктури.

У квітні 2023 року стало відомо про затвердження Порядку реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі (Постанова Кабінету Міністрів України від 04.04.23 р. № 299) [28], який запроваджує етапи виявлення кібератак, реагування суб'єктів забезпечення кібербезпеки на різні види подій у кіберпросторі.

Низка заходів, спрямованих на реалізацію державної політики у сфері захисту критичної інфраструктури, визначена нормативними актами основних суб'єктів національної системи кібербезпеки, серед яких виділяються Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Національний банк.

Попри очевидний прогрес у реформуванні національної системи кібербезпеки та значну кількість нормативно-правових актів, спрямованих на забезпечення її функціонування, відповідна правова база потребує удосконалення у напрямку наближення до стандартів ЄС і країн-членів НАТО з кібербезпеки, досягнення сумісності з цими стандартами. Під цим кутом зору поглибленого дослідження потребує досвід ЄС та країн-членів НАТО.

На рівні ЄС заслуговують на увагу Директиви Європейського Парламенту та Ради (ЄС) 2016/1148 від 6 липня 2016 року "Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу" [29], Директиви Ради 2008/114/ЄС від 8 грудня 2008 р. "Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та

захисту" [30]. Ця Директива є першим кроком поступового підходу до ідентифікації і визначення ЄКІ, а також оцінювання необхідності покращення їх охорони та захисту. Фактично, Директива робить основний акцент на енергетичному і транспортному секторах, та вимагає перегляду для оцінки її впливу і необхідності додати до сфери її застосування інші сектори, між іншим, сектор інформаційно-комунікаційних технологій.

Для того, щоб посилити кіберзахист таких об'єктів, Європейська Комісія затвердила Європейську програму захисту критичної інфраструктури (European Programme for Critical Infrastructure Protection – EPCIP), зміст якої спрямований на забезпечення заходів з покращення захисту критичної інфраструктури держав ЄС. Однією із найбільш важливих є ініціатива ЄС щодо захисту критичної інформаційної інфраструктури (Critical Information Infrastructure Protection – CIP), котра спрямована на посилення безпеки та стійкості життєво важливих інфраструктур інформаційно-комунікаційного спрямування [31].

Доповнює перелік таких заходів Директива ЄС "Мережева та інформаційна безпека" від 14 грудня 2022 року, яка стосується стійкості окремих секторів критичної інфраструктури, серед яких виділяється: енергетика, транспорт, банківська справа, цифрова інфраструктура [32].

Уособлює різноманітні підходи до захисту критичної інфраструктури усіх держав ЄС Стратегія кібербезпеки ЄС (2020 – 2030) [33], яка закріплює основоположні дії щодо захисту громадян та бізнесу ЄС від кіберзагроз, створення безпечних інформаційних систем та створення відкритого, вільного та безпечного кіберпростору.

Концептуальна ідея визначення кіберпростору як сфери операцій, а також колективної оборони і безпеки в євроатлантичній зоні закладена в Стратегічній концепції НАТО 2022 року [34]. Ця концепція передбачає інтеграцію наступальних кіберзасобів при плануванні місій і операцій за допомогою SCEPVA – структури суверенних кіберефектів, наданих союзниками на добровільній основі. Як і у Стратегії кібербезпеки ЄС (2020 – 2030), у Стратегії НАТО визнається необхідність у тіснішому партнерстві між НАТО і ЄС в обороні і безпеці. НАТО може допомогти не лише з розробкою і запровадженням заходів з кібероборони і кіберстійкості, які покращили б загальну стабільність кіберпростору, а також і з посиленням нормативних аспектів цих форм регулювання і врядування [35].

Розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими країнами-членами НАТО, є одним з ключових напрямків Стратегії забезпечення кібербезпеки України. Зокрема, цією Стратегією передбачено [1]:

- налагодження систематичного обміну інформацією про деструктивну діяльність у кіберпросторі з міжнародними партнерами, насамперед Сполученими Штатами Америки, державами-членами ЄС та країнами-членами НАТО, створення платформи такого обміну;
- поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі;
- проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами країн-членів НАТО задля досягнення оперативної сумісності;
- співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія).

Для вдосконалення такої взаємодії Україна відповідно до цієї Стратегії має забезпечити активну участь у діалозі в рамках міжнародних організацій щодо спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної нормативно-правової бази.

Розділ 4 Стратегії забезпечення кібербезпеки, який має назву "Національна система кібербезпеки: засади розбудови", передбачає, що для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є:

- посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування);
- набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість) [1].

Однак, на жаль, можна констатувати, що попри успішну реалізацію більшості положень Стратегії, частина її заходів залишається невиконаною. Зокрема, серед нереалізованих виділяються заходи правового характеру щодо:

- розроблення системи індикаторів стану кібербезпеки;
- запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони;
- внесення необхідних змін до деяких законодавчих актів щодо створення та визначення завдань кібервійськ;
- розроблення нормативно-правових актів, які регламентують функціонування загальнодержавної системи виявлення кібератак;
- доповнення нормативно-правових актів, які регламентують питання функціонування загальнодержавної системи боротьби з тероризмом, положеннями щодо протидії актам кібертероризму.

Їх виконання передбачено Планом заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України, який затверджено Розпорядженням Кабінету Міністрів України від 19.12.23 р. № 1163 [36].

Висновки.

Формування законодавчої бази забезпечення системи кібербезпеки України має відносно недавню історію. Процес її формування ще триває. Після збройного вторгнення рф у цьому законодавстві відбулися динамічні зміни, пов'язані із зростанням небезпеки кіберзагроз, потребою посиленого кіберзахисту об'єктів критичної інфраструктури. Основні напрямки правового забезпечення формування національної системи кібербезпеки стосуються захисту державних інформаційних ресурсів, реагування на кібератаки та кіберінциденти, а також міжнародного співробітництва в сфері кібербезпеки. Ключовими напрямками розвитку цієї системи є: посилення захисту об'єктів критичної інфраструктури в умовах воєнного стану, створення та розвиток кадрового потенціалу основних суб'єктів національної системи кібербезпеки, розвиток цифрової грамотності, регулярні кібернавчання та тренінги для всіх верств населення, обмін досвідом та найкращими практиками з іноземними партнерами, поглиблення міжнародного співробітництва України з ЄС і НАТО.

Невідкладного виконання потребують всі заплановані заходи Стратегії, а процес її реалізації має бути максимально прозорим, відкритим та супроводжуватися

демократичним цивільним контролем.

Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища [1].

Ключовим на сьогоднішньому етапі є імплементація в законодавство України стандартів ЄС І НАТО з питань кібербезпеки.

Використана література

1. Стратегія кібербезпеки України: Указ Президента України від 26.08.21 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

2. Алексеєва О.А. Правове забезпечення кібербезпеки об'єктів критичної інфраструктури *Інформація і право*. № 4(47)/2023. С. 168-176.

3. Довгань О.Д., Доронін І.М. Розвиток законодавства у сфері кібербезпеки: інформаційно-правове дослідження. Наукові часописи УДУ імені Махайла Драгоманова. Сер. 18. Право. 2017. Вип. 32. С. 91-100. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/24333/Dovgan_ Doro nin.pdf?sequence=1&isAllowed=y

4. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право*. 2017. № 5. С. 174-180.

5. Когут Ю. Правові засади формування та розвитку державної системи протидії кібертероризму в Україні. *Підприємництво, господарство і право*. 2020. № 12. С. 170-174.

6. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. / Бобро Д.Г., Іванюта С.П., Кондратов С.І., Суходоля О.М. / за заг. ред. О.М. Суходолі. Київ: НІСД, 2019. 224 с. URL: https://niss.gov.ua/sites/default/files/ 2019-05/Dopov_Suchodolya_print.pdf

7. Рогов П.Д. Ворович Б.О., Ткаченко В.А. Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері: збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2017. № 1. С. 64-72. URL: http:// nbuv.gov.ua/UJRN/Znpcvsd_2017 _1_13

8. Ткачук Н.А. Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. *Інформація і право*. № 1(24)/2018. С. 133-138. URL: http://ippi.org.ua/sites/default/files/16_4.pdf

9. Про захист інформації в інформаційно-комунікаційних системах: Закон України 05.07.94 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

10. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах: Постанова Кабінету Міністрів України від 07.09.22 р. № 177. URL: https://zakon.rada.gov.ua/laws/ show/1772-2002-п#Text

11. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 22.07.22 р. № 821. URL: https://zakon. rada.gov.ua/laws/show/821-2022- п#Text

12. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах: Постанова Кабінету Міністрів України від 29.03.06 р. № 373 URL: https://zakon.rada.gov.ua/laws/show/1772-2002-п# Text

13. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: Постанова Кабінету Міністрів України від 23.08.16 р. № 563. URL: https://zakon.rada.gov.ua/laws/show/563-2016- п#Text

14. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

15. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.19 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF

16. Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки та визначила відповідальним за функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова Кабінету Міністрів України від 23.12.20 р. № 1295). URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text

17. Порядок віднесення об'єктів до критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.20 р. № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text. (дата звернення: 30.10.2024).

18. Порядок формування переліку об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.20 р. № 943. URL: https://zakon.rada.gov.ua/ laws/ show/943-2020-%D0%BF#Text (дата звернення: 30.10.2024).

19. Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератак: Постанова Кабінету Міністрів України від 23.12.20 р. № 1295 URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text

20. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.21 р. № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

21. Про критичну інфраструктуру: Закон України від 16.11.21 р. №1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#n80

22. Стратегія забезпечення державної безпеки: Указ Президента України від 16.02.22 р. № 56/2022. URL: https://www.president.gov.ua/documents/562022-41377

23. Порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 22.07.22 р. № 821. URL: https://zakon.rada. gov.ua/ laws/show/821-2022-%D0%BF#Text

24. Регламент обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури: Постанова Кабінету Міністрів України від 14.10.22 р. № 1174. URL: https://zakon.rada.gov.ua/laws/show/1174-2022-%D0%BF#Text

25. Порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, що визначає механізм організації та проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та вимоги до його проведення: Постанова Кабінету Міністрів України від 24.03.23 р. № 257. URL: https://zakon.rada.gov.ua/ laws/show/257-2023-%D0%BF#Text

26. Порядок ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього: Постанова Кабінету Міністрів України від 28.04.23 р. №415. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0 %BF#Text

27. Порядок розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури: Постанова Кабінету Міністрів України від 04.08.23 р. № 818. URL: https://zakon. rada. gov.ua/laws/show/818-2023-%D0%BF#Text

28. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від 04.04.23 р. № 299. URL: https://zakon. rada.gov.ua/laws/show/299-2023-%D0%BF#Text

29. Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: Директива Європейського Парламенту і Ради (ЄС) № 2016/1148 від 06.07.2016 р. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

30. Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту: Директива Ради ЄС № 2008/114/ЄС від 08.12.2008 р. URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text

31. Communication from the commission on a European Programme for Critical Infrastructure Protection. Commission of the European Communities Brussels, 12.12.2006. COM (2006) 786 final. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786: FIN:EN:PD

32. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high overall level of security for network and information systems within the Union territory. Site. URL: https:// eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

33. Рада ЄС прийняла Стратегію кібербезпеки ЄС 2020 – 2030. URL: https://medialeague.com.ua/rada-yes-pryjnyala-strategiyu-kiberbezp

34. NATO 2022/ STRATEGIC CONCEPT. URL: https://www.nato.int/strategic-concept

35. НАТО і стратегічна конкуренція в кіберпросторі. URL: https://www.nato.int/docu/review/uk/articles/2023/06/06/nato-strategchna-konkurentsya-v-kberprostor/index.html

36. План заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки: Розпорядження Кабінету Міністрів України від 19.12.23 р. № 1163. URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text

* * *