УДК 342.95

https://doi.org/10.52058/3041-1254-2025-6(16)-43-52

Бейкун Андрій Леонардович кандидат юридичних наук, доцент, доцент кафедри правового забезпечення та правоохоронної діяльності факультету забезпечення державної безпеки, Київський інститут Національної гвардії України, м. Київ, тел.: (098) 001-30-15, https://orcid.org/0000-0002-4895-1361

Волуйко Олексій Миколайович кандидат юридичних наук, доцент, начальник кафедри правового забезпечення та правоохоронної діяльності факультету забезпечення державної безпеки, Київський інститут Національної гвардії України, м. Київ, тел.: (098) 001-30-15, https://orcid.org/0000-0002-0894-5004

ТЕНДЕНЦІЇ ОНОВЛЕННЯ І РОЗВИТКУ НОРМАТИВНОГО МАСИВУ ТА ПРОГРАМНИХ ДОКУМЕНТІВ З ПИТАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРЗАХИСТУ В УМОВАХ КРИТИЧНОГО ПОСИЛЕННЯ ЗОВНІШНІХ ЗАГРОЗ ТА НЕБЕЗПЕК

Анотація. В епоху цифрової трансформації телекомунікаційні системи та мережеві технології перетворилися на фундаментальні елементи сучасного життя, проникаючи у всі сфери державного функціонування: від оборонного сектору та політичного управління до бізнес-процесів, громадської безпеки та захисту законних інтересів громадян, включаючи майнові права. Проте, динамічний прогрес у галузі інформаційних технологій породжує нові виклики та небезпеки, особливо в контексті забезпечення кібернетичної безпеки.

Кіберзлочинність, здатна дестабілізувати роботу державних механізмів, систем національної безпеки, стратегічно важливої інфраструктури та створювати ризики для населення, перетворюється на визначальний чинник у сучасних конфліктах. Показовим випадком є війна між росією та Україною, яка, попри свій всеосяжний характер, демонструє типові ознаки «гібридного» протистояння. Держава-агресор у збройному протиборстві використовує різноманітні «додаткові інструменти», включаючи кіберакції та атаки на множинні цілі української держави: інформаційну сферу, фінансовий та медійний сектори, комунікаційні та керуючі системи, об'єкти стратегічної інфраструктури тощо. Отже, ці порівняно нові загрози державній безпеці потребують комплексного підходу до організації кіберзахисту та створення дієвих (включаючи організаційно-правові) механізмів протидії.

Термінологія кібербезпеки, кіберконфліктів, інформаційного протиборства, кіберзахисту, віртуального простору поступово набуває відповідного

етимологічного та правового наповнення, стаючи основними каталізаторами формування спеціалізованої нормативної бази, орієнтованої передусім на охорону: сфери національної безпеки та оборони, суспільного простору країни, економічних суб'єктів, громад та індивідуальних громадян у цьому кіберпротистоянні.

Ключові слова: інформаційна безпека, кібербезпека, кібероперації, інформаційно-психологічний вплив, кіберзахист, кіберсфера.

Beikun Andrii Leonardovich PhD in Law, Associate Professor, Associate Professor of the Department of Legal Support and Law Enforcement Activities, Faculty of State Security, Kyiv Institute of the National Guard of Ukraine, Kyiv, tel.: (098) 001-30-15, https://orcid.org/0000-0002-4895-1361

Voluiko Oleksii Mykolayovych PhD in Law, Associate Professor, Head of the Department of Legal Support and Law Enforcement Activities, Faculty of State Security, Kyiv Institute of the National Guard of Ukraine, Kyiv, tel.: (098) 001-30-15, https://orcid.org/0000-0002-0894-5004

TRENDS IN UPDATEMENT AND DEVELOPMENT OF REGULATORY BASE AND PROGRAM DOCUMENTS ON INFORMATION SECURITY AND CYBER PROTECTION IN THE CONDITIONS OF CRITICAL INCREASE IN EXTERNAL THREATS AND DANGERS

Abstract. In the era of digital transformation, telecommunications systems and network technologies have become fundamental elements of modern life, penetrating all areas of state functioning: from the defense sector and political administration to business processes, public security, and the protection of citizens' legitimate interests, including property rights. However, dynamic progress in the field of information technology creates new challenges and dangers, especially in the context of ensuring cybersecurity.

Cybercrime, which can destabilize the work of state mechanisms, national security systems, strategically important infrastructure and create risks for the population, is becoming a determining factor in modern conflicts. A case in point is the war between Russia and Ukraine, which, despite its comprehensive nature, demonstrates typical signs of a “hybrid” confrontation. The aggressor state uses various "additional tools" in armed confrontation, including cyberattacks and attacks on multiple targets of the Ukrainian state: the information sphere, financial and media sectors, communication and control systems, strategic infrastructure facilities, etc. Therefore, these relatively new threats to national security require a comprehensive approach to organizing cyber defense and creating effective (including organizational and legal) countermeasures.

The terminology of cybersecurity, cyber conflicts, information confrontation, cyber defense, and virtual space is gradually acquiring appropriate etymological and legal content, becoming the main catalysts for the formation of a specialized regulatory framework focused primarily on protection: the sphere of national security and defense, the public space of the country, economic entities, communities, and individual citizens in this cyber confrontation.

Keywords: information security, cybersecurity, cyber operations, information and psychological influence, cyber defense, cybersphere.

Постановка проблеми. Проблематика забезпечення інформаційної та кібербезпеки, передусім, зумовлена потребою охорони національного інформаційного середовища та вдосконалення інформаційно-комунікаційних технологій для реалізації державної інформаційної стратегії, особливо в контексті загострення зовнішніх викликів та ризиків для країни до граничних показників.

На завершення трьох з половиною років з моменту початку широкомасштабної військової агресії, російська федерація продовжує бути головним генератором ризиків для національної та глобальної кібербезпеки. Вона активно впроваджує стратегію інформаційного протистояння, що ґрунтується на комбінуванні руйнівних кібероперацій та інформаційно-психологічного впливу, інструментарій якої широко використовується у конфлікті з Україною. Подібна деструктивна діяльність становить серйозну небезпеку для ефективності наявного потенціалу протидії актам кібертероризму та кібердиверсій щодо національної інформаційної інфраструктури.

Як відомо, як перед початком подій березня-квітня 2014 року, так і повномасштабного вторгнення лютого 2022 року, росія інтенсифікувала кібернапади на урядові структури, військово-промисловий сектор, критичну інфраструктуру, IT-системи та медіаресурси України. Фактично кіберпротиборство та кіберзахист перетворились на центральні компоненти війни. Українські експерти та добровольці-хакери не тільки ефективно відбивають атаки, але й наносять відчутні контрудари. Минулого року зареєстровано понад 1,25 мільйона DDoS-атак на російську інфраструктуру (що складає 8,4% від загальної кількості кібератак у світі). Згідно з оцінками керівника служби інформаційної безпеки та кібербезпеки Апарату РНБО, Україна є єдиною державою, що змогла отримати стратегічну перевагу у протиборстві кібернападам та інформаційній експансії російської федерації. Однак необхідно розуміти: про кінцеву перемогу поки говорити зарано. Противник еволюціонує, адаптується, змінює напрямки атак. Сучасна тенденція – «розумні» атаки з метою ідентифікації вразливих точок в інфраструктурі. Міжнародна практика підтверджує: ефективне функціонування систем кіберзахисту залишатиметься пріоритетним завданням і після закінчення війни [1].

Отже, кіберсфера поряд з іншими фізичними просторами, офіційно визнана і реально функціонує як один із театрів бойових дій. Посилюється тренд формування кібервійськових підрозділів, функції яких охоплюють не тільки гарантування безпеки національної критичної інформаційної інфраструктури від кіберзагроз, але й здійснення попереджувальних offensive-операцій у кіберсфері, що передбачає знешкодження стратегічно важливих інфраструктурних об'єктів супротивника через деструкцію інформаційних систем, що керують такими об'єктами.

Аналіз останніх досліджень і публікацій. Питання кібернетичної безпеки та державної стратегії, орієнтованої на її гарантування, є об'єктом наукових доробок численних дослідників, передусім, спеціалістів у сфері адміністративного, кримінального права, а також права інтелектуальної власності, зокрема: В.Б. Авер'янова, І.В. Арістової, І.Л. Бачило, П.П. Богуцького, І.П. Голосніченка, О.Д. Довганя, Р.О. Додонова, І.М. Дороніна, В.В. Зуй, Л.В. Кузенка, О.Є. Кутафіна, В.Л. Манілова, О.В. Нестеренка, Г.В. Падалка, В.Л. Сидоренко, О.Ю. Синявської, С.Г. Стеценка, С.С. Теленика, М.М. Тищенка, Ю.П. Тихомірова, О.М. Шевчука, В.М. Фурашева, І.О. Харитоненка та інших.

Мета статті – проаналізувати нормативні та програмні аспекти питань кібернетичної та інформаційної безпек та державної стратегії, орієнтованої на їх гарантування, насамперед, як складових структури забезпечуючих елементів національної безпеки в умовах особливих правових режимів.

Виклад основного матеріалу. У контексті поточної повномасштабної війни низка науковців, включаючи А. Савчука, А. Жарикову, О. Радутного, - передбачають подальше нарощування інтенсивності міждержавного суперництва та розвідувально-диверсійної активності у кіберсфері. Розширюється спектр організацій, які прагнуть створити власні кіберрозвідувальні служби, опанувати передові технології розвідувально-диверсійної роботи у цифровому просторі, посилюють державний нагляд за національними сегментами глобальної мережі. Водночас, поширюється інструментарій, який передбачає акумуляцію значних обсягів даних про поведінкові моделі індивідів, соціальних спільнот та застосування новітніх розробок у галузі штучного інтелекту. Зростає тенденція реалізації розвідувально-диверсійної діяльності у кіберпросторі через залучення спецслужбами російської федерації міжнародних хакерських груп для здійснення кіберінтервенцій [2, с. 27].

Підвищується технологічна складність втілення кіберзагроз, безперервно удосконалюються та створюються нові засоби і методи кібернападів. Зміцнюється тенденція застосування кібератак як засобу спеціальних інформаційних кампаній, маніпулювання громадською свідомістю, втручання у виборчі процедури.

За словами експерта А. Жарикової, російська агресія щодо України не обмежилась виключно військовими зіткненнями. Агресивні дії у кіберсфері

існували і раніше, однак з 2022 року вони набули відкритого характеру. Водночас, до початку відкритої російської агресії було проведено серію розвідувальних операцій, спрямованих на збирання інформації, переважно з інституцій оборонно-безпекового комплексу, а також впливових суб'єктів бізнесу. Це дозволяло військово-політичному керівництву російської федерації формувати відповідну стратегію подальших кроків, базуючись на відомих намірах української сторони. До речі, найпотужнішим джерелом хакерських нападів упродовж 2022-2024 років у світі стає саме російська федерація, яка здійснює понад половину всіх злочинних активностей у цій галузі на глобальному рівні – 58%. Друге місце займає КНДР з показником 23%. Україна посідає лідируючу позицію серед країн-мішеней таких атак. На Україну припадає 19% усіх глобальних кібератак. Для порівняння: частка кібератак на Бельгію, Японію та Німеччину не досягає 3% від загального світового обсягу [3].

Згідно з доповіддю Microsoft, росія збільшила кіберпотенціал за 2022-першу половину 2024 року з 21% до 32%. Також було ідентифіковано ключові сектори, що зазнають атак. Найбільше зусиль хакерів спрямовується на сферу державного управління та дипломатії – 48%. До речі, саме на цю галузь увага російських хакерів зросла з 3% до 53%. 31% кібератак припадає на Збройні Сили, інші військові формування, правоохоронні та розвідувальні органи, телекомунікаційні мережі. Зі значним відставанням до переліку цілей потрапляє освітня сфера – 3% та медіа, охорона здоров'я, ІТ – 1%. Загалом, 2022-2024 роки складно охарактеризувати як «кіберспокійні» для України. Проте, січень 2022 року встановив абсолютний рекорд. Лише за один місяць було виявлено та нейтралізовано понад масштабних 120 атак, і це тільки офіційні дані. За даними СБУ, більшість здійснених кібератак відносилися до 4 категорій: атаки на веб-додатки; зловмисне програмне забезпечення; неавторизоване підключення до командно-контрольних серверів; спроби отримання несанкціонованого доступу [3].

Доцільно, як видається, підтримати думку Л.Ю. Веселової та В.В. Зуя про те, що й сьогодні, незважаючи на жорсткі умови повномасштабної війни, зберігається проблематика недосконалості правового регулювання у галузі кібербезпеки, застарілості інформаційно-правових приписів, неадекватного рівня санкцій за інформаційні порушення, уповільненої та безсистемної імплементації норм європейського законодавства у зазначену сферу [4, с. 18; 5, с. 231].

Водночас, вивчення діючого законодавства демонструє наявність низки прогалин стосовно врегулювання питань кібербезпеки (кібероборони), які вимагають невідкладного розроблення пропозицій щодо способів розв'язання наявних проблем як з огляду на потреби забезпечення національної безпеки в умовах повномасштабної війни, так і необхідності європейської інтеграції національного законодавства загалом. У цьому контексті цілком слушно зауважує С.С. Теленик про те, що держава має стати ініціатором та гарантом

ефективного розвитку і застосування інформаційного простору України, особливо у військовій сфері. Система кібербезпеки повинна бути багатоступеневою і стійкою, тобто такою, що виключить можливість отримання неправомірного доступу до відомостей військового характеру, даних, що становлять державну таємницю. У зв'язку з цим, деякі автори, зокрема: В.В. Зуй та С.С. Теленик пропонують розробити Інформаційний кодекс України, який би систематизував інформаційно-правові норми та, зокрема, більш точно, детально і змістовно врегульовував би питання гарантування кібербезпеки. Погоджуємося, що наразі існує проблема недосконалості законодавства у сфері кібербезпеки, застарілості інформаційно-правових норм, неадекватного рівня санкцій за інформаційні правопорушення, уповільненого застосування положень європейського законодавства у даній галузі. Пропонується також розроблення уніфікованого понятійно-термінологічного апарату у сфері кібербезпеки, а також його узгодження з термінологією чинного українського законодавства та міжнародних актів з питань кібернетичної безпеки [5, с. 233; 6].

Модернізація та удосконалення діючого інформаційного законодавства потребує, на думку дослідників у галузі кіберзахисту, насамперед О.М. Суходолі, системного підходу, який має базуватися на наступних принципах:

1. Створення та імплементація регулятивних інструментів для ефективного забезпечення функціонування нормативної бази з питань кібербезпеки.
2. Партнерство зі стратегічними союзниками у сфері обміну даними, найкращим досвідом та ресурсами для гарантування кібербезпеки.
3. Формування національних інструментів захисту інформаційного середовища та цифрових ресурсів.
4. Підготовка та протидія кібернападам, що має охоплювати: ідентифікацію, захист, виявлення, реагування та відновлення.
5. Реалізація загальнодержавної програми забезпечення кіберосвіти та підвищення поінформованості громадян та юридичних осіб з питань кібербезпеки.
6. Системність підходу до кіберзагроз та міжсекторальне співробітництво у зазначеній сфері.
7. Систематичне оновлення Стратегії забезпечення державної безпеки, Стратегії кібербезпеки та інших галузевих стратегій з метою своєчасного визначення та окреслення механізму реагування на нові виклики у сфері кібернетичних та пов’язаних загроз.
8. Міжгалузевий обмін досвідом та найкращими практиками з метою підвищення загального рівня кібербезпеки.
9. Застосування спільних ресурсів у процесі міжсекторіального співробітництва (інформаційні бази, технічні засоби та експертні знання).
10. Гарантування впровадження комплексних захистів при кібератаках одночасно різних галузей або секторів [7].

Як уже відзначалося концептуально, прогнозування майбутніх загроз у галузі кібербезпеки є пріоритетним завданням для забезпечення національної безпеки за цим напрямом. Відповідно, на думку М. Сироватченко, ключовими є наступні аспекти:

1. Активне становлення шостого технологічного укладу (біо-, нано-, інфо-, когнотехнологій, їх конвергенцію) та ризики, з якими стикається держава внаслідок впровадження зазначених новітніх технологій.

2. Зростання впливу кіберзагроз на функціонування управлінських структур, як національних, так і транснаціональних.

3. Розподіл сфер впливу у кіберпросторі між світовими центрами сили та посилення їх прагнення за рахунок такого розподілу забезпечити реалізацію власних геополітичних інтересів.

4. Необхідність створення нового роду військ – кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі супротивника [8].

Певні імперативи застосування законодавства у сфері кібербезпеки та напрями його розвитку пропонує Стратегія кібербезпеки України [9]. Аналізуючи положення зазначеного програмного документу, доцільно акцентувати увагу на таких її аспектах:

1. Стратегія кібербезпеки визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних; окреслені виклики та загрози повною мірою зберігають свою актуальність і в сучасних умовах правового режиму воєнного стану.

2. Метою означеної Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина;

3. Досягнення мети здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії (у тому числі, - спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України), забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки;

4. В Україні триває процес становлення системи стратегічних комунікацій. Органами державної влади України здійснено низку організаційних та практичних заходів зі зміцнення власної інституційної спроможності у сфері стратегічних комунікацій, однак не створено дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до здійснення заходів із протидії загрозам в інформаційній сфері. Зазначене послаблює можливості розбудови комплексного стратегічного планування інформаційного потоку, здійснення системної комунікативної діяльності Кабінету Міністрів України, об'єднання всіх ключових суб'єктів у сфері інформаційних відносин, суб'єктів формування і реалізації державної політики щодо ефективного захисту національного інформаційного простору, утвердження позитивного іміджу України, реалізації цілей захисту національної безпеки України в інформаційній сфері [9; 10; 5, с. 234].

Висновки. Таким чином, як вбачається, пріоритетна увага забезпечувальних структур має зосереджуватись на розробці стратегічних нормативних документів з питань кібербезпеки, їх систематичному оновленні та моніторингу виконання відповідного плану заходів реалізації на базі оцінки ефективності та можливостей. Для своєчасної актуалізації таких нормативів в Україні необхідно сформувати критерії оцінювання стану кібербезпеки в державі, особливо в умовах особливих правових режимів, а після здійснення відповідного правового аналізу - визначити ключові вектори формування нової Стратегії кібербезпеки України, яка розраховуватиметься на період після 2025 року. Враховуючи міжнародну практику, включно з фундаментальними рекомендаціями та директивами НАТО та ЄС, основний стратегічний вектор діяльності суб'єктів національної системи кібербезпеки має бути орієнтований на кіберзахист критичної інформаційної інфраструктури. Також варто відзначити, що наразі Україна знаходиться на передовій кібервійни. І хоча ці обставини негативно впливають на наше життя, їх можна застосувати для апробації нових ідей та технологій у сфері захисту інформації. Досвід, який ми отримуємо у протиборстві з ворогом, є безцінним надбанням для розвитку кібернетичної галузі.

Література:

1. Кириченко Анастасія. Кібербезпека в Україні: шляхи розвитку та можливості. *Укрінформ.* 07 січня 2024. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html.

2. Савчук А.В. Кібербезпека в системі національної безпеки України. *Кваліфікаційна (бакалаврська) робота*. 58 с. ДоНУ імені Василя Стуса, Вінниця, 2022. URL: https://jarch.donnu.edu.ua/article/ view/12715/1261883.pdf (lsej.org.ua).

3. Жарикова Анастасія. Кількість кібератак у 2023 році зросла на 16 % – Держспецзв'язку. *Українська правда*. Розділ: Економічна правда. 31 січня 2024. [Інформаційний портал]. URL: https://www.epravda.com.ua/news/2024/ 01/31/709355.

4. Веселова Л.Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни: *автореф. дис. докт. юр. наук*: 12.00.07; Одеський державний університет внутрішніх справ, 2021. 38 с.

5. Зуй В.В. Актуальні проблеми кібербезпеки в Україні з урахуванням європейської інтеграції. *Південноукраїнський правничий часопис*. Правове забезпечення адміністративної реформи. 4-2022, Ч.1. С. 231-235. URL: http:// www.sulj.oduvs.od.ua/archive/ 2022/4/part_1/35.pdf.

6. Теленик С.С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання. *Монографія.* URL:https://jurkniga.ua/contents/derzhavna-sistema-zakhistu-kritichnoi-infrastrukturi-ukraini-kontseptualni-zasadi-administrativno-pravovogo-regulyuvannya.pdf?srsltid=AfmBOopbP3IBUus1V-aeQGzd 7p8muhVRxx5YrBm WgRWWbAIcVnT7JDmq [in Ukrainian].

7. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: *аналітична доповідь* / за ред. О.М. Суходолі. Київ: НІСД, 2020. 28 с.

8. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка»*. Серія: «Юридичні науки». № 1 (41), 2024. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2024/may/34615/sirovatchenko41.pdf.

9. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року №447/2021. URL: https://www.president.gov. ua/documents/4472021-40013.

10. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 07 березня 2025 р. № 204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text.

References:

1. Kyrychenko Anastasiya. Kiberbezpeka v Ukrayini: shlyakhy rozvytku ta mozhlyvosti. Ukrinform. 07 sichnya 2024. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html [in Ukrainian].

2. Savchuk A.V. Kiberbezpeka v systemi natsionalnoyi bezpeky Ukrayiny. Kvalifikatsiyna (bakalavrska) robota. 58 s. DoNU imeni Vasylya Stusa, Vinnytsya, 2022. URL: https://jarch.donnu.edu.ua/article/view/12715/1261883.pdf (lsej.org.ua) [in Ukrainian].

3. Zharykova Anastasiya. Kilkist kiberatak u 2023 rotsi zrosla na 16 % – Derzhspetszvyazku. Ukrayinska pravda. Rozdil: Ekonomichna pravda. 31 sichnya 2024. [Informatsiynyy portal]. URL: https://www.epravda.com.ua/news/2024/01/31/709355 [in Ukrainian].

4. Veselova L.YU. Administratyvno-pravovi osnovy kiberbezpeky v umovakh hibrydnoyi viyny: avtoref. dys. dokt. yur. nauk: 12.00.07; Odeskyy derzhavnyy universytet vnutrishnikh sprav, 2021. 38 s. [in Ukrainian].

5. Zuy V.V. Aktualni problemy kiberbezpeky v Ukrayini z urakhuvannyam yevropeyskoyi intehratsiyi. Pivdennoukrayinskyy pravnychyy chasopys. Pravove zabezpechennya administratyvnoyi reformy. 4-2022, CH.1. S. 231-235. URL: http://www.sulj.oduvs.od.ua/archive/ 2022/4/part_1/35.pdf [in Ukrainian].

6. Telenyk S.S. Derzhavna systema zakhystu krytychnoyi infrastruktury Ukrayiny: kontseptualni zasady administratyvno-pravovoho rehulyuvannya. Monohrafiya. URL:

https://jurkniga.ua/contents/derzhavna-sistema-zakhistu-kritichnoi-infrastrukturi-ukraini-kontseptualni-zasadi-administrativno-pravovogo-regulyuvannya.pdf?srsltid=AfmBOopbP3IBUus1V-aeQGzd 7p8muhVRxx5YrBm WgRWWbAIcVnT7JDmq [in Ukrainian].

7. Derzhavna systema zakhystu krytychnoyi infrastruktury v systemi zabezpechennya natsionalnoyi bezpeky: analitychna dopovid / za red. O.M. Sukhodoli. Kyyiv: NISD, 2020. 28 s. [in Ukrainian].

8. Syrovatchenko M. Pravovi aspekty zabezpechennya kiberbezpeky v Ukrayini: suchasni vyklyky ta rol natsionalnoho zakonodavstva. Visnyk Natsionalnoho universytetu «Lvivska politekhnika». Seriya: «Yurydychni nauky». № 1 (41), 2024. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2024/may/34615/sirovatchenko41.pdf [in Ukrainian].

9. Pro rishennya Rady natsionalnoyi bezpeky i oborony Ukrayiny vid 14 travnya 2021 roku «Pro Stratehiyu kiberbezpeky Ukrayiny»: Ukaz Prezydenta Ukrayiny vid 26 serpnya 2021 roku №447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 [in Ukrainian].

10. Pro zatverdzhennya planu zakhodiv na 2025 rik z realizatsiyi Stratehiyi kiberbezpeky Ukrayiny: Rozporyadzhennya Kabinetu Ministriv Ukrayiny vid 07 bereznya 2025 r. № 204-r. URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text [in Ukrainian].