УДК 34

https://doi.org/10.52058/2786-6025-2025-1(42)-72-81

Кокошко Федір Іванович, кандидат історичних наук, доцент, Доцент кафедри права, ПЗВО «Міжнародний класичний університет імені Пилипа Орлика», м. Миколаїв, тел.: +38(050)394-72-87, +3(095) 103-99-17, https://orcid.org/0000-0002-3561-6396

Берекет Марина Станіславівна здобувачка другого (магістерського) рівня вищої освіти освітньої програми «Право», ПЗВО «Міжнарожний класичний університет імені Пилипа Орлика», м. Миколаїв, тел.: +38(066) 453-17-28, https://orcid.org/0009-0006-9806-3051

Чемьоркін Олексій Сергійович здобувач другого (магістерського) рівня вищої освіти освітньої програми «Право», ПЗВО «Міжнародний класичний університет імені Пилипа Орлика», м. Миколаїв, вул. Котельна, 2, тел.: +38(093) 349-99-73, https://orcid.org/0009-0006-3153-9748

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА СКОЄННЯ АТАК ПО ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У статті розглядається кримінальна відповідальність за скоєння атак по об'єктахкритичної інфраструктури у якості механізму забезпечення стабільної та сталої роботи державних органів та запобігання завданню економічної та соціальної шкоди суспільству.

Проаналізовано особливості нормативного регулювання аспекту кримінальної відповідальності за атаки по критичній інфраструктурі в Україні та країнах-партнерах (США, ЄС).

В рамках законодавства України, пристосовно до обставин об'єктивної дійсності, пов'язаних із запровадженням правового режиму воєнного стану Указом Президента України № 64/2022 від 24.02.2022 р. Про введення воєнного стану в Україні, акцентовано увагу на таких нормативних документах, як Кримінальний кодекс України № 2341-III (ст. 361, ст. 113), а також Законі України «Про основні засади забезпечення кібербезпекиУкраїни» № 2163-VIII та Законі України «Про критичну інфраструктуру» № 1882-IX.

Аспекти притягнення відповідальності за скоєння атак по об'єктах критичної інфраструктури в США проаналізовані такі нормативні документи, як Закон про комп'ютерне шахрайство та зловживання1986 р. (Computer Fraud and Abuse Act of 1986), Патріотичний акт США 2001 р. (USA PATRIOT Actof 2001) та Закон про кібербезпеку та безпеку інфраструктури 2002 р. (Cybersecurity andInfrastructure Security Act (CISA) of 2018).

Особливості кримінальної відповідальності за скоєння атак по об'єктах критичної інфраструктури у кримінально-правовій парадигмі ЄС розкриті крізь призму Директиви NIS 2 2022 р. (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Ключові слова: критична інфраструктура, об'єкти критичної інфраструктури, кримінальна караність, кримінальна відповідальність, скоєння атак, національна безпека, інформаційна безпека, кібербезпека.

Kokoshko Fedir Ivanovich PhD in History, Docent, Associate Professor of the Department of Law, Pylyp Orlyk International Classical University, Mykolaiv, str. Kotelna, 2, tel.: +38(050)394-72-87, +3(095) 103-99-17, https://orcid.org/0000-0002-3561-6396

Bereket Maryna Stanislavivna the applicant for the second (masters) level of higher education in the field of Jurisprudence, Pylyp Orlyk International Classical University, Mykolaiv, tel.: +38(066) 453-17-28, https://orcid.org/0009-0006-9806-3051

Chemyorkin Oleksiy Serhiyovych the applicant for the second (masters) level of higher education in the field of Jurisprudence, Pylyp Orlyk International Classical University, Mykolaiv, tel.: +38(093) 349-99-73, https://orcid.org/0009-0006-3153-9748

CRIMINAL LIABILITY FOR COMMITTING ATTACKS ON CRITICAL INFRASTRUCTURE FACILITIES

Abstract. The article considers criminal liability for committing attacks on critical infrastructure facilities as a mechanism for ensuring stable and sustainable work of state bodies and preventing economic and social harm to society.

The features of the regulatory regulation of the aspect of criminal liability for attacks on critical infrastructure in Ukraine and partner countries (USA, EU) are analyzed.

Within the framework of the legislation of Ukraine, in accordance with the circumstances of objective reality related to the introduction of the legal regime of martial law by Decree of the President of Ukraine No. 64/2022 of 02/24/2022. On the introduction of martial law in Ukraine, attention is focused on such regulatory documents as the Criminal Code of Ukraine No. 2341-III (Art. 361, Art. 113), as well as the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" No. 2163-VIII and the Law of Ukraine "On Critical Infrastructure" No. 1882-IX.

Aspects of bringing to justice for attacks on critical infrastructure facilities in the USA are analyzed in such regulatory documents as the Computer Fraud and Abuse Act of 1986, the USA PATRIOT Act of 2001, and the Cybersecurity and Infrastructure Security Act (CISA) of 2018.

The features of criminal liability for attacks on critical infrastructure facilities in the EU criminal law paradigm are revealed through the prism of the NIS 2 Directive 2022 (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Keywords: critical infrastructure, critical infrastructure facilities, criminal punishment, criminal liability, attacks, national security, information security, cybersecurity.

Постановка проблеми. Необхідно зауважити, що притягнення до кримінальної відповідальності за атаки на об’єкти критичної інфраструктури виступає важливим інструментом гарантування як національного, так і глобального рівня безпеки, через що такі правопорушення здебільшого прирівнюються до тяжких злочинів (США, ЄС), оскільки їхні наслідки підривають стабільність суспільства, завдаючи значних економічних збитків та ставлять під загрозу функціонування державних інституцій.

Вищеописана парадигма в узагальненому форматі створює необхідність належного аналізу зазначеного феномену. Актуальності даному процесу додає протидія російській військовій агресії Україною в умовах воєнного стану, регламентованого Указом Президента України № 64/2022 від 24.02.2022 р. Про введення воєнного стану в Україні. Повномасштабне вторгнення рф до України є викликом як щодо захисту національної критичної інфраструктури та забезпечення функціонування усіх реєстрів, так і стратегічним завданням у контексті безпеки інфраструктури, що забезпечує повноцінне функціонування держави та, таким чином, має статус критичної.

Потрібно відмітити, що характерним та притаманним для скоєння атак по критичній інфраструктурі в умовах сьогодення є розмивання відповідальності за такі дії. Саме через це, ми пропонуємо сконцентруватися у основній частині зазначеного дослідження на законодавчих особливостях регулювання даного кластеру в Україні, США та ЄС з метою виявлення позитивних та негативних тенденцій процесу, що покликаний сприяти превенції правопорушень у зазначеній галузі.

Аналіз останніх досліджень і публікацій. Кримінальна відповідальність за скоєння атак по об’єктах критичної інфраструктури як категорія доктринального інтересу розглядалася в українській та, одночасно, іноземній парадигмах аналізу.

Серед представників української доктрини пропонуємо насамперед звернути увагу на таких науковців, як О. Предместніков, С. Кучерина, А. Мельниченко, О. Таран та О. Сандул. В рамках зазначених праць, зокрема, розглянуто питання етимологічного розуміння атак на критичну інфраструктуру, особливості атак на критичну інфраструктуру в кримінально-правовому аспекті, проаналізовано види атак на критичну інфраструктуру з точки зору їхньої криміногенності та, водночас, здійснено дослідження проблем кримінальної відповідальності за атаки, здійснені щодо об'єктів критичної інфраструктури, агресором (на прикладі України).

Іноземні дослідження у зазначеному науковому спектрі, в свою чергу, представлені науковими напрацюваннями таких авторів, як Е. Вігано, М. Лої, Е. Ягмаель, А. Карло, К. Гірз та ін. У зазначених дослідженнях, зокрема, приділяється увага питанню співвідношення понять «критична інфраструктура» та «кібернетична безпека», а також, окрім понятійно-категоріального осмислення кримінальної відповідальності за скоєння атак по об'єктах критичної інфраструктури у причинно-наслідковій моделі, розглядаються особливості стратегічного значення захисту критичної інфраструктури від протиправних зловживань якраз-таки у форматі визначення таких дій кримінально караними та формування щодо них контексту криміногенності.

Мета статті — аналіз сучасного стану правового регулювання кримінальної відповідальності за атаки на критичну інфраструктуру, визначення основних проблем у цій сфері та обґрунтування необхідності вдосконалення законодавства України в даній галузі пристосовно до законодавства країн-партнерів (таких розвинених держав світу, як США та ЄС, зокрема).

Виклад основного матеріалу. Першочергової необхідності у контексті розуміння та наукового аналізу кримінальної відповідальності за скоєння атак по об'єктах критичної інфраструктури набуває безпосереднє наукове розуміння даного явища з точки зору теорії.

Так, наприклад, у праці-описі проблематики атак на критичну інфраструктуру з позиції їхньої криміногенності та кримінальної караності, а також кібернетичної природи представник ійськово-морська служба кримінальних розслідувань (NCIS) та Спільний центр кіберзахисту НАТО передового досвіду (CCDCOE) К. Гірз [1] відмітив, що кримінальна відповідальність за скоєння атак на об'єкти критичної інфраструктури охоплює сукупність правових норм, які передбачають покарання за дії, спрямовані на порушення нормального функціонування об'єктів критичної інфраструктури, що мають ключове значення для безпеки держави, суспільства та окремих громадян.

Персонально можемо погодитися із вищезапропонованим визначенням та розумінням етимології кримінальної відповідальності за скоєння атак по об'єктах критичної інфраструктури, відзначивши, що узагальнене моделювання практичної складової останніх та реагування держав на подібні

протиправні дії носить переважно індивідуалізований характер та не підлягає певному юридичному правилу.

Нижче, відтак, ми пропонуємо зосередитися на особливостях формування підвалин кримінальної відповідальності за скоєння атак по об'єктах критичної інфраструктури у національних законодавствах — України, США та ЄС.

Перш за все, нагальної необхідності у контексті огляду проблематики кримінальної відповідальності за скоєння атак по об'єктах критичної інфраструктури в Україні набуває визначення національним законодавцем понять «критична інфраструктура» та поділ критичної інфраструктури за типами пропорційно виконанню ними сегментованих завдань із життєзабезпечення державного функціонування. Так, відповідно до п. 9 ч. 1 ст. 1 Закону України «Про критичну інфраструктуру» № 1882-IX, під останньою запропоновано розуміти сукупність об'єктів критичної інфраструктури згідно із нормативною класифікацією, а у п. 4 ст. 9 зазначеного Закону до таких віднесено, зокрема, державне адміністрування, енергозабезпечення, водопостачання та водовідведення, охорону здоров'я, інформаційні послуги, електронні комунікації, фінансові послуги, транспортне забезпечення, оборону, державну безпеку, цивільний захист населення тощо [2]. Відповідно, саме атаки на зазначеного виду категорії об'єктів, що визначені у законодавстві України як критично-інфраструктурні, і буде вважатися порушенням (прямим або опосередкованим) нормативних приписів (наявних прямих або, знову-таки, аналогово-правових).

Архітектура нормативно-правовоого регулювання настання відповідальності за скоєння атак по об'єктах критичної інфраструктури в Україні базується на Кримінальному кодексі України № 2341-III, а також — Законі України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII та Законі України «Про критичну інфраструктуру» № 1882-IX. Розглянемо положення зазначених актів законодавства у зазначеному контексті детальніше.

Так, наприклад, у ст. 361 Розділу XVI Кримінального кодексу України № 2341-III (Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку) питання кримінальної відповідальності за скоєння атак по об'єктах критичної інфраструктури розглянуті у полі насамперед несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж [3]. Тобто, можна говорити про наявність колізії, котра полягає у тому, що фактично національний законодавець у даному випадку лише побічно слідує загальній концепції розуміння критичної інфраструктури, викладеної у ст. 9 Розділу III Закону України «Про критичну інфраструктуру» № 1882-IX, положення котрого були означені вище.

В свою чергу, у Законі України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII [4] аспект відповідальної за скоєння атак на критичну інфраструктуру України має аналового-правовий формат вираження, адже у ст. 6 даного нормативно-правового акту відзначено, що об'єкти критичної інфраструктури для цілей даного Закону детерміновані аналогічно зі ст. 9 Розділу III Закону України «Про критичну інфраструктуру» № 1882-IX. Одночасно, кібербезпеки та реалізація стандартів її забезпечення в Україні, згідно із положеннями ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, має власною ціллю саме формування сталості критично-інфраструктурного сектору. Це означає, що критична інфраструктура (окрім банківського сектору), спрямовується і координується за допомогою засобів інформаційно-комунікаційних технологій (ІКТ) та за певних умов може підлягати законодавчому регулюванню в рамках нормативних актів, відповідальних за діджиталізацію (як-от Закон України «Про електронні комунікації» № 1089-IX). Проте останній, на жаль, на часі не відзначається врегульованістю у означеному секторальному вимірі і не формує підстав відповідальності за атаки на критичну інфраструктуру.

Сукупність проаналізованої інформації дозволяє говорити про те, що кримінальна відповідальність за скоєння атак по об'єктам критичної інфраструктури в Україні наразі має розгалужене, в дечому — взаємовиключне коло розуміння та юридичного ототожнення. Не дивлячись на факт повномасштабної збройної військової агресії рф проти України, національний законодавець станом на зараз не вніс до відповідних законодавчих актів положень, що визначали б відповідальність держави-терориста за вчинення систематичних протиправних дій відносно об'єктів, що знаходяться у віданні та власності Української держави забезпечують належне функціонування не лише державного, але й соціально-економічного кластерів управлінсько-адміністративної діяльності.

Натомість, стандарти та особливості регулювання особливостей настання кримінальної відповідальності за скоєння атак по об'єктах критичної інфраструктури в США мають більш розгалужений та, водночас, сутнісно ефективний формат реалізаційного виконання. Нормативна рамка складається із Закону про комп'ютерне шахрайство та зловживання 1986 р. (Computer Fraud and Abuse Act of 1986), Патріотичного акту США 2001 р. (USA PATRIOT Act of 2001) та Закону про кібербезпеку та безпеку інфраструктури 2018 р. (Cybersecurity and Infrastructure Security Act (CISA) of 2018). Примітно, що протягом часу їхнього застосування до даних нормативних документів фактично не вносилися зміни, натомість деякі із зазначених документів були у подальшому доповнені прецедентами.

Наприклад, у Законі про комп'ютерне шахрайство та зловживання 1986 р. (Computer Fraud and Abuse Act of 1986) [5] деталізовано відповідальність за

такі дії проти американської критичної інфраструктури, як комп'ютерне шпигунство (18 U.S.C. § 1030(a)(1)), порушення відносно скоєння протиправних дій щодо урядової, фінансової чи комерційної інформації (18 U.S.C. § 1030(a)(2)), здійснення посягань на урядові реєстри (18 U.S.C. § 1030(a)(3)), скоєння кібератак на урядові чи комерційні реєстри за допомогою наявних або викрадених паролів (18 U.S.C. § 1030(a)(6)) та ін. Видами кримінальної відповідальності є штрафи, позбавлення волі, конфіскація майна та заходи обмежень — залежно від ступеню тяжкості вчиненого злочину пропорційно негативному впливу на інтереси держави, державних реєстрів та населення, що може постраждати від некоректної роботи критичної інфраструктури.

Генеральною видозміною та сутнісним перепрофілюванням у контексті формування кримінальної відповідальності за скоєння атак на критичну інфраструктуру прямим чи опосередкованим способом у США після Закону про комп'ютерне шахрайство та зловживання 1986 р. (Computer Fraud and Abuse Act of 1986) став Патріотичний акт США 2001 р. (USA PATRIOT Act of 2001) [6]. У останньому в своїй основі було генералізовано заходи протидії тероризму та терористичним загрозам. У рамках даного процесу, зокрема, було впроваджено розширені можливості стеження правоохоронних органів, у тому числі шляхом прослуховування внутрішніх і міжнародних телефонних розмов та посилено покарання за терористичні злочини та розширено перелік дій, які кваліфікуватимуться як звинувачення в тероризмі, тобто матимуть власною ознакою криміногенність (Sec. 201, 202, 206; Sec. 202, 810, 814). Враховуючи, що атаки на критичну інфраструктуру за своєю ґенезою можна прирівняти до актів тероризму, адже останні посягають на національну безпеку держави, її економічний добробут та опції фінансової конвергентності бізнес-структур, вбачаємо зазначений нормативний акт одним із ключових у питаннях створення належної карти протидії даному виду загроз державності.

В свою чергу, Закон про кібербезпеку та безпеку інфраструктури 2018 р. (Cybersecurity and Infrastructure Security Act (CISA) of 2018) [7] у системі кримінального нормативного інструментарію протидії скоєнню атак по об'єктах критичної інфраструктури має на меті насамперед інформаційний складник. Так, у контексті приватно-публічної взаємодії у інформаційно-безпековій сфері з точки зору сутності даного процесу виділяємо положення Секції 4 даного нормативного акту (Sec. 4), де презюмується обов'язок держави надати юридико-правовий захист компаніям, установам та організаціям, що здійснюють власну діяльність у галузі передачі інформації та котрі повідомили про наявні факти або потенційні факти порушення інформаційного суверенітету держави. Цим американський законодавець де-факто впроваджує фактор тотожності між інформаційною та безпекою та національною безпекою, визначаючи таким чином першу складовою критичної інфраструктури. Хоча даним нормативним актом не передбачено кримінальної

відповідальності за дані дії, це сприяє розширенню розуміння посягань на критичну інфраструктуру держави як явища.

Натомість, прикладом практичного трактування законодавства, що детермінує кримінальну відповідальність за порушення специфічного законодавства, що, зокрема, стосується критичної інфраструктури в США можемо визнати судовий прецедент Van Buren v. United States, No. 19-783, 593 U.S. (2021) [8]. У рамках тлумачення застосування права щодо того, чи перевищення дозволеного використання комп'ютерної системи в межах доступу підпадає під кримінальну відповідальність, Верховний суд США дійшов висновку, що Закон про комп'ютерне шахрайство та зловживання 1986 р. (Computer Fraud and Abuse Act 1986) не охоплює випадки, коли особа мала законний доступ до комп'ютерної системи, але використовувала її з порушенням умов або політики, стосуючись лише оказій, коли особа отримує доступ до інформації, яку вона взагалі не мала права бачити, а не способу використання інформації, до якої доступ був дозволений (за матеріалами розгляду, американський поліцейський Н. Ван Бюрен був засуджений після того, як використав поліцейську базу даних для перевірки автомобільної інформації в обмін на гроші, що порушило політику та умови використання доступних йому ресурсів та було кваліфіковано як «перевищенням дозволеного доступу» відповідно до Sec. 1030(e)(6) CFAA).

На відміну від розгалуженого формату реалізації кримінальної відповідальності за скоєння атак на державні реєстри, котрі іменуються критичною інфраструктурою та, власне, критичну інфраструктуру як таку, що наявна у США, ЄС регламентує регулювання зазначеним простором за Директиви NIS 2 2022 р. (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [9].

У даному нормативному акті, зокрема, не встановлено кримінальної відповідальності за зазначені дії як такої, проте має місце стимулювання держав-членів до інтеграції власного законодавства за такими орієнтирами, як обов'язок держав-членів ухвалювати додаткові національні закони, які передбачають відповідальність за порушення, включаючи можливість кримінального переслідування за атаки на критичну інфраструктуру (ст. 3), можливість вжиття заходів щодо контролю та нагляду, зокрема обов'язки операторів критичних послуг і постачальників цифрових послуг дотримуватись стандартів кібербезпеки, а також механізми моніторингу їхньої діяльності та впровадження кримінальної відповідальності за невиконання зазначених положень (ст. 39) та, наостанок, презумпція обов'язку держав забезпечити запровадження санкцій за невиконання положень даного

законодавчого акту, включаючи ефективні, пропорційні та стримуючі штрафи, що надає можливості теоретичного запровадження кримінальної відповідальності (ст. 41) [9].

Як бачимо, особливості встановлення кримінальної відповідальності за скоєння атак по об'єктах критичної інфраструктури є варіативним питанням, що проєктується від нормативної бази, правової сім'ї, ролі та місця судового прецеденту в системі встановлення покарань. Приклади України, США та ЄС демонструють як залежність даного процесу від внутрішньо- та геополітичної ситуації, так і походження зазначеного кластеру публічно-нормативного регулювання від наявності потужних інструментів впливу на правопорушника (правопорушників) в умовах розмивання правового поля відповідного протиправного діяння.

Висновки. Аналіз ґенези та особливостей кримінальної відповідальності за скоєння атак по об'єктах критичної інфраструктури як явища та феномену дозволив дійти наступних умовиводів.

Нормативне регулювання процесу встановлення кримінальної відповідальності за скоєння атак по об'єктах критичної інфраструктури в Україні в умовах правового режиму воєнного стану не набуло належного рівня конкретизації та регуляційної здатності. Положення ст. 113 та ст. 361 Кримінальний кодекс України № 2341-III, а також ст. 1, ст. 9 Закону України «Про критичну інфраструктуру» № 1882-IX та ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII визначають лише основні засади протидії загрозам критичних ресурсів держави, проте прямо не регулюють питання відповідальності саме за атаки рф на критичну інфраструктуру в міжнародно-правовому вимірі.

У США та ЄС питання регулювання кримінальної відповідальності за скоєння атак по критичній інфраструктурі має більш деталізований характер. Окрім оглянутого нормативного інструментарію, у США є приклад активного застосування права (судовий прецедент Van Buren v. United States, No. 19-783, 593 U.S. (2021), яким трактується положення Sec. 1030(e)(6) Закону про комп'ютерне шахрайство та зловживання 1986 р. (Computer Fraud and Abuse Act 1986), що регулює питання відмітності та криміногенності діяння, спрямованого на критичні файли та вузли держави, що і є її критичною інфраструктурою. В свою чергу, монорегулювання зазначеного питання у ЄС передбачає використання ст. 3, ст. 39, ст. 41 Директиви NIS 2 2022 р. (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) як керівної для держав-членів Союзу у контексті створення належної архітектури управління сектором.

***Література*:**

1. Geers, K. The Cyber Threat to National Critical Infrastructures: Beyond Theory. Information Security Journal: A Global Perspective. Vol. 18 (1-7). 2009. 10 p.
2. Закон України «Про критичну інфраструктуру» № 1882-IX від 16.11.2021 р. (ред. від 21.09.2024 р.). Відомості Верховної Ради. Режим доступу : https://zakon.rada.gov.ua/laws/show/1882-20#Text
3. Кримінальний кодекс України № 2341-III від 05.04.2001 р. (ред. від 26.12.2024 р.). Відомості Верховної Ради. Режим доступу : https://zakon.rada.gov.ua/laws/show/2341-14#Text
4. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р. (ред. від 28.06.2024 р.). Відомості Верховної Ради. Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. US Congress. H.R.4718 - Computer Fraud and Abuse Act of 1986. USC official website. Режим доступу : https://www.congress.gov/bill/99th-congress/house-bill/4718
6. US Congress. H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. USC official website. Режим доступу : https://www.congress.gov/bill/107th-congress/house-bill/3162/text
7. US Congress. Cybersecurity and Infrastructure Security Act (CISA) of 2018. USC official website. 20 p.
8. Supreme Court of the United States. Van Buren v. United States, No. 19-783, 593 U.S. (06/03/2021). SCUS official website (Resolution). 2020. 37 p.
9. EurLex. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). EurLex official website. Режим доступу : https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

References:

1. Geers, K. The Cyber Threat to National Critical Infrastructures: Beyond Theory. Information Security Journal: A Global Perspective. Vol. 18 (1-7). 2009. 10 p.
2. Law of Ukraine “On Critical Infrastructure” No. 1882-IX of 11/16/2021 (as amended on 09/21/2024). Verkhovna Rada Bulletin. Access mode: https://zakon.rada.gov.ua/laws/show/1882-20#Text
3. Criminal Code of Ukraine No. 2341-III of 04/05/2001 (as amended on 12/26/2024). Verkhovna Rada Bulletin. Access mode: https://zakon.rada.gov.ua/laws/show/2341-14#Text
4. Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" No. 2163-VIII of 05.10.2017 (as amended on 28.06.2024). Verkhovna Rada Bulletin. Access mode: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. US Congress. H.R.4718 - Computer Fraud and Abuse Act of 1986. USC official website. Access mode: https://www.congress.gov/bill/99th-congress/house-bill/4718
6. US Congress. H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. USC official website. Mode of access: https://www.congress.gov/bill/107th-congress/house-bill/3162/text
7. US Congress. Cybersecurity and Infrastructure Security Act (CISA) of 2018. USC official website. 20 p.m.
8. Supreme Court of the United States. Van Buren v. United States, No. 19-783, 593 U.S. (03/06/2021). SCUS official website (Resolution). 2020. 37 p.
9. EurLex. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). EurLex official website. Access mode: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng