УДК 342.951

СТЕЖКО С.М., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-7386-1221.
ФИЦА В.М., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-6590-8082.

КІБЕРБЕЗПЕКА ЯК ВАЖЛИВИЙ ФАКТОР ЗАБЕЗПЕЧЕННЯ ЖИТТЄДІЯЛЬНОСТІ ВІТЧИЗНЯНОЇ ЕНЕРГЕТИЧНОЇ ГАЛУЗІ

Анотація. *Досліджено питання забезпечення кібербезпеки вітчизняної енергетичної галузі. Розглянуто стратегічні засади підвищення рівня кіберстійкості комунікаційних та технологічних систем підприємств енергетичної галузі. Висвітлено позитивний досвід США та Великобританії щодо організаційно-правових засад запобігання та мінімізації посягань на об'єкти критичної енергетичної інфраструктури. Деталізовано методологію аналізу кіберзагроз та оцінки ризиків порушення кібербезпеки об'єктів енергетичної інфраструктури. Узагальнено питання забезпечення кібербезпеки енергетичних об'єктів та автоматизованих систем. Висвітлено ініціативи та напрями діяльності РНБО України в контексті розбудови кібербезпеки енергетичних систем. Визначено шляхи удосконалення формування концептуальних засад забезпечення кібербезпеки в енергетичному секторі України.*

Ключові слова: *енергетична галузь, кібербезпека, кіберстійкість, державна безпекова політика, кібератака, кіберзагроза, цифровізація, критична інфраструктура.*

Summary. *The issue of cybersecurity of the domestic energy industry has been studied. The strategic principles of increasing the level of cyber resilience of communication and technological systems of energy industry enterprises are considered. The positive experience of the United States and the United Kingdom on the organizational and legal framework for preventing and minimizing encroachment on critical energy infrastructure is highlighted. The methodology of cyber threat analysis and risk assessment of cybersecurity violations of energy infrastructure facilities is detailed. The issue of cybersecurity of energy facilities and automated systems is generalized. The initiatives and directions of activity of the National Security and Defense Council of Ukraine for the purpose of development of cybersecurity of power systems are opened. The directions of the improvement to the formation of conceptual foundations for cybersecurity in the energy sector of Ukraine are identified.*

Keywords: *energy industry, cybersecurity, cyberresilience, state security policy, cyber attack, cyber threat, digitalization, critical infrastructure.*

Аннотация. *Исследованы вопросы обеспечения кибербезопасности отечественной энергетической отрасли. Рассмотрены стратегические основы повышения уровня киберустойчивости коммуникационных и технологических систем предприятий энергетической отрасли. Освящен позитивный опыт США и Великобритании касаемо организационно-правовых основ предотвращения и минимизации посягательств на объекты критической энергетической инфраструктуры. Детализирована методология анализа киберугроз и оценки рисков нарушения кибербезопасности объектов критической энергетической инфраструктуры. Раскрыты инициативы и направления деятельности СНБО Украины в контексте развития кибербезопасности энергетических систем. Обобщены направления усовершенствования формирования концептуальных основ обеспечения кибербезопасности в энергетическом секторе Украины.*

Ключевые слова*: энергетическая отрасль, кибербезопасность, киберустойчивость, государственная политика безопасности, кибератака, киберугрозы, цифровизация, критическая инфраструктура.*

Постановка проблеми. Важливою складовою національної безпеки України є енергетична безпека як стратегічна галузь економіки нашої держави. Безперебійне функціонування енергетичної галузі України є запорукою стабільних процесів підтримання енергонезалежності, успішного процвітання України як європейської держави. Адже докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення дієвої галузевої системи забезпечення кібербезпеки енергетичних об'єктів як важливої складової системи національної безпеки. На цьому фоні розвиток інтелектуальних енергетичних систем посилює проблему забезпечення кібербезпеки в енергетиці, особливо в умовах появи нових гібридних загроз та прагнень політичного керівництва РФ дестабілізувати ситуацію в енергетичному секторі Україні.

У положеннях Стратегії енергетичної безпеки України [1] деталізовано перелік загроз енергетичній безпеці, серед яких вагому роль відіграє поширення у світі коронавірусу, що зумовлює виникнення цілого ряду викликів та ризиків функціонування вітчизняного енергетичного сектору. Оскільки запровадження карантинних заходів у всіх країнах призводить до зменшення обсягів споживання енергії та енергоресурсів і, як наслідок, погіршення фінансово-економічних показників роботи суб'єктів енергетичного ринку. Крім того, в умовах епідемії перед енергетичним сектором виникає додаткове завдання – забезпечення стабільності надання послуг з енергопостачання в умовах карантинних заходів та обмежень.

Викладене зумовлює потребу активізації діяльності держави за напрямом забезпечення кібербезпеки та фізичної безпеки критичної інфраструктури енергетичного сектору, оскільки забезпечення безпеки критичної інфраструктури в енергетиці – одна з найбільших проблем цієї стратегічної галузі вітчизняної економіки. Це підтверджується й положеннями нещодавно схваленої на державному рівні Концепції забезпечення національної системи стійкості [2], відповідно до якої важливим завданням держави є прискорення розроблення та впровадження заходів з підвищення рівня кіберстійкості комунікаційних та технологічних систем, які забезпечують функціонування органів державної влади, об'єктів критичної інфраструктури, зокрема в енергетиці. Потребує активізації процес підвищення рівня кіберстійкості критичної інфраструктури енергетичного сектору України. За таких умов визначення ефективних шляхів удосконалення кібербезпеки в енергетичній галузі є необхідним та доцільним, включаючи розробку алгоритмів забезпечення розумного балансування усієї енергетичної системи та її надійного захисту.

Результати аналізу наукових публікацій. Останнім часом проблемні питання розбудови та управління вітчизняною критичною інфраструктурою на науковому рівні досліджували такі фахівці, як: С. Вдовенко та Ю. Даник [3], І. Мальцева, Ю. Черниш, В. Овсянніков [4], О. Мельничук [5], С. Теленик [6], В. Ємельянов [7] тощо. У загальному плані, питання тлумачення кібербезпеки розглядав О. Баранов [8], забезпечення кібербезпеки та її складових були предметом праць таких науковців, як І. Діориця [9], Р. Лук'янчук [10], Н. Ткачук [11]. Проте, нажаль, у працях згаданих науковців не було приділено достатню увагу питанням забезпечення кібербезпеки в енергетичному секторі, що підкреслює актуальність цієї тематики.

Метою статті є актуалізація проблем забезпечення кібербезпеки вітчизняної енергетичної галузі, визначення перспектив доцільності схвалення на державному рівні концептуальних організаційно-правових засад забезпечення кібербезпеки в енергетичному секторі України.

Виклад основного матеріалу. Світова енергетика слідує тенденціям децентралізації у виробництві електроенергії, а також декарбонізації. Тільки тотальна цифровізація дозволить створити комплексну енергетичну систему. Величезна кількість датчиків в сучасних енергетичних системах дозволяє збирати великі обсяги даних, забезпечуючи взаємодію на абсолютно новому рівні і в новому масштабі. Штучний інтелект і аналітика великих даних докорінно змінюють процес прийняття управлінських рішень. Найважливішими факторами успіху в цифровій економіці є гнучка інфраструктура і системи, що дозволяє адаптуватися до вимог майбутнього. Крім того, захист даних фізичних осіб і підприємств має першочергове значення для мінімізації ризику кібератак.

В сучасних умовах загрозливого масштабу набувають непоодинокі спроби стороннього впливу на стійкість функціонування енергетичних систем країни, насамперед з використанням можливостей технічних та технологічних новацій у розвитку енергетичних технологій. Тобто особливого значення набуває необхідність забезпечення безпеки ланцюга постачання технологій, обладнання, а також сервісних послуг щодо їх обслуговування. Крім того, збільшення кількості та рівня складності автоматизованих систем управління, керованих віддалено через інформаційні канали, формує високі ризики здійснення різноманітних кібератак. Потужні кібератаки такого формату, спрямовані на відповідні системи, можуть спричинити критичні наслідки у функціонуванні енергетичної інфраструктури. Таким чином, не можна недооцінювати масштаби та наслідки кіберзагроз, які посягають на об’єкти критичної інфраструктури енергетичного сектору.

Проникнення сучасних цифрових технологій в енергетику, як і в інші сфери зростає. Паралельно виникають загрози, пов’язані із суцільною цифровізацією. Країни світу, де “розумні” мережі і цифрові технології розвиваються швидше, змушені вживати дедалі більш потужних заходів з метою захисту власної енергосистеми, оскільки останнім часом на інфраструктурні енергетичні об’єкти по всьому світу здійснюються серйозні кібератаки, які спричиняють масштабні відключення електроенергії. Однією із найбільш серйозних ініціатив в зазначеному контексті став Акт США про безпеку енергетичної інфраструктури (Securing Energy Infrastructure Act) [12]. В американському Акті про безпеку енергетичної інфраструктури враховується, в тому числі, й концепція фізичної ізоляції, яка передбачає кіберзахист локальних мереж. Але цю концепцію можливо обійти, як демонструє досвід поширення вірусу Stuxnet, який успішно атакував ядерні об’єкти Ірана ще у 2010 році, уразивши комп’ютерні мережі, які керували їх роботою. У зв’язку з чим “розумні технології”, які контролюють роботу тих чи інших об’єктів залишаються потенційно уразливими для кібератак, навіть якщо вони фізично ізольовані від мережі Інтернет. Передбачувано, що причиною розробки цього документу стала потужна кібератака на енергосистему України ще у 2015 році, яка залишила без електроенергії понад 200 тис. осіб. Слід вказати, що у травні 2021 року Міністерство енергетики США оголосило про 100-денний план щодо посилення кібербезпеки електроенергетичної інфраструктури. Цей план передбачає активну співпрацю міністерства енергетики, приватних компаній, а також агентства з кібербезпеки й інфраструктурної безпеки з метою реагування на кіберзагрози.

Адже широке застосування старих технологій для захисту від втручань хакерів – це логічна стратегія, яка використовується в різних сферах енергетичного сектора.

Наприклад, для моніторингу, експлуатації, контролю та захисту ядерних ректорів (в тому числі і в Україні) використовуються як цифрові, так і аналогові системи. Цифрові активи, критично важливі для систем підприємства, є ізольованими від зовнішніх мереж та Інтернету. Це забезпечує їхній захист від багатьох кіберзагроз. Таким чином, саме низька цифровізація і відсутність цифрових комунікацій, які зв'язують той чи інший актив з іншими інформаційними системами, можуть вберегти енергетичний об'єкт від кіберзагроз. Ручне управління об'єктами енергетичної інфраструктури у рази безпечніше в плані реагування на потенційні кіберзагрози, але дорожче обходиться і вимагає наявності кваліфікованого персоналу. Крім того, ручне управління може бути менш безпечними для співробітників того чи іншого енергопідприємства.

Проте останньою світовою тенденцією розвитку ринку енергетики стало масштабне запровадження новітніх технологій, зокрема "Smart Grid" (розумні мережі електропостачання). "Smart Grid" – набір технологій, які перетворюють енергетичну інфраструктуру на сучасну цифрову систему. Тобто електронне керування параметрами електроенергії, керування її виробництвом і розподілом є важливими аспектами інноваційної розумної енергосистеми. Запровадження інноваційних технологій розумних енергосистем також передбачає фундаментальний перегляд сфери послуг енергетики, хоча типове використання цього терміна фокусується на технічній інфраструктурі [13]. Основними очікуваними результатами впровадження цієї концепції мають стати контрольованість та автоматизація процесів управління енергетичною системою, які мають забезпечувати її високу надійність та високі економічні показники. Інтелектуальна енергетична система передбачає інтеграцію енергетичних систем з новими інформаційно-комунікаційними технологіями та цілісною багаторівневою автоматизованою системою управління. Підвищення рівня тотального запровадження інтелектуальних енергетичних систем посилює проблему забезпечення кібербезпеки.

Таким чином, кібербезпека є життєво важливим фактором існування енергетичного комплексу та його складових. В сучасних умовах критично важливим є не лише запровадження новітніх технологій забезпечення енергоефективності, але й виконання завдання щодо захисту енергетичної системи від реальних та потенційних загроз у кіберпросторі. Кібератаки можуть бути спрямовані як на об'єкти генерації енергоресурсів, так і на об'єкти транспортування та споживання. Найбільш уразливою ланкою є системи управління та диспетчеризації енергетичних систем. При цьому уразливість буде постійно посилюватися по мірі поширення концепції та технологій "Smart Grid".

Проблеми кібербезпеки енергетичних систем посилюються тим, що понад 75 % енергетичного обладнання має іноземне походження, не враховуючи 100 % комп'ютерного та програмного забезпечення. На цьому фоні важливим завданням є забезпечення безпеки критичної інфраструктури й зокрема енергетичної інфраструктури, що являє собою сукупність енергетичних об'єктів та систем енергетики, включаючи енергетичні транспортні магістралі. Тобто подальше зростання ролі ІТ-технологій обумовлює виключне значення, якого набуває кібербезпека для забезпечення безпеки та стійкості функціонування енергетичної галузі.

Методологія аналізу кіберзагроз та оцінки ризиків порушення кібербезпеки об'єктів енергетичної інфраструктури включає: поточний аналіз стану кіберзагроз об'єктів енергетичної інфраструктури, формування сценаріїв ймовірних екстремальних ситуацій, пов'язаних з реалізацією кіберзагроз, моделювання та оцінювання ризиків порушення кібербезпеки енергетичної інфраструктури. Критерії захищеності вказаних об'єктів також включають інструменти попередження та запобігання некоректних або помилкових дій та

процесів, потенційну уразливість програмного забезпечення, яка непомітна на етапах проведення тестування. До переліку ризиків, які специфічні для підприємств енергетичної галузі, належать: використання в автоматизованих системах застарілого програмного забезпечення, обладнання та комунікаційних протоколів, які не передбачають можливості та вірогідності щодо кіберзагроз; наявність адміністративних та технологічних труднощів оновлення програмного забезпечення; неконтрольоване підключення автоматизованої системи управління до мережі Інтернет; можливий доступ "сторонніх" компаній до технологічної мережі об'єкта критичної інфраструктури. Енергетична галузь залишається найбільш уразливою з позиції ризиків техногенних катастроф. На цьому фоні вірогідним та прогнозованим є збільшення кількості кіберзагроз щодо енергетичної галузі. Це логічно особливо в умовах глибокої інформатизації та цифровізації. Також очікується тенденційна зміна ландшафту таких загроз.

Доцільно враховувати той факт, що підприємства енергетичної галузі у переважній більшості перебувають у стані модернізації, особливо щодо систем релейного захисту та автоматики. Як наслідок цих процесів виникає чимало частково реконструйованих об'єктів із різноманітними рівнями цифровізації вторинних систем та різними рівнями доступу як до програмних пристроїв, так і систем передачі сигналів й управління модулями. В результаті цього виникають непрямі проблеми, пов'язані із кібербезпекою, які не призводять до моментального виникнення несправностей, але які мають накопичувальний характер та стають "бомбою уповільненої дії". Тому на підприємствах енергетичної галузі кожен встановлений інтелектуальний електронний пристрій повинен мати працездатне програмне і мікропрограмне забезпечення. Захисні пристрої оснащуються комунікаційним і основним модулями, кожен з окремим мікропрограмним забезпеченням. Маршрутизатори мають власне мікропрограмне забезпечення, а на ПК встановлюється операційна система і додаткове програмне забезпечення. Для забезпечення кібербезпеки і функціональної безпеки необхідно здійснювати постійне оновлення компонентів такого мікропрограмного і програмного забезпечення.

Таким чином, питанням кібербезпеки енергетичних об'єктів та автоматизованих систем необхідно приділяти особливу увагу. Основною метою вирішення цієї проблеми є забезпечення стабільного та надійного функціонування відповідних систем та модулів при одночасному зменшенню ризиків та ймовірних збитків. Загрози кібератак безумовно існують, проте їх вірогідність та спричинені збитки необхідно оцінювати застосовуючи до кожної системи окремо. Також велике значення для забезпечення кібербезпеки має захист периметру мережі енергетичного об'єкта (фізичної та інформаційної). Зменшенню ризиків також сприяє запровадження заходів організаційного характеру, здійснення моніторингу мереж системи автоматичного управління, періодичний аналіз стану захищеності.

Враховуючи наявні виклики та ризики світового масштабу МАГАТЕ опікується вказаною проблематикою у зв'язку з чим розробило стандарт стосовно посилення рівня кібербезпеки на АЕС у 2020 році. Цей стандарт дозволить грамотно проводити тренування та навчання з комп'ютерної безпеки. Він враховує позитивні практики та напрацювання в системах захисту, а також містить рекомендації для оперативного реагування на атаки, що можуть виникнути. Таким чином, вказаний документ стане інструкцією для тренувань з кібербезпеки в атомній енергетиці. Забезпечення безпеки критичної енергетичної інфраструктури представляє собою концепцію протидії серйозним загрозам роботи важливих об'єктів інфраструктури та об'єктів підвищеної загрози в регіоні чи державі, особливо в умовах розповсюдження інформаційних

технологій, тоді як динамічний розвиток інформаційних технологій обумовлює появу нових видів кібератак, націлених на об'єкти національної енергосистеми.

У липні 2021 року Великобританія схвалила на державному рівні Стратегію цифровізації вітчизняної енергосистеми та план заходів щодо її реалізації [14]. Достатня увага приділяється саме кібербезпеці енергетичних систем. До 2050 року в енергетичному секторі планується запровадити мільйони низьковуглецевих технологій, включаючи сонячні батареї, теплові насоси та електромобілі. На цьому фоні роль та значення кібербезпеки потужно зростає.

Розуміючи необхідність посилення стану кібербезпеки, у свою чергу, Міністерство енергетики України як профільний орган має намір створити галузевий операційний центр кібербезпеки (Security operations center, SOC). Операційний центр безпеки — це об'єкт, де корпоративні інформаційні системи (веб-сайти, додатки, бази даних, центри обробки даних, сервери, активне мережеве обладнання, комп'ютери та інше кінцеве обладнання) контролюються, оцінюються та захищаються. Це означає запровадження та розбудову кібер-фізичної інфраструктури для інформаційних систем децентралізованого інтелектуального управління енергосистемами. Одним із стратегічних завдань галузевого операційного центру кібербезпеки є навчання та інформування користувачів, зокрема, прищеплення їм культури кібербезпеки, а також оперативне їх інформування про виникнення загроз та план дій на випадок скоєння кібератак.

Проблематикою забезпечення кібербезпеки енергетичної галузі останнім часом також переймається і РНБО України. 22 грудня 2020 року Укренерго підписало Меморандум з Радою національної безпеки та оборони України про взаємодію та співробітництво у сфері кібербезпеки та кіберзахисту. Співпраця здійснюватиметься шляхом обміну технічною та технологічною інформацією у сфері забезпечення кібербезпеки, зокрема індикаторами кіберзагроз, інформацією про кіберінциденти тощо. На виконання положень меморандуму Міністерство енергетики України планує створити проєктний офіс для залучення міжнародної технічної допомоги, провести аудит поточного стану кібербезпеки в енергетиці та організувати секторальний центр кібербезпеки критичної інфраструктури енергетичного сектору.

29 квітня 2021 року в Апараті Ради національної безпеки і оборони України у рамках співпраці між Національним координаційним центром кібербезпеки при РНБО України (НКЦК) і Фондом цивільних досліджень та розвитку Сполучених Штатів Америки (CRDF Global) (за підтримки Державного департаменту США) відбулося третє засідання Національного кластера з кібербезпеки [15]. За підсумками зустрічі було визначено, що розбудова цілісної системи забезпечення кібербезпеки ОКІ держави вимагає також чіткого визначення переліку їх ІТС, створення та ведення загальнодержавного реєстру ОКІ, проведення аудиту інформаційної безпеки на об'єктах критичної інфраструктури, а також ухвалення відповідного законодавства.

29 – 30 вересня 2021 року в Одесі відбулося виїзне засідання (у рамках конференції Energy CyberCon 2021) Робочої групи з питань розбудови кіберзахисту об'єктів критичної інфраструктури енергетичної галузі Міністерства енергетики України, на якому було презентовано кращі проекти захисту енергетичного сектору від провідних виробників та постачальників рішень у сфері цифровізації та кібербезпеки. Також учасники заходу обмінялися думками щодо місця секторальної кібербезпеки в організаційно-технічній моделі національної кібербезпеки, стандартів кібербезпеки в енергетичному секторі та законодавства в сфері критичної інфраструктури. Слушно висловився з цього приводу заступник Секретаря РНБО С. Демедюк щодо необхідності посилення координації дій державних та приватних суб'єктів енергетичної галузі у

питаннях забезпечення надійного кіберзахисту. На його переконання, критично важливим є не лише запровадження новітніх технологій забезпечення енергоефективності, а й захист енергетичної системи від загроз у кіберпросторі [16].

Таким чином, кібербезпека енергетичної галузі перебуває у фокусі уваги державного апарата, сектору безпеки і оборони та приватних компаній. Атаки на об'єкти критичної енергетичної інфраструктури можуть привести до масштабних катастрофічних наслідків для галузі, екології та економіки країни. Ситуація з атакою у травні 2021 року на американську трубопровідну систему Colonial Pipeline переконливо це продемонструвала. Атака зупинила роботу всіх трубопроводів системи на цілих 5 днів. В результаті атаки Президент Д. Байден оголосив надзвичайний стан, а за оцінками експертів – це була найбільша успішна кібератака на нафтову інфраструктуру в історії США.

Враховуючи виклики та загрози світового масштабу, Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб'єктів забезпечення кібербезпеки [17].

Висновки.

Сучасне суспільство практично повністю залежить від стану захищеності інформації та кібер-інфраструктури у всіх сферах життєдіяльності. Україна вже тривалий час є об'єктом регулярних і масштабних кібератак, які ставлять під загрозу стабільну роботу критичної інфраструктури. На території України в кожному регіоні є енергетичні системи, які відносяться до об'єктів критичної інфраструктури. Проблема забезпечення кібербезпеки в енергетичній галузі актуалізується та посилюється у зв'язку з поширенням практичного впровадження концепції інтелектуальних енергетичних систем. На жаль, прогнозується подальша уразливість енергетичної інфраструктури та її об'єктів від кібератак, несанкціоноване втручання у роботу вітчизняних енергосистем та здійснення її збоїв, що провокує посилення їхньої кіберстійкості. Кіберстійкість енергетичної критичної інформаційної інфраструктури – це такий її стан, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз. Вітчизняна енергетична галузь не є виключенням. Однією із важливих складових енергетичної галузі України є система управління, яка відіграє важливу роль функціонування усього енергетичного комплексу України. Автоматизована система управління вітчизняною енергетичною галуззю повинна бути стійкою до будь-яких кібервпливів та мати сучасну комплексну систему протидії кібератакам.

Гібридна війна РФ проти України, елементом якої є також акції кібервпливу, залишається на сьогодні найбільшою загрозою національній безпеці держави. В цьому контексті важливим елементом функціонування національної системи кібербезпеки є забезпечення кібербезпеки об'єктів критичної інфраструктури, зокрема, енергетичного сектору. За таких умов саме кібербезпека має стати одним з пріоритетів розвитку підприємств енергетичної галузі. Підвищення рівня кіберстійкості критичної інфраструктури енергетичного сектору України є важливим стратегічним завданням держави.

Враховуючи викладене, доцільно прискорити схвалення на державному рівні Концепції забезпечення кібербезпеки в енергетичному секторі України на 2022 − 2024 роки. Серед інших завдань Концепції кібербезпеки в енергетичному секторі виділяється: прискорення впровадження сучасних технологій кібербезпеки на базі європейських та

євроатлантичних принципів та стандартів; врегулювання нормативно-правових і організаційно-технічних аспектів галузевої кібербезпеки в енергетичній галузі; впровадження механізмів моніторингу та оцінки якості виконання рекомендацій та вимог підприємствами та суб'єктами забезпечення кібербезпеки в енергетиці; впровадження засад державно-приватного та приватно-публічного партнерства тощо.

Використана література

1. Про схвалення Стратегії енергетичної безпеки: розпорядження Кабінету Міністрів України від 4.08.21 р. № 907. URL: https://zakon.rada.gov.ua/laws/show/907-2021-р#Text
2. Концепція забезпечення національної системи стійкості: Указ Президента України від 27.09.21 р. № 479/2021: URL: https://www.president.gov.ua/documents/4792021-40181
3. Даник Ю.Г., Вдовенко С.Г. Ланцюгові ефекти в кібердіях: зб. наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2019. № 64. С.71-90.
4. Мальцева І., Черниш Ю., Овсянніков В. Аналіз методик оцінки кіберстійкості критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2021. № 12. Т. 4. С. 29-35.
5. Мельничук О. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об'єктів. *Державне управління та місцеве самоврядування*. 2019. № 3 (42). С. 13-27.
6. Теленик С.С. Адміністративно-правове регулювання державної системи захисту критичної інфраструктури України: автореф. дис. …д-ра юрид. наук: спеціальність 12.00.07. Запоріжжя, 2021. 37 с.
7. Ємельянов В.М., Бондар Г.Л. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. *Публічне управління та регіональний розвиток*. 2019. № 5. С. 493-523.
8. Баранов О.А. Про тлумачення та визначення поняття "кібербезпека". *Правова інформатика*. № 2(42)/2014. С. 54-62.
9. Діордиця І.В. Адміністративно-правове регулювання кібербезпеки України: автореф. дис. …д-ра юрид. наук: спеціальність 12.00.07. Запоріжжя, 2018. 40 с.
10. Лук'янчук Р.В. Державне стратегічне планування у сфері забезпечення кібербезпеки: реалії сьогодення. *Вісник Національної академії державного управління при Президентові України*. *Серія: Державне управління*. 2016. № 3. С. 131-137.
11. Ткачук Н. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134.
12. Securing Energy Infrastructure Act of the USA 2021. URL: https://www.congress.gov/bill/116th-congress/senate-bill/174
13. Релейний захист та кібербезпека енергетичних систем: підручник / Є.І. Сокол та ін. ; під заг. ред. проф. Є.І. Сокола. Харків: Панов А.М., 2019. 389 с.
14. Digitalising our energy system for net zero. Strategy and Action Plan 2021. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004011/energy-digitalisation-strategy.pdf
15. В Апараті РНБО України відбулося третє засідання Національного кластера з кібербезпеки. URL: https://www.rnbo.gov.ua/ua/Diialnist/4887.html
16. Демедюк С. Кібербезпека сьогодні – життєво важливий фактор існування енергетичної галузі. URL: https://www.rnbo.gov.ua/ua/Diialnist/5024.html
17. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~