УДК 351.81

ЦЯПА С.М., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-9263-1050.

ПРАВОВЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК

Анотація. *У статті розглядаються правові та організаційні аспекти забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак. Звертається увага на позитивний досвід США у забезпеченні стійкості об'єктів критичної інфраструктури. Аналізуються положення нової Стратегії кібербезпеки України, одним з пріоритетів якої визначено удосконалення нормативного забезпечення з питань кіберзахисту об'єктів критичної інформаційної інфраструктури. Відзначаються недоліки попередньої Стратегії кібербезпеки України 2016 року. Міститься детальний аналіз законодавчих актів та ініціатив з питань забезпечення кібербезпеки. Розглядаються загальні вимоги до кіберзахисту об'єктів критичної інфраструктури. На підставі аналізу чинного законодавства з питань забезпечення кібербезпеки України запропоновані шляхи удосконалення правового та організаційного забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак.*

Ключові слова: *кіберпростір, кібератака, об'єкти критичної інфраструктури, кіберзахист об'єктів критичної інфраструктури, правове забезпечення, організаційне забезпечення.*

Summary. *The article considers the legal and organizational aspects of ensuring the protection of the critical information infrastructure from cyberattacks. Attention is drawn to the positive experience of the United States in ensuring the resilience of the objects of critical infrastructure. The provisions of the new Cyber Security Strategy of Ukraine are analyzed, one of the priorities of which is to improve the regulatory framework for cyber security of critical information infrastructure. The shortcomings of the previous Cyber Security Strategy of Ukraine (2016) are noted. Contains a detailed analysis of legislation and initiatives on providing cybersecurity. General requirements for cyber protection of critical infrastructure objects are considered. Based on the analysis of the current legislation on cyber security of Ukraine, ways to improve the legal and organizational support for the protection of the critical information infrastructure from cyber attacks are proposed.*

Keywords: *cyberspace, cyber attack, critical infrastructure objects, cyber protection of critical infrastructure objects, legal support, organizational support.*

Аннотация. *В статье рассматриваются правовые и организационные аспекты обеспечения защиты объектов критической информационной инфраструктуры от кибератак. Обращается внимание на положительный опыт США в обеспечении устойчивости объектов критической инфраструктуры. Анализируются положения новой Стратегии кибербезопасности Украины, одним из приоритетов которой определены совершенствование нормативного обеспечения по вопросам киберзащиты объектов критической информационной инфраструктуры. Отмечаются недостатки предыдущей Стратегии кибербезопасности Украины 2016 года. Содержится детальный анализ законодательных актов и инициатив по вопросам обеспечения кибербезопасности. Рассматриваются общие требования киберзащиты объектов критической инфраструктуры. На основании анализа действующего законодательства по вопросам обеспечения кибербезопасности Украины предложены пути совершенствования правового и организационного обеспечения защиты объектов критической информационной инфраструктуры от кибератак.*

Ключевые слова: *киберпространство, кибератака, объекты критической инфраструктуры, киберзащита объектов критической инфраструктуры, правовое обеспечение, организационное обеспечение.*

Постановка проблеми. 26 серпня 2021 року Указом Президента України №447 затверджено нову Стратегію кібербезпеки України [1] (далі – Стратегія), одним з пріоритетів якої визначено удосконалення нормативного забезпечення з питань кіберзахисту об'єктів критичної інформаційної інфраструктури, порядку її визначення та вимог до її кіберзахисту. Стратегія констатує, що зростає технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти і механізми кібератак. Набуває значимості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди [1].

Як і раніше, гібридна агресія Російської Федерації проти України у кіберпросторі залишається однією із серйозних загроз кібербезпеці України. Кібератаки Російської Федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Не меншу загрозу складають організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство). Особливостями таких кібератак є їх тривалість, складність та прихований характер, що ускладнює їх запобігання, виявлення та нейтралізацію [1].

Лише протягом першого півріччя 2020 року Служба безпеки України нейтралізувала понад 300 кібератак і кіберінцидентів на об'єкти критичної інфраструктури. До цих кібератак були причетні майже 20 хакерських угруповань, які також викрито і знешкоджено спецслужбою. Значну частину хакерів напряму контролювали з Російської Федерації. Їх метою було завдання шкоди українським державним органам і підприємствам оборонно-промислового комплексу. Була за цей період і спроба кібератаки на українські ЗМІ [2].

Підвищення ризиків терористичних актів, збільшення кількості кібератак на енергетичні об'єкти, руйнування та пошкодження об'єктів інфраструктури в зоні військового конфлікту на сході України обумовлюють нагальність питання розбудови державної системи захисту критичної інфраструктури в Україні [3, с. 2]. У Стратегії відзначається, що надзвичайно важливі для розвитку національної системи кібербезпеки завдання Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.16 р. № 96, не були виконані, зокрема: не сформовано перелік об'єктів критичної інформаційної інфраструктури, не створено модель державно-приватного партнерства.

Поширення кіберзагроз на усі сфери життєдіяльності та вдосконалення інструментарію їх реалізації зумовлює необхідність зміни стратегії і тактики протидії ним [1]. Ці обставини підкреслюють актуальність досліджуваної проблематики захисту критичної інформаційної інфраструктури від кібератак.

Результати аналізу наукових публікацій. Питання захищеності об'єктів критичної інфраструктури досліджували Іванюта С.П. [3], Кондратов С.І. [4], Леонов Б.Д. [5], Серьогін В.С. [5], Суходоля О.М. [4], Рижов І.М. [6]. Питанню визначення кібербезпеки стосувалася робота Баранова О.А. [7], реалізації Стратегії кібербезпеки України розглядали такі науковці, як Гнатюк С.О. [8], Лук'янчук Р.В. [9], Ткачук Н.А. [10] та ін. Водночас, затвердження нової Стратегії висуває новий порядок

денний з правового та організаційного забезпечення захисту об'єктів критичної інфраструктури від кібератак.

Метою статті є удосконалення на підставі аналізу чинного законодавства нормативного та організаційного забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак.

Виклад основного матеріалу. Серед усіх загроз різного походження для безпеки критичної інфраструктури найбільш актуальними можна виокремити такі: природні; а) незловмисні: промислові аварії, ядерні/радіологічні аварії, аварії на транспорті, втрата критично важливої інфраструктури; б) зловмисні: кібератаки, терористичні атаки [4].

Не випадково сьогодні набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами [1]. Так, 14 травня 2021 року РНБО України прийнято рішення РНБО України "Про невідкладні заходи з кібероборони держави" (введено в дію Указом Президента України від 26.08.21 р. № 447), яким передбачено створення у системі Міністерства оборони України кібервійськ та набуття ними відповідних спроможностей для захисту суверенітету держави, забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії у кіберпросторі. Цим рішенням також передбачено розробку та внесення на розгляд Верховної Ради України законопроекту щодо створення та функціонування у системі Міністерства оборони України кібервійськ [11].

Відповідно до Стратегії національної безпеки України [12] одним із основних напрямів державної політики в сфері національної безпеки визначено забезпечення безпеки та необхідного рівня захищеності об'єктів критичної інфраструктури України, насамперед від загроз терористичного та диверсійного характеру. Об'єктами критичної інформаційної інфраструктури є комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури (п. 19 ст. 1 Закону України "Про основні засади забезпечення кібербезпеки України") [13].

Концепція боротьби з тероризмом [14] проголошує, що усунення та мінімізація наслідків терористичної діяльності передбачає вирішення завдань опрацювання комплексу заходів щодо забезпечення якнайшвидшого відновлення штатного режиму функціонування об'єктів, передусім об'єктів критичної інфраструктури, щодо яких вчинено терористичний акт.

Сьогодні не викликає здивування, що кіберпростір є одним з можливих театрів воєнних дій разом з іншими фізичними просторами.

На думку зарубіжних дослідників, критична інфраструктура являє собою складну систему, яка характеризується атрибутами, серед яких виділяється: 1) необмежена кількість варійованих об'єктів та параметрів системи; 2) важко прогнозована поведінка об'єктів, для яких характерна велика кількість взаємозв'язків, які класифіковано по різних секторах [15]. Наприклад, в США, яка є піонером у розробці та запровадженні концепції критичної інфраструктури, функціонує збалансована система забезпечення захисту критичної інфраструктури держави, зміст якої охоплює: визначений уповноважений орган для організації, координації та здійснення контрольно-наглядових функцій щодо заходів безпекового напряму; методичний апарат для аналізу та прогнозування наслідків як подій техногенного характеру, так і диверсій чи терористичних актів; систему науково-дослідних установ, які забезпечують науково-

технічне супроводження функціонування системи аналізу стану критичної інфраструктури та експертизу з оцінки прогнозування наслідків впливів на стійкість об'єктів критичної інфраструктури [5, с. 93].

США продовжують зберігати свої лідерські позиції у цій сфері, у т.ч. завдяки застосуванню апробованих на інших напрямах сучасних управлінських підходів, удосконаленню інформаційно-аналітичної підтримки процесу прийняття рішень, використанню новітніх технологій та активному поширенню різноманітних форм і форматів підготовки кадрів і населення задля забезпечення захисту та стійкості критичної інфраструктури тощо. Інші розвинені країни світу широко використовують напрацьовані у США підходи, звичайно, враховуючи при цьому власну національну специфіку [4, с. 4, 5].

В Україні, де ще за радянських часів існувала збалансована система управління техногенною безпекою об'єктів підвищеної небезпеки, проблематика забезпечення захисту критичної інформаційної інфраструктури від кібератак давно є предметом активних дискусій. На державному рівні активні заходи щодо розв'язання цієї проблематики почали вживатися з 2016 року.

У червні 2016 року утворено Національний координаційний центр кібербезпеки, положення про який затверджено Указом Президента України від 07.06.16 р. № 242. До основних завдань цього Центру, зокрема, віднесено: здійснення координації та контролю за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку; здійснення аналізу: стану кібербезпеки та стану кіберзахисту критично важливих об'єктів інфраструктури; здійснення заходів щодо забезпечення кіберзахисту об'єктів критичної інфраструктури та захисту технологічних процесів на виробництві у реальному секторі економіки [16] тощо.

Затвердження у 2016 році Стратегії кібербезпеки України стало важливим кроком у запровадженні підходів довгострокового планування в цій сфері. За роки реалізації попередньої Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.16 р № 96, було докладено зусиль до становлення та розвитку національної системи кібербезпеки. Важливим етапом її інституалізації стало прийняття Закону України "Про основні засади забезпечення кібербезпеки України" [13], 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].

Утворено центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України [1].

Рішенням РНБО від 29.12.16 р. "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури" (введено в дію Указом Президента України від 16.01.17 р. № 8) заплановано внесення в установленому порядку на розгляд Верховної Ради України проект Закону України "Про критичну інфраструктуру та її захист", в якому слід передбачити врегулювання питань, зокрема, щодо: створення державної системи захисту критичної інфраструктури; визначення органу, відповідального за координацію діяльності із захисту критичної інфраструктури в мирний час та в умовах особливого періоду; визначення функцій, повноважень та відповідальності центральних

органів виконавчої влади та інших органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників і операторів об'єктів критичної інфраструктури; запровадження єдиної методології проведення оцінки загроз критичній інфраструктурі та реагування на них, зокрема щодо аварій і технічних збоїв, небезпечних природних явищ, зловмисних дій; запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації [17].

Розпорядженням Кабінету Міністрів України від 06.12.17 р. затверджено Концепцію створення державної системи захисту критичної інфраструктури, де серед проблем, що потребують розв'язання, визначено відсутність єдиних критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації. Аналогічна проблема фіксується й у Концепції боротьби з тероризмом, одним із завдань якої є підвищення ефективності систем і режимів охорони найбільш уразливих об'єктів можливих терористичних посягань, у тому числі шляхом розроблення та впровадження уніфікованих стандартів, правил, технічних умов і вимог, обов'язкового оформлення паспортів антитерористичної захищеності таких об'єктів [18].

У 2019 р. Кабінет Міністрів України на виконання вимог Закону "Про основні засади забезпечення кібербезпеки України" затвердив загальні вимоги до кіберзахисту об'єктів критичної інфраструктури [19]. Цим актом, зокрема, установлено, що кіберзахист об'єкта критичної інфраструктури є складовою частиною робіт із створення (модернізації) та експлуатації об'єкта критичної інформаційної інфраструктури відповідного об'єкта. Заходи з кіберзахисту передбачатимуться та впроваджуватимуться на всіх стадіях життєвого циклу об'єкта критичної інформаційної інфраструктури відповідного об'єкта, а створення системи інформаційної безпеки об'єкта критичної інформаційної інфраструктури відповідного об'єкта здійснюватиметься відповідно до вимог технічного завдання на створення системи інформаційної безпеки. Таке завдання формуватиметься за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об'єкті критичної інформаційної інфраструктури. За такого підходу власник та/або керівник об'єкта критичної інфраструктури організовуватиме проведення незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури згідно з вимогами законодавства у сфері захисту інформації та кібербезпеки. Він невідкладно інформуватиме урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності – галузеву команду реагування на комп'ютерні надзвичайні події), а також функціональний підрозділ контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідний підрозділ регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єкта критичної інформаційної інфраструктури [20].

У додатку до загальних вимог наведено перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури, до змісту яких включено формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки, управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури, ідентифікацію та автентифікацію користувачів та адміністраторів відповідного об'єкта критичної інформаційної інфраструктури тощо. Зазначені вимоги є усталеною практикою в ЄС та в США і гармонізовані з вимогами міжнародних стандартів ЄС, НАТО та NIST з питань забезпечення кіберзахисту [20].

Нова Стратегія кібербезпеки України враховує попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО [1].

Ціль С.2 Стратегії визначається як ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму. Проголошується, що для досягнення цілі С.2 Україна забезпечить ефективну протидію розвідувально-підривній діяльності у кіберпросторі та кібертероризму шляхом: створення відповідно до схвалених концептуальних засад загальнодержавної системи виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури. Цьому сприятиме реалізація інших цілей Стратегії, зокрема: завершення процесів визначення об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури; створення і забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури; постійний перегляд та оновлення вимог щодо їх кіберзахисту з урахуванням сучасних міжнародних стандартів з питань кібербезпеки; запровадження на постійній основі оцінки стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість; встановлення обов'язковості та періодичності проведення такої оцінки з урахуванням категорій критичності об'єктів; стимулювання участі у цих заходах фахівців з кібербезпеки приватного сектору [1].

Впровадження заходів кіберзахисту дасть змогу підприємствам, установам та організаціям, які віднесені до об'єктів критичної інфраструктури, забезпечити захист від кібератак, запобігти порушенню конфіденційності, цілісності та доступності своїх інформаційних ресурсів, порушенню режиму сталого функціонування об'єкта критичної інфраструктури [20].

Проблеми забезпечення об'єктів критичної інфраструктури все частіше стають предметом обговорення за участі зарубіжних експертів. Так, 27 травня 2021 року у рамках співпраці між Національним координаційним центром кібербезпеки при Раді національної безпеки і оборони України (НКЦК) і Фондом цивільних досліджень та розвитку Сполучених Штатів Америки (CRDF Global) (за підтримки Державного департаменту США), відбулося четверте засідання Національного кластера з кібербезпеки, присвячене питанням захисту критичної інфраструктури, її стійкості, а також проблемам, які існують у цій сфері. Майже 200 українських та американських фахівців з кібербезпеки відпрацювали захист об'єктів критичної інфраструктури та обговорили аспекти відповідного законопроєкту [21].

Заступник секретаря РНБО України С. Демедюк наголосив, що цей проєкт є платформою, на якій провідні фахівці "можуть безпосередньо обмінятися думками, пропозиціями, цікавими ідеями". Зокрема, захист об'єктів критичної інфраструктури є вкрай важливим для забезпечення життєдіяльності держави та кожного громадянина, а під час засідання кластера можна напрацювати шляхи безперервного забезпечення "безпеки цих об'єктів – починаючи від атомної енергетики і закінчуючи маленькими фінансовими компаніями, які можуть бути віднесені до об'єктів критичної інфраструктури"[21].

Висновки.

На базі аналізу законодавства з питань забезпечення кібербезпеки можна дійти висновку, що забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак потребує удосконалення за напрямами:

1) законодавчого забезпечення – прийняття Закону України “Про об’єкти критичної інфраструктури”;

2) організаційно-адміністративного забезпечення – ідентифікації об’єктів критичної інфраструктури; розробки правил антитерористичної безпеки для об’єктів критичної інфраструктури; регламентації повноважень державних органів із захисту об’єктів критичної інфраструктури від кібератак.

Використана література

1. 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. URL: https://www.president.gov.ua/documents/4472021-40013

2. За півроку СБУ нейтралізувала 300 кібератак на об’єкти критичної інфраструктури URL: https://ssu.gov.ua/novyny/za-pivroku-sbu-neitralizuvala-300-kiberatak-na-obiekty-krytychnoi-infrastruktury

3. Іванюта С.П. Пріоритетні напрями законодавчого та організаційного забезпечення паспортизації об’єктів критичної інфраструктури. URL: https://niss.gov.ua/sites/default/files/2018-07/1_Ivaniuta-9af75.pdf

4. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О.М. Суходолі. Київ: НІСД, 2020. 28 с.

5. Леонов Б.Д., Шостак Р.М., Серьогін В.С. Розвиток методичного забезпечення антитерористичної захищеності об’єктів критичної інфраструктури (на прикладі США). *Інформація і право.* № 3(34)/2020. С. 88-95.

6. Рижов І.М. Базові концепти антитерористичної безпеки: монографія. Київ: Нац. акад. СБУ, 2016. 327 с.

7. Баранов О.А. Про тлумачення та визначення поняття “кібербезпека”. *Правова інформатика*. 2014. № 2 (42). С. 54-62.

8. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19. № 2. С. 118-129.

9. Лук’янчук Р.В. Державне стратегічне планування у сфері забезпечення кібербезпеки: реалії сьогодення. *Вісник Національної академії державного управління при Президентові України*. *Сер.: Державне управління*. 2016. № 3. С. 131-137.

10. Ткачук Н. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134.

11. Про невідкладні заходи з кібероборони держави: рішення РНБО України від 04.05.21 р.: Указ Президента України від 26.08.21 р. № 447). URL: https://zakon.rada.gov.ua/laws/show/n0053525-21#Text

12. Про Стратегію національної безпеки України: рішення РНБО України від 06.05.15 р.: Указ Президента України від 26.05.15 р. № 287. *Офіційний вісник України*. 2015. № 43. Ст. 1353.

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

14. Концепція боротьби з тероризмом: Указ Президента України від 05.03.19 р. № 53. URL: https://zakon.rada.gov.ua/laws/show/53/2019#Text

15. Congressional Research Service Report for Congress. Critical Infrastructures. Background, Policy and Implementation. 2002. URL: https://sgp.fas.org/crs/homesec/RL30153.pdf

16. Положення про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.16 р. № 242. URL:https://zakon.rada.gov.ua/laws/show/242/2016#Text

17. Про удосконалення заходів забезпечення захисту об’єктів критичної інфраструктури: рішення РНБО від 29.12.16 р.: Указ Президента України від 16.01.17 р. № 8. URL: https://zakon.rada.gov.ua/laws/show/n0014525-16#Text

18. Концепція створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 06.12.17 р. № 1009 URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

19. 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#Text

20. Визначено вимоги до кіберзахисту об'єктів критичної інфраструктури. URL: https://jurliga.ligazakon.net/ua/news/170010_zakon-pro-kberbezpeku-nabuv-chinnost

21. Українські та американські фахівці обговорили стійкість критичної інфраструктури. URL: https://www.ukrinform.ua/rubric-society/3254378-ukrainski-ta-amerikanski-fahivci-obgovorili-stijkist-kriticnoi-infrastrukturi-do-kiberatak.html

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