УДК 351.862.4:340.13+338.583
DOI https://doi.org/10.32782/pdu.2024.1.12

М. В. Сокіран
кандидат юридичних наук, докторант
Науково-дослідного інституту публічного права

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПРИНЦИПІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА СТІЙКОСТІ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

У статті представлено аналіз вітчизняних нормативно-правових актів, міжнародних документів та юридичної літератури у результаті якого сформовано систему принципів забезпечення безпеки та стійкості критичної інформаційної інфраструктури України. З'ясовано, що на сучасному етапі нові загрози та небезпеки генеруються набагато швидше ніж відповідальні актори формують системи захисту критичної інформаційної інфраструктури. Тому дедалі більше уваги необхідно приділяти саме системі стійкості зазначеної інфраструктури поряд із заходами безпеки. Детально проаналізовано Національну систему стійкості, в якій вперше на національному рівні визначено мету, основні принципи, напрями, механізми і строки запровадження та функціонування національної системи стійкості. Акцентується, що у ній міститься визначення термінів «національна стійкість» та «національна система стійкості».

Автором сформована наступна система принципів забезпечення безпеки і стійкості критичної інформаційної інфраструктури: 1) верховенства права і поваги до прав та свобод людини і громадянина; 2) дотримання національних інтересів України; 3) балансу між відкритістю/доступністю та безпекою й стійкістю; 4) державно-приватного партнерства; 5) пропорційності та адекватності заходів захисту реальним та потенційним ризикам; 6) пріоритетності запобіжних заходів; 7) об'єктивності та правової визначеності об'єктів критичної інформаційної інфраструктури; 8) стандартизації процедур та унормування технічних вимог. Зроблено висновок, що систему принципів забезпечення безпеки і стійкості критичної інформаційної інфраструктури необхідно розуміти як сукупність основних керівних засад, приписів, які враховують інтереси людини, суспільства і держави та на підставі яких формується така державна політика щодо адміністративно-правового регулювання, що дозволяє критичній інформаційній інфраструктурі протистояти загрозам та швидко відновлюватися вразі порушення її функціонування.

Ключові слова: *критична інформаційна інфраструктура, забезпечення, безпека, захист, стійкість, принципи, система, національна система стійкості.*

Вступ. Останніми роками у розвинених країнах світу посилюється тенденція щодо розширення контексту заходів, пов'язаних із забезпеченням функціонування критичної інформаційної інфраструктури: питання її безпеки почали розглядатися разом із питаннями її стійкості. При цьому, питанням забезпечення стійкості приділяється дедалі більше уваги у порівнянні з питаннями безпеки [1]. Це пояснюється в першу чергу тим, що в сучасному світі нові загрози та небезпеки генеруються набагато швидше ніж відповідальні актори формують відповідні системи захисту.

За таких умов, жодна створена система безпеки не може у повній мірі забезпечити захист від усіх загроз і небезпек [1]. Тому дедалі більше уваги необхідно приділяти саме системі стійкості критичної інформаційної інфраструктури поряд із заходами безпеки.

У 2021 році в Україні була прийнята Національна система стійкості [2]. Зазначена Концепція вперше на національному рівні визначила мету, основні принципи, напрями, механізми і строки запровадження та функціонування національної системи стійкості. Також вона визначає

© Сокіран М. В., 2024

терміни «національна стійкість» та «національна система стійкості».

Так, під національною стійкістю визначено: «здатність держави і суспільства ефективно протистояти загрозам будь-якого походження і характеру, адаптуватися до змін безпекового середовища, підтримувати стале функціонування, швидко відновлюватися до бажаної рівноваги після кризових ситуацій», а під національною системою стійкості – «комплекс цілеспрямованих дій, методів та механізмів взаємодії органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, інститутів громадянського суспільства, які гарантують збереження безпеки і безперервності функціонування основних сфер життєдіяльності суспільства і держави до, під час і після настання кризової ситуації» [2].

Метою статті є на підставі аналізу чинних нормативно-правових актів, міжнародних документів та юридичної літератури сформувати та схарактеризувати систему принципів забезпечення безпеки та стійкості критичної інформаційної інфраструктури України.

Виклад основного матеріалу. На підставі проведеного аналізу чинного законодавства, а саме: Закону України «Про основні засади забезпечення кібербезпеки України»; Указів Президента України «Про запровадження національної системи стійкості», «Про Доктрину інформаційної безпеки України», «Про Стратегію кібербезпеки України»; розпорядження Кабінету Міністрів України «Про схвалення концепції створення державної системи захисту критичної інфраструктури», нами виокремленні наступні принципи забезпечення безпеки та стійкості критичної інформаційної інфраструктури України: 1) верховенства права і поваги до прав та свобод людини і громадянина; 2) дотримання національних інтересів України; 3) балансу між відкритістю/доступністю та безпекою й стійкістю; 4) державно-приватного партнерства; 5) пропорційності та адекватності заходів захисту реальним та потенційним ризикам; 6) пріоритетності запобіжних заходів; 7) об'єктивності та правової визначеності об'єктів критичної інформаційної інфраструктури; 8) стандартизації процедур та унормування технічних вимог.

Коротко схарактеризувавши ці принципи, маємо наступне.

Принцип верховенства права і поваги до прав та свобод людини та громадянина відноситься до основних загальних принципів. У контексті забезпечення стійкості критичної інформаційної інфраструктури принцип верховенства права і поваги до прав та свобод людини і громадянина передбачає таке:

– по-перше, існує необхідність змінити домінуючу думку про те, що права людини є перешкодою для безпеки. Мабуть, найбільш широко цитованим прикладом щодо прав людини, які перешкоджають безпеці, є твердження, що шифрування, яке є критично важливим для здійснення права на приватне життя, перешкоджає правоохоронним органам у проведенні своєї роботи. Тому уряди деяких країн висловлюють аргументи щодо послаблення шифрування, щоб забезпечити доступ до зашифрованого зв'язку для правоохоронних органів. Однак експерти сходяться на думці, що неможливо забезпечити доступ до зашифрованих комунікацій для одних суб'єктів, не роблячи цього для інших (у тому числі зловмисників [3]. Іншими словами, послаблення кібербезпеки для цілей правоохоронних органів неможливо зробити, не послабивши безпеки для всіх і не поставивши під загрозу права людини. Це пов'язано з тим, що кібербезпека невідступно пов'язана з безпекою людини, яка є основним правом людини. Кібербезпека та права людини є взаємодоповнюючими та взаємозалежними. Для того, щоб ефективно забезпечувати свободу та безпеку, потрібно прагнути до захисту першої та стійкості другої;

– по-друге, критично важливо застосовувати підходи, засновані на правах людини, до законів, політики та практики кібербезпеки. Кібернебезпека ніколи не повинна бути приводом для порушення прав людини. Натомість визнання того, що індивідуальна та колективна безпека є основою кібербезпеки, означає, що захист прав людини повинен бути в центрі розробки політики кібербезпеки. Наприклад, Робоча група Коаліції свободи в Інтер-

неті «Безкоштовний та безпечний Інтернет» (Freedom Online Coalition «Internet Free and Secure») [4] розробила набір рекомендацій щодо кібербезпеки та прав людини, спрямованих на забезпечення того, щоб політика та практика кібербезпеки базувались і повністю відповідали правам людини.

Отже, принцип верховенства права і поваги до прав та свобод людини і громадянина полягає у забезпеченні балансу захисту особистості від свавільного втручання державних органів та станом безпеки й стійкості критичної інформаційної інфраструктури через створення певних обмежень, визначених у законі.

Принцип дотримання національних інтересів України щодо забезпечення безпеки та стійкості критичної інформаційної інфраструктури. Необхідно відмітити, що вказаний принцип неповинен суперечити вище зазначеному принципу, адже ще раз акцентуємо, що дотримання принципу верховенства права і поваги до прав та свобод людини і громадянина є одним із основних фундаментальних прав. Однак, це не означає, що від цього повинні «страждати» національні інтереси у сфері забезпечення безпеки і стійкості критичної інформаційної інфраструктури.

Уточнимо, що національні інтереси – інтегральний вираз інтересів усіх членів суспільства, що реалізуються через політичну систему відповідної держави як компроміс у поєднанні запитів кожної людини й суспільства загалом [5]. Крім того, поєднання інтересів при побудові національних інтересів, повинно не тільки бути дороговказом, а й згуртовувати націю навколо певних центральних ідей. Для України пошук нової системи ідеалів і орієнтирів є сьогодні складним, але важливим завданням, адже без цього етапу пізнавального й світоглядного пошуку неможливо розробити програми економічних, політичних й інших реформ і подолати системну кризу [6]. І, як вірно зазначив український правозахисник і співзасновник Української Гельсінської групи М. Маринович, – «ми погано вміємо в мирний час об'єднуватися для того, щоб втілювати в життя добрі справи» [7; 8]. Тому ми погоджуємося із Л. Сорокою, яка визначаючи національні космічні інтереси вказала, що це «основоположні інтереси особи, громадянського суспільства та держави, забезпечення яких є підґрунтям для сталого розвитку України, добробуту її громадян, а також безпеки життєдіяльності…» [9]. Отже, при формуванні будь-яких заходів, направлених на дотримання національних інтересів, на першому місці повинні стояти інтереси особи, а вже потім – суспільства і держави.

Про пріоритетність інтересів особи при формуванні національних інтересів йде мова в Указі Президента України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Зокрема визначається, що національними інтересами України в інформаційній сфері першочергово є: «життєво важливі інтереси особи: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів…» [10]. Необхідно відмітити, що в деяких нормативно-правових актах національні інтереси формуються з огляду на пріоритетність саме державних інтересів, як наприклад, у Законі України «Про національну безпеку України» [11].

Отже, під принципом дотримання національних інтересів України щодо забезпечення безпеки та стійкості критичної інформаційної інфраструктури ми розуміємо створення умов для безпечного та стійкого функціонування критичної інформаційної інфраструктури задля використання їх для захисту життєво важливих інтересів особи, суспільства та держави в інформаційній сфері, зокрема враховуючи поточні виклики, що походять від зовнішніх і внутрішніх загроз.

Принцип забезпечення балансу між відкритістю/доступністю та безпекою й стійкістю критичної інформаційної інфраструктури. Для більшості національних урядів серед пріоритетних завдань у сфері національної безпеки залишається забезпечення сталого функціонування критично важливих для повсякденного життя країн об'єктів (зокрема й критичної інформаційної інфраструктури), завдяки чому насе-

лення, суспільні та державні інститути мають можливість доступу до життєво важливих ресурсів та послуг [1]. У зазначеному контексті відкритість означає: відкритий доступ до інформації; стандартизація відкритих даних для забезпечення сумісності та обміну даними між різними системами, а також розвиток механізмів співпраці з іншими суб'єктами для спільного вирішення проблем та обміну досвідом. Доступність критичної інформаційної інфраструктури означає забезпечення доступності до сервісів та функцій зазначеної інфраструктури в умовах збоїв або атак; використання резервних систем та механізмів, які можуть призначатися для автоматичного відновлення роботи у разі відмови.

Принцип державно-приватного партнерства у забезпеченні безпеки та стійкості критичної інформаційної інфраструктури. Цей принцип базується на співпраці між державними органами та приватними компаніями для ефективного управління ризиками та забезпечення надійності критичної інформаційної інфраструктури. Наприклад, у США та Німеччині необхідною умовою для розбудови державно-приватного партнерства визначається формування довіри [12] між партнерами та стимулів для співпраці. Політика країн має стимулювати приватних власників й органи державного управління до створення на всіх рівнях такої системи захисту критичної інформаційної інфраструктури, яка була б спроможною переборювати надзвичайні ситуації, знижувати ризики й наслідки виникнення таких ситуацій [13].

Основні аспекти принципу державно-приватного партнерства у забезпеченні безпеки та стійкості критичної інформаційної інфраструктури включають: 1) обмін інформацією, тобто забезпечення двостороннього обміну, шляхом встановлення механізмів для обміну інформацією між державними структурами та приватним сектором стосовно поточних загроз і вразливостей; 2) конфіденційність, забезпечення захисту конфіденційної інформації, обмін якою може сприяти вирішенню проблем безпеки; 3) спільне планування, що полягає у спільному визначенні стратегій та політик безпеки та стійкості критичної інформаційної інфраструктури з урахуванням інтересів обох сторін; 5) спільне реагування, тобто створення механізмів спільного кризового управління для ефективної реакції на кібератаки та інші інциденти; 6) спільне тестування та тренування критичної інформаційної інфраструктури шляхом проведення спільних заходів для підвищення реагування на екстрені ситуації; 7) розробка законодавства, яке регулює взаємодію між державними та приватними структурами у сфері кібербезпеки та забезпечення безпеки і стійкості критичної інформаційної інфраструктури; 8) розвиток ефективних механізмів комунікації між усіма сторонами для оперативного обміну інформацією та координації дій.

Отже, цей принцип допомагає створити стан, при якому враховується різноманіття інтересів та компетенцій різних суб'єктів, забезпечуючи таким чином ефективність у сфері кібербезпеки та стійкості критичної інформаційної інфраструктури.

Принцип пропорційності та адекватності заходів захисту реальним та потенційним ризикам у системі забезпечення безпеки та стійкості критичної інформаційної інфраструктури. Цей принцип означає, що впроваджені заходи безпеки та стійкості повинні бути відповідні реальним і потенційним ризикам, з якими ця інфраструктура може зіткнутися. Також цей принцип визначає необхідність узгодженості та розуміння між рівнем захисту та рівнем загрози. Декілька ключових аспектів цього принципу передбачають наступне. По-перше, його дотримання вимагає постійного аналізу потенційних загроз, які можуть впливати на критичну інформаційну інфраструктуру Також необхідно визначати можливі наслідки і збитки, які можуть виникнути внаслідок різних типів атак чи інцидентів. Тільки після цього актуальною є розробка та впровадження заходів, які будуть протидіяти конкретним загрозам, із вираховуванням їх можливого впливу.

По-друге, вказаний принцип вимагає збалансованого підходу, тобто забезпечення балансу між ефективністю та вартістю заходів, щоб вони були адекватними реальним ризикам під час забезпечення

безпеки і стійкості критичної інформаційної інфраструктури. Отже, цей принцип дозволяє оптимально використовувати обмежені ресурси та забезпечити ефективний та адекватний рівень безпеки і стійкості для критичної інформаційної інфраструктури.

Принцип забезпечення пріоритетності запобіжних заходів щодо безпеки та стійкості критичної інформаційної інфраструктури. Цей принцип передбачає акцент на уникненні можливих загроз та мінімізації ризиків заздалегідь, перед тим, як вони можуть спричинити негативні наслідки для критичної інформаційної інфраструктури. Його дотримання можливе шляхом проведення превентивних заходів, зокрема таких як: систематичний аналіз потенційних загроз та визначення слабких місць у критичній інформаційній інфраструктурі; використання інструментів та методів для прогнозування можливих атак або інцидентів; застосування сучасних технологій та методів для зміцнення безпеки і підвищення стійкості систем; проведення навчань та тренувань з персоналом для ефективної реакції на можливі загрози; встановлення систем реагування на інциденти для оперативного виявлення та припинення атак; підвищення рівня інформаційної грамотності серед персоналу та користувачів критичної інформаційної інфраструктури про потенційні загрози та відповідальність у сфері безпеки і стійкості критичної інформаційної інфраструктури.

Принцип забезпечення об'єктивності та правової визначеності об'єктів критичної інформаційної інфраструктури. Проблема правової визначеності об'єктів критичної інфраструктури в Україні стоїть дуже гостро. Адже, на законодавчому рівні це питання врегульовується лише останні п'ять років. Так, 1) ідентифікація та категоризація об'єктів критичної інформаційної інфраструктури; 2) формування переліку об'єктів критичної інформаційної інфраструктури; 3) формування та функціонування реєстру об'єктів критичної інформаційної інфраструктури [14] – повинні здійснюватись на підставі розроблених та прийнятих порядків. Станом на кінець 2023 року в Україні прийнятий Порядок ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього [15]. Отже, цей принцип допомагає уникнути суб'єктивності та невизначеності в оцінці та захисті об'єктів критичної інформаційної інфраструктури. Він також сприяє ефективній координації державних та приватних структур у сфері кібербезпеки та робить можливим вчасну реакцію на зміну умов та нові загрози для критичної інформаційної інфраструктури.

Принцип стандартизації процедур та уніфікації технічних вимог щодо забезпечення безпеки та стійкості критичної інформаційної інфраструктури. Розробка та впровадження уніфікованих методологій та стандартів щодо оцінки ризиків, планування безпеки, моніторингу та реагування на інциденти – допоможе забезпечити системний та послідовний підхід до забезпечення безпеки та стійкості критичної інформаційної інфраструктури. А встановлення спільних технічних стандартів та вимог для обладнання, програмного забезпечення та комунікаційних технологій, що використовуються в критичній інформаційній інфраструктурі, – сприятиме розробці узгоджених критеріїв безпеки, які визначатимуть мінімальні стандарти та вимоги для системи захисту критичної інформаційної інфраструктури від різноманітних загроз. Таким чином, цей принцип сприяє підвищенню ефективності та взаємодії між різними частинами критичної інформаційної інфраструктури, спрощує процес впровадження та управління заходами безпеки, а також полегшує взаємодію між різними структурами, які відповідають за безпеку та стійкість цих об'єктів.

Отже, під системою принципів забезпечення безпеки і стійкості критичної інформаційної інфраструктури ми розуміємо сукупність основних керівних засад, приписів, які враховують інтереси людини, суспільства і держави, на підставі яких формується така державна політика щодо адміністративно-правового регулювання, що дозволяє критичній інформаційній інфраструктурі протистояти загрозам та швидко відновлюватися вразі порушення її функціонування [16].

Висновки і пропозиції. Останні роки свідчать про тенденцію до розширення переліку заходів, спрямованих на забезпечення функціонування критичної інформаційної інфраструктури України. Своєю чергою, забезпечення безпеки критичної інформаційної інфраструктури почали розглядається разом із питаннями стійкості, враховуючи швидку еволюцію загроз та потребу в адаптації до змін. Адже, жодна система безпеки не може бути повністю захищеною від усіх загроз, що вимагає підвищеної уваги до її системи стійкості.

Як підсумок проведеного аналізу, запропоновано таку систему принципів забезпечення безпеки та стійкості критичної інформаційної інфраструктури: 1) верховенства права і поваги до прав та свобод людини і громадянина; 2) дотримання національних інтересів України; 3) балансу між відкритістю/доступністю та безпекою й стійкістю; 4) державно-приватного партнерства; 5) пропорційності та адекватності заходів захисту реальним та потенційним ризикам; 6) пріоритетності запобіжних заходів; 7) об'єктивності та правової визначеності об'єктів критичної інформаційної інфраструктури; 8) стандартизації процедур та унормування технічних вимог.

Список використаної літератури:

1. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналітична доповідь. За ред. О. М. Суходолі. Київ: НІСД, 2020. 28 с.
2. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості»: Указ Президента України від 27 вересня 2021 року № 479/2021. Верховна Рада України офіційний сайт. URL: https://www.president.gov.ua/documents/4792021-40181
3. Deborah Brown and Anriette Esterhuysen. Why cybersecurity is a human rights issue, and it is time to start treating it like one. APCNews, 2019. URL: https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one#:~:text=Cybersecurity%20and%20human%20rights%20are,cybersecurity%20laws%2C-%20policies%20and%20practices.
4. FOC Documents. Freedom Online Coalition, 2023. URL: https://freedomonlinecoalition.com/about-us/foc-documents/
5. Бабкіна О. В., Горбатенко В. П. Політологія. Навчальний посібник. К.: ВЦ, 2006. 568 с.
6. Дашутін Г. П., Михальченко М. І. Український експеримент на терезах гуманізму. К.: Парлам. вид-во, 2001. 335 с.
7. Ціннісні орієнтири – основа життєвого вибору та успішної самореалізації особистості, 2019. URL: https://citizen.in.ua/photos/topic/f/20190128_132011_rozdil-1-4.pdf
8. The Ukrainians: Розмова із Мирославом Мариновичем. 2014. URL: https://ucu.edu.ua/news/the-ukrainians-rozmova-iz-myroslavom-marynovychem/
9. Сорока Л. В. Адміністративно-правовий механізм реалізації космічної доктрини України: теорія і практика. Київ: ФОП Чалчинська Н. В., 2020. 395 с.
10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 47/2017. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text
11. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
12. Partnering for Critical Infrastructure Security and Resilience / U.S. Department of Homeland Security, National Infrastructure Protection Plan, NIPP 2013. URL: www.dhs.gov/nationalinfrastructure-protection-plan
13. Маркєєва О. Д., Розвадовський Б. Л. Актуальні проблеми правового забезпеченнядержавно-приватного партнерства у сфері захисту критичної інфраструктури. Національний інститут стратегічних досліджень, 2019. URL: https://niss.gov.ua/sites/default/files/2020-09/derzhavno-pryvatne-partnerstvo.pdf
14. Циплинський Ю. Порядок віднесення об'єктів до об'єктів критичної інфраструктури. Вимоги до кіберзахисту об'єктів критичної інфраструктури. Державна служба спеціального зв'язку та захисту інформації України, 2019. URL: https://niss.gov.ua/sites/default/files/2019-10/fayl5-prezentaciya-ciplinskogo-peretvoreno.pdf
15. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього:

постанова Кабінету Міністрів України від 28 квітня 2023 р. № 415. URL: Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text

16. Сокіран М. В. Система принципів адміністративно-правового забезпечення стійкості критичної інформаційної інфраструктури України. Наукові записки. Серія: право. 2020. Вип. 8. Спецвипуск. С. 73–77.

Sokiran M. GENERAL CHARACTERISTICS OF THE PRINCIPLES OF ENSURING SECURITY AND SUSTAINABILITY OF CRITICAL INFORMATION INFRASTRUCTURE IN UKRAINE

The article analyzes domestic legal acts, international documents and legal literature, on the basis of which a system of principles for ensuring the safety and stability of Ukraine's critical infrastructure was formed. It has been found that at the current stage, new threats and dangers are generated much faster than the responsible actors will form systems for the protection of critical information infrastructure, so more and more attention should be paid to the system of stability of the specified infrastructure along with security measures. The National Sustainability System was analyzed in detail, in which the purpose, main principles, directions, mechanisms and terms of the introduction and functioning of the National Sustainability System were defined for the first time at the national level. It also defines what «national resilience» and «national resilience system» are.

The author has formed the following system of principles for ensuring the security and stability of critical information infrastructure, they are: 1) the rule of law and respect for the rights and freedoms of a person and a citizen; 2) compliance with the national interests of Ukraine; 3) the balance between openness/accessibility and security and stability; 4) public-private partnership; 5) proportionality and adequacy of protection measures to real and potential risks; 6) priority of preventive measures; 7) objectivity and legal certainty of KII objects; 8) standardization of procedures and standardization of technical requirements. It was concluded that the system of principles for ensuring the safety and stability of critical information infrastructure must be understood as a set of basic guidelines, prescriptions that take into account the interests of man, society and the state, on the basis of which such a state policy regarding administrative and legal regulation is formed that allows critical information infrastructure to withstand threats and quickly recover in the event of a disruption in its functioning.

Key words: *critical information infrastructure, provision, security, protection, resilience, principles, system, national resilience system.*