Загрози критичній інфраструктурі та їх вплив на стан національної безпеки
(моніторинг реалізації Стратегії національної безпеки)
(аналітична записка)

Анотація

Визначено тенденції і характер змін загроз критичній інфраструктурі в контексті моніторингу реалізації Стратегії національної безпеки України. Проаналізовано вплив актуальних загроз критичній інфраструктурі на стан національної безпеки держави. Запропоновано пріоритетні напрями діяльності Кабінету Міністрів України, Міністерству внутрішніх справ України, Міністерству енергетики та вугільної промисловості України, Міністерству інфраструктури України, Державній службі України з надзвичайних ситуацій щодо відпрацювання заходів із зниження та відвертання актуальних загроз критичній інфраструктурі.

Загрози критичній інфраструктурі та їх вплив на стан національної безпеки
(моніторинг реалізації Стратегії національної безпеки)
(аналітична записка)

Резюме

Визначено тенденції і характер змін загроз критичній інфраструктурі в контексті моніторингу реалізації Стратегії національної безпеки України.

Акцентовано увагу на необхідності створення дієвої системи захисту критичної інфраструктури в Україні, що має вирішуватись в рамках загального реформування сектору безпеки і оборони із врахуванням всього існуючого спектра загроз та забезпечення взаємопов'язаності різних систем.

Наголошено на необхідності вирішення комплексу проблемних питань, пов'язаних із захистом критичної інфраструктури, що включають визначення критеріїв та процедур віднесення об'єктів до критичної інфраструктури, розвиток державно-приватного партнерства в сфері безпеки, створення мережі ситуаційних центрів, формування нормативно встановленого порядку проведення комплексної оцінки загроз критичній інфраструктурі, загальної методології оцінки ризиків, пов'язаних із функціонуванням критичної інфраструктури.

Враховуючи наведені оцінки динамічного розвитку чинників формування загроз безпеці критичній інфраструктурі, запропоновано пріоритетні напрями діяльності Кабінету Міністрів України, Міністерству внутрішніх справ України, Міністерству енергетики та вугільної промисловості України, Міністерству інфраструктури України, Державній службі України з надзвичайних ситуацій щодо відпрацювання заходів із зниження та відвертання загроз критичній інфраструктурі.

Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки)

Відповідно до Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287/2015, загрозами безпеці критичної інфраструктури (КІ) визначено[1]:

- критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту;
- недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій;
- неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення.

Загрози КІ в разі їх реалізації проявлятимуться у вигляді припинення надання послуг та товарів, що є життєво важливими для населення, економіки, державного управління. Такими є забезпечення населення, суб'єктів господарювання та органів влади електроенергією, зв'язком, послугами з транспортних перевезень, водопостачання, водовідведення, каналізації тощо. Припинення надання таких послуг та товарів, в деяких випадках навіть суттєве підвищення вартості тарифів, може призводити до соціально-політичної нестабільності, загострення внутрішньополітичних конфліктів, значних економічних втрат, послаблення інститутів влади.

Загрози КІ, як правило, розподіляються на три групи, що включають аварії й технічні збої, природні лиха та небезпечні природні явища, зловмисні дії (груп або окремих осіб, таких як терористи, злочинці й диверсанти, промислове шпигунство, а також бойові дії). Особливо небезпечними є комбіновані загрози й загрози, реалізація яких може призвести до катастрофічних і різноманітних каскадних ефектів унаслідок взаємозалежності елементів критичної інфраструктури.

Розглядаючи аварії й технічні збої, варто зауважити, що в Україні через високий рівень ***зношеності основних фондів*** існує загроза виникнення аварій на об'єктах підвищеної небезпеки, об'єктах електроенергетики й мережах життєзабезпечення. Так, зношеність основних фондів промислових підприємств за даними Державного комітету статистики становила в середньому 60,3%. Значний ризик техногенних аварій пов'язаний із наявністю на території України численних об'єктів підвищеної небезпеки, що використовують в діяльності значні обсяги небезпечних речовин. За даними ДСНС, аварії на 955 з них можуть призвести до виникнення надзвичайних ситуацій державного або регіонального рівня.

В житлово-комунальному комплексі проблеми зносу інфраструктури залишаються неподоланими. Так, протяжності ветхих та аварійних водопровідних мереж в середньому по Україні становить понад 34%, а

[1] Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України". [Електронний ресурс]. − Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015/paran7#n7

теплових і парових мереж – понад 18% від загальної протяжності таких мереж, що впливає на втрати води та теплової енергії при їх доставці споживачам, підвищення тарифів, і як наслідок провокує соціальну нестабільність.

В групі загроз природні лиха та небезпечні природні явища слід виділити: метеорологічні або надзвичайні погодні умови (снігопади, ожеледь, хуртовини, зливи, градобій, заморозки, посухи, спека, урагани, шквали, смерчі), гідрологічні (повені, селі, паводки, підтоплення, цунамі), геологічні (небезпечні екзогенні геологічні процеси – зсуви, просідання та карст), епідемії та пандемії. Поміж зазначених видів загроз варто виділити метеорологічні, частота яких в Україні значно збільшилася останніми десятиліттями, зокрема таких як обледеніння, підтоплення, посухи тощо. Найнебезпечнішими гідрологічними загрозами за наслідками для критичної інфраструктури є паводки.

Зокрема, найбільш масштабний за останні роки паводок в Україні у 2008 р. спричинив пошкодження понад 500 автомобільних мостів, розмивання 1660 км автомобільних доріг різного значення. Значну загрозу для функціонування та безпеки КІ становлять небезпечні екзогенні геологічні процеси (підтоплення, просідання, карст, зсуви). Так, до 20 % залізничних колій перебувають під впливом регіонального підтоплення земель, близько 40 % – у зонах карстових загроз, до 11 % – на територіях можливої активізації зсувних процесів. До 59 % магістральних газопроводів знаходяться в зонах можливого прояву карсту, до 21 % – регіонального підтоплення земель. Активізація небезпечних екзогенних геологічних процесів погіршує інженерно-геологічні умови експлуатації промислових споруд та інженерних мереж промислово-міських агломерацій.

Напружена воєнно-політична ситуація, в умовах якої наша держава відстоює власну територіальну цілісність і суверенітет, характеризується значним зростанням рівня таких загроз зловмисних дій, як вчинення терористичних актів і диверсійних операцій на території України, спрямованих на об’єкти КІ. Безумовно, найсерйознішою може бути потенційна загроза використання з терористичною метою об’єктів ядерної енергетики. При цьому потрібно зауважити, що на сьогодні на українських АЕС забезпечується рівень фізичного захисту, адекватний поточним загрозам.

За час проведення АТО інфраструктурні об’єкти, що знаходяться на території Харківської, Донецької, Луганської та Запорізької областей неодноразово ставали ціллю атак з боку терористично-диверсійних формувань шляхом підривів залізничного полотна та опор мостів, ЛЕП. Можна говорити про ***недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій.*** Велика протяжність інфраструктурних об’єктів унеможливлює забезпечення їх повсюдної охорони, проте мають бути захищені вузлові об’єкти та ретельно сплановані та організовані дії із забезпечення та використання резервних можливостей інфраструктурних мереж.

Відзначається значне зростання інтенсивності кібератак, здійснюваних на інформаційно-телекомунікаційну інфраструктуру в Україні. Кібератак через мережу Інтернет зазнають сервери державних установ, великих компаній, фінансових установ, політичних партій та ЗМІ, інформаційно-телекомунікаційна інфраструктура воєнних об'єктів.

Перша зареєстрована успішна кібератака на енергетичну систему України з виведенням її із ладу сталася 23 грудня 2015 р., коли російським зловмисникам вдалося успішно атакувати комп'ютерні системи управління трьох енергопостачальних компаній. Наступна, і набагато менш масштабна за наслідками, кібератака сталась вночі з 16 на 17 грудня 2016 року[2]. Протягом трохи більше однієї години була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», без струму залишились споживачі північної частини правого берега м. Києва та прилеглих районів області. Найбільше від першої кібератаки постраждали споживачі «Прикарпаття обленерго», оскільки було вимкнено близько 30 підстанцій, біля 230 тисяч мешканців залишались без світла протягом однієї-шести годин. Атака відбувалась із використанням троянської програми BlackEnergy[3].

У грудні 2016 р. в результаті обстрілів було зупинено Авдіївський коксохімічний завод, що є одним з найбільших у Європі і найбільшим в Україні виробником коксової продукції для металургії. Через обстріли та пов'язані з цим пошкодження на завод перестала в достатній кількості надходити електроенергія, і через це довелось вживати аварійних заходів. Згодом зупинилася остання лінія подачі електроенергії, що потягнуло за собою повну зупинку заводу[4]. 30 січня 2017 р. в м. Авдіївка в результаті обстрілів було перебито останню лінію постачання, що живила енергією Авдіївський коксохімічний завод. В результаті цього завод знеструмлений і було розпочато процес консервації. Завдяки роботі заводу місто отримувало тепло, воду і електрику[5].

Джерелом загроз є не тільки незадовільний стан інфраструктурних мереж (їх висока зношеність, аварійність) та вплив природних факторів (карсти, зсуви, підтоплення та ін.), а ще і комплекс економічних факторів, що проявляються через незацікавленість операторів таких мереж поліпшувати ситуацію. В цілому це впливає на ***неефективне управління безпекою критичної інфраструктури, зокрема, систем життєзабезпечення***. Так, суттєвою є загроза припинення надання життєво важливих послуг для населення через невирішені питання розрахунків між операторами інфраструктурних мереж та їх компаніями-постачальниками. В групу зловмисних дій включають також загрози, спричинені діяльністю

---

[2] Kim Zetter (January 10, 2017). The Ukrainian Power Grid Was Hacked Again. Vice Motherboard.
[3] Кім Зеттер, Wired (17 березня 2016).Хакерська атака Росії на українську енергосистему: як це було. *ТЕКСТИ*. Процитовано 18 березня 2016.
[4] [Електронний ресурс]. − Режим доступу: http://tsn.ua/ukrayina/v-avdiyivci-znestrumleno-koksohimichniy-zavod-872169.html
[5] [Електронний ресурс]. − Режим доступу: http://tsn.ua/ukrayina/v-avdiyivci-znestrumleno-koksohimichniy-zavod-872169.html

розвідувальних служб інших країн на території України, спрямованій на нанесення шкоди об'єктам критичної інфраструктури.

Незважаючи на визначення «комплексного вдосконалення правової основи захисту критичної інфраструктури» в Стратегії національної безпеки України в якості пріоритету забезпечення безпеки КІ, це завдання досі не покладено на жодний орган виконавчої влади.

Відповідно до Стратегії національної безпеки, пріоритетами забезпечення безпеки критичної інфраструктури є[6]:

- комплексне вдосконалення правової основи захисту критичної інфраструктури, створення системи державного управління її безпекою;
- посилення охорони об'єктів критичної інфраструктури, зокрема енергетичної і транспортної;
- налагодження співробітництва між суб'єктами захисту критичної інфраструктури, розвиток державно-приватного партнерства у сфері запобігання надзвичайним ситуаціям та реагування на них;
- розробка та запровадження механізмів обміну інформацією між державними органами, приватним сектором і населенням стосовно загроз критичній інфраструктурі та захисту чутливої інформації у цій сфері;
- профілактика техногенних аварій та оперативне і адекватне реагування на них, локалізація і мінімізація їх наслідків;
- розвиток міжнародного співробітництва у цій сфері.

Для виконання цих завдань протягом минулого року було здійснено і реалізовано комплекс заходів, орієнтованих на вдосконалення правової основи захисту КІ та формування системи державного управління її безпекою. Так, формування загальних підходів до забезпечення захисту критичної інфраструктури було здійснено Національним інститутом стратегічних досліджень, що розробив та представив Зелену книгу з питань захисту критичної інфраструктури[7]. Зелена книга має за мету формування узгодженої позиції щодо основ та способу реалізації державної політики в сфері захисту КІ.

У розвиток даної роботи, з метою реалізації практичних дій щодо формування системи захисту КІ в Україні, НІСД організував 25 лютого 2016 р. засідання круглого столу «Організаційні аспекти побудови системи захисту критичної інфраструктури в Україні», на якому були обговорені організаційно-інституційні аспекти розвитку даної системи на основі пропозицій, що надійшли від центральних органів виконавчої влади на запит Апарату Ради національної безпеки і оборони України (від 02.12.2015р. №3168/14-6-5-3). Разом з тим, певна повільність запровадження системи захисту КІ пов'язується із відсутністю законодавчого визначення термінології та основних засад державної політики у цій сфері.

---

[6] Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України". [Електронний ресурс]. − Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015/paran7#n7

[7] Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / Упоряд. Д.С. Бірюков, С.І Кондратов ; за заг. ред. О.М.Суходолі. – К. : НІСД, 2016. – 176 с.

У Стратегії кібернетичної безпеки України[8], термін «критична інформаційна інфраструктура» отримав таке тлумачення: «інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України». По тексту цього документу неодноразово використовується термін «критична інфраструктура» в поєднанні з поняттями «об'єкт», «кіберзахист» і т.д., що створює проблему прив'язки функцій захисту до певної категорії об'єктів, що нормативно не визначена.

Проблема відсутності чіткого визначення терміну «критична інфраструктура» в українському законодавстві, відповідно, відсутності переліку об'єктів такої категорії досі створює перешкоду для ефективного виконання невідкладних завдань забезпечення національної безпеки. В якості ілюстрації можна згадати п.6 рішення Ради національної безпеки і оборони «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України»[9], згідно якого Міністерству внутрішніх справ України доручалося забезпечити «посилену охорону об'єктів енергетики та критичної інфраструктури» при відсутності формального переліку останніх.

Потрібно підкреслити, що незважаючи на окремі кроки виконані з формування переліків об'єктів КІ, досі не затверджено порядку та критеріїв для визначення об'єктів даної категорії. Принциповою складністю, що виникає при оцінці об'єктів інфраструктури за різними критеріями є необхідність врахування взаємозв'язків між об'єктами, що неможливо без застосування науково обґрунтованих методологій, затвердженого порядку проведення комплексної оцінки загроз КІ.

Завдання захисту КІ сфокусовані на попередженні кризових ситуацій, пов'язаних із функціонуванням такої інфраструктури. Без сумніву, моніторинг та прогнозування таких кризових ситуацій має здійснюватись із застосуванням сучасних інформаційних технологій та систем підтримки прийняття рішень, реалізованих у вузлах мережі ситуаційних центрів. При цьому має бути сформований координатор діяльності різних системи державного управління.

Крім того, значно активізовано зусилля щодо посилення захисту від кіберзагроз та створення національного центру кіберзахисту для забезпечення потреб обороноздатності держави в особливий період. Питання кібербезпеки стало предметом окремого рішення РНБО, прийнято Стратегію кібербезпеки України[10], де також відображено питання формування правової

---

[8] Указ Президента України від 15.03.2016 р. № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" http://zakon2.rada.gov.ua/laws/show/96/2016

[9] Указ Президента України №189/2014 від 02.03.2014р. «Про рішення Ради національної безпеки і оборони України від 1 березня 2014 року «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» http://zakon2.rada.gov.ua/laws/show/189/2014

[10] Указ Президента України від 15.03.2016 р. № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" http://zakon2.rada.gov.ua/laws/show/96/2016

основи кіберзахисту об’єктів КІ загалом та формування системи захисту інформаційної КІ.

Прийнято Концепцію розвитку сектору безпеки і оборони України[11], де окремо акцентовано увагу на необхідності забезпечення безпеки об’єктів КІ, контррозвідувального захисту КІ, захисту критичної інформаційної інфраструктури, забезпечення відповідного інформаційно-аналітичного супроводу, зокрема шляхом створення мережі ситуаційно-кризових центрів. Удосконалено низку інших нормативно-правових актів з питань захисту об’єктів та оборони, зокрема, уточнено правові засади діяльності відновленої Національної гвардії України, зокрема щодо охорони органів державної влади, ядерних установок, важливих державних об’єктів та інших об’єктів, що можуть бути віднесені до КІ[12].

Прийняття зазначених стратегічних документів ставить нові завдання для сектору безпеки і оборони щодо посилення спроможності України забезпечити стійкість країни та сталість суспільного розвитку. Водночас, поряд із формуванням завдань та цілей політики, що на стратегічному рівні адекватно відображають виклики сьогодення, на практиці спостерігається інерційність та недостатнє розуміння проблем у цій сфері.

Варто зазначити, що на користь координації діяльності різних систем державного управління безпекою КІ свідчить порівняльний аналіз завдань Єдиної державної системи цивільного захисту, Єдиної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків та Державної системи фізичного захисту із завданнями, які визначені для системи захисту критичної інфраструктури в Зеленій книзі.

Утворення нової системи захисту КІ поряд із названими існуючими державними системами лише доповнить необхідні функції та, на основі взаємодії, дозволить покращити на стратегічному рівні здатності загальної системи забезпечення національної безпеки. Так, наприклад, протидія тероризму є широким напрямом дій що включає зокрема фізичний захист об'єктів, на які можливо здійснення терористичних актів (очевидно частина цих об’єктів буде віднесена й до критичної інфраструктури), проте боротьба з терористичною ідеологією або фінансуванням тероризму вже виходить за межі захисту критичної інфраструктури.

З метою забезпечення комплексного вдосконалення правової основи захисту КІ та створення системи державного управління її безпекою Рада національної безпеки і оборони України 29 грудня 2016 року на своєму засіданні розглянула стан реалізації пріоритетних напрямів державної політики національної безпеки України щодо забезпечення безпеки

---

[11] Указ Президента України від 14.03.2016 № 92/2016 Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року "Про Концепцію розвитку сектору безпеки і оборони України" http://zakon0.rada.gov.ua/laws/show/92/2016

[12] Постанова Кабінету Міністрів України від 1 березня 2017 р. № 106 «Про внесення зміни до переліку ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання державної власності, важливих державних об’єктів, що підлягають охороні Національною гвардією» http://zakon2.rada.gov.ua/laws/show/106-2017-п

критичної інфраструктури, визначених Стратегією національної безпеки України[13].

Указом Президента України №8/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» було введено в дію рішення Ради національної безпеки і оборони України з цього питання[14].

Висновки

В умовах ведення проти України гібридної війни значно зросли загрози критичній інфраструктурі, підтвердженням чому стали випадки пошкодження об'єктів і здійснені кібератаки на енергетичну інфраструктуру, що засвідчили вразливість об'єктів критичної інфраструктури держави до нових типів загроз.

Створення дієвої системи захисту критичної інфраструктури в Україні є актуальним завданням, що має вирішуватись в рамках загального реформування сектору безпеки і оборони із врахуванням всього існуючого спектра загроз та забезпечення взаємопов'язаності різних систем.

Зелена книга з питань захисту критичної інфраструктури, розроблена НІСД з урахуванням рекомендацій вітчизняних та зарубіжних експертів, створила необхідну основу для подальшого розроблення державної політики в сфері захисту критичної інфраструктури.

Потребує узгодження комплекс проблемних питань, пов'язаних із захистом критичної інфраструктури:

- визначення критеріїв та процедур віднесення об'єктів до критичної інфраструктури;
- розвиток державно-приватного партнерства в сфері безпеки, що вимагає вдосконалення організаційних та правових основ такої взаємодії;
- створення мережі ситуаційних центрів;
- формування нормативно встановленого порядку проведення комплексної оцінки загроз критичній інфраструктурі, загальної методології оцінки ризиків, пов'язаних із функціонуванням критичної інфраструктури.

З метою узгодження діяльності різних систем державного управління доцільним є розробка та прийняття окремого закону України «Про критичну інфраструктуру». В ньому мають бути вказані принципи державної політики щодо захисту критичної інфраструктури, відображені питання державно-приватного партнерства в частині розподілу відповідальності, визначені повноваження органів державної влади із побудови системи захисту критичної інфраструктури, а також визначення термінів та зміни у пов'язані нормативно-правові акти.

---

[13] http://www.rnbo.gov.ua/news/2678.html

[14] Указ Президента України №8/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури». [Електронний ресурс]. − Режим доступу: http://www.president.gov.ua/documents/82017-21058

Завдання щодо створення державної системи захисту критичної інфраструктури знайшло своє відображення у рішенні Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», введеного в дію Указом Президента України № 8/2017 від 16 січня 2017 року.

Важливим також є активізація міжнародного співробітництва у сфері захисту критичної інфраструктури, на що поряд із посиленням спроможності національних урядів забезпечувати захист критичної інфраструктури, звертає увагу резолюція Ради безпеки ООН щодо захисту критичної інфраструктури від терористичних атак №2341 від 13 лютого 2017 р.

Пропозиції

Враховуючи активізацію загроз критичній інфраструктури в державі та їх зростаючий вплив на національну безпеку уявляється доцільним рекомендувати:

Кабінету Міністрів України:

- забезпечити розробку та прийняття Концепції створення державної системи захисту критичної інфраструктури в Україні як основи для розроблення відповідних нормативно-правових актів і програм захисту критичної інфраструктури;
- розробити проект Закону України "Про захист критичної інфраструктури", в якому передбачити створення державної системи захисту критичної інфраструктури та визначити орган, відповідальний за координацію діяльності із захисту критичної інфраструктури;
- визначити функції, повноваження та відповідальність 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;
- запровадити критерії віднесення об’єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації;
- визначити засади державно-приватного партнерства та ресурсного забезпечення у сфері захисту критичної інфраструктури.

Міністерству внутрішніх справ України, Міністерству енергетики та вугільної промисловості України, Міністерству інфраструктури України, Держспецзв’язку:

- розробити та внести в установленому порядку на розгляд Кабінету Міністрів України проект розпорядження Кабінету Міністрів України «Про затвердження плану дій щодо реалізації Закону України «Про критичну інфраструктуру та її захист»;
- розробити та затвердити постанову Кабінету Міністрів України «Про порядок функціонування державної системи захисту критичної інфраструктури та її взаємодію із існуючими державними системами»;

- опрацювати питання щодо формування критеріїв віднесення об’єктів до критичної інфраструктури, оцінки загроз критичній інфраструктурі, планів забезпечення стійкості функціонування критичної інфраструктури та формування загальнодержавної системи взаємодії відповідно до компетенції;
- розробити та затвердити в установленому порядку державний стандарт щодо запровадження єдиних підходів до класифікації безпекових інцидентів та криз, єдиної термінології щодо оцінки та рівнів загроз тощо;
- розробити та внести в установленому порядку на розгляд Кабінету Міністрів України проект Постанови Кабінету Міністрів України «Про затвердження порядку віднесення секторів, об’єктів та систем до національної критичної інфраструктури».

Відділ енергетичної та техногенної безпеки
(С.П. Іванюта)