ПРОБЛЕМИ ОЦІНКИ ТЕРОРИСТИЧНОЇ ВРАЗЛИВОСТІ ТА ФОРМУВАННЯ ПАСПОРТІВ БЕЗПЕКИ ОБ'ЄКТІВ ЕНЕРГЕТИКИ

Анотація

Проаналізована терористична небезпека в сучасних умовах щодо об'єктів паливно-енергетичного комплексу України та проблематика адекватної оцінки терористичних загроз, зокрема, щодо оцінки достовірності інформації про них.

Обґрунтована необхідність комплексного підходу до оцінки загроз як за характером їх походження, так і за спрямованістю на окремі елементи критичної енергетичної інфраструктури.

Розбудову державної системи захисту критичної інфраструктури (КІ) запропоновано робити з урахуванням досвіду функціонування державної системи фізичного захисту, єдиної державної системи запобігання, реагування і припинення терористичних актів і мінімізації їх наслідків та єдиної державної системи цивільного захисту.

Зроблено висновок, що одними з ключових механізмів забезпечення функціонування державної системи захисту критичної інфраструктури є проведення паспортизації об'єктів КІ та використання єдиної національної системи ситуаційних центрів державних органів, яка має бути створена відповідно до Концепції розвитку сектору безпеки і оборони України, для управління в кризовій ситуації.

ПРОБЛЕМИ ОЦІНКИ ТЕРОРИСТИЧНОЇ ВРАЗЛИВОСТІ ТА ФОРМУВАННЯ ПАСПОРТІВ БЕЗПЕКИ ОБ'ЄКТІВ ЕНЕРГЕТИКИ

Небезпека тероризму в Україні

Терористична небезпека в сучасних умовах України характеризується масштабністю та розвинутою організаційною структурою. При цьому, на відміну від терористичних загроз, з якими світ стикався раніше, в Україні основна небезпека тероризму походить не від окремих терористичних угруповань, а від держави-агресора – Російської Федерації. Відповідно, ознаками тероризму в Україні є ретельна конспірація, ефективна мотивація та заохочення осіб, відібраних для вчинення злочинів, наявність агентури в державних органах, у т.ч. правоохоронних та силових, сучасне технічне оснащення, науково-інформаційна підтримка, високий рівень підготовки, наявність мережі конспіративних укриттів, навчальних баз, полігонів тощо.

Ситуацію ускладнює наявність в Україні низки ядерних об'єктів, радіоактивних та ядерних матеріалів, які можуть стати ціллю та/або засобами зловмисних дій. Привабливість цих об'єктів/матеріалів для терористів пояснюється масштабністю негативних наслідків терористичних атак на них, як радіологічних, так і соціально-політичних, які дестабілізують ситуацію у країні, переконуючи суспільство у нездатності держави забезпечити безпеку та підвищуючи злочинний статус терористів. Це стосується як можливих диверсій на ядерних установках, так і несанкціонованого поводження з радіоактивними матеріалами, які можуть бути використані, наприклад, для виготовлення «брудної» бомби та приведення її в дію, у т.ч. і за межами України з покладанням відповідальності на українську владу.

Якщо ж враховувати каскадні ефекти, коли порушення в роботі одного об'єкту критичної інфраструктури (далі – КІ) призводять до порушень в роботі інших об'єктів і систем унаслідок їх взаємозалежності, наслідком чого буде дестабілізація ситуації в країні, стає зрозумілим привабливість крупних енергетичних об'єктів для терористичних атак. Так, серйозної уваги потребує

зростання інтенсивності кібератак, що здійснюються на енергетичну інфраструктуру в Україні.

Звідси витікає, що забезпечення антитерористичного та кіберзахисту критичної енергетичної інфраструктури (включаючи ядерну) є одним із важливіших завдань держави, яке потребує єдиного системного підходу на державному, відомчому та об'єктовому рівнях.

Відповіддю на терористичні загрози стало створення в Україні державної система боротьби з тероризмом. На державному рівні було сформовано концептуальні засади та нормативно-правову базу державної політики протистояння загрозам тероризму. Так, відповідно до Закону України «Про боротьбу з тероризмом» [1] Кабінетом Міністрів України затверджено «Положення про єдину державну систему запобігання, реагування і припинення терористичних актів і мінімізації їх наслідків» [2]. Головним органом у загальнодержавній системі боротьби з терористичною діяльністю визначена Служба безпеки України. Координуючим органом цієї системи є Антитерористичний центр при СБУ (АТЦ).

Проблеми оцінки терористичної загрози

Слід зазначити, що достовірність інформації про загрозу вчинення терористичного акту (або диверсії чи будь-яких інших зловмисних дій щодо об'єктів ПЕК) можна визначити далеко не завжди. Зокрема, це стосується ситуації, коли увага суб'єктів боротьби з тероризмом може спеціально відволікатися та переключатися з одних об'єктів (регіонів) на інші. Звідси витікає невизначеність у встановленні рівня терористичної загрози, що з однієї сторони може призвести до недооцінки загрози та невчасного приведення у готовність сил та засобів, що залучаються до проведення антитерористичної операції. З іншої сторони, переоцінка загрози та перманентне знаходження суб'єктів боротьби з тероризмом у підвищеному стані готовності виснажує їх сили, а інформація про загрозу, яка має бути доведена до населення, підвищує психологічний тиск на нього, що, навпаки,

замість запобігання виникненню паніки, може призвести до поширення панічних настроїв.

Зазначене об’єктивно підвищує роль розвідувальних і контррозвідувальних заходів та органів в оцінці терористичної загрози (відповідні підрозділи СБУ та МВС, ГУР МО, СЗР, Держприкордонслужби, інших суб’єктів боротьби з тероризмом) та вимагає налагодження чіткої взаємодії цих органів та ефективного (своєчасного) обміну інформацією між ними, у т.ч. такої, що становить державну таємницю. При цьому слід враховувати, що це потребує, з одного боку, значного зменшення бар’єрів, у тому числі національних та відомчих, на шляху обміну розвідувальною інформацією, а з іншого – дотримання необхідних вимог конфіденційності та захисту джерел інформації.

При цьому слід враховувати, що інформація про загрозу теракту як будь-яка інформація про загрози, має ймовірнісний характер. Тому коли йдеться про те, що ця інформація є достовірною, то це повинно означати, що інформація була отримана з кількох джерел, вона була проаналізована, перевірена і оцінена, і на основі цієї оцінки були зроблені висновки про значиму ймовірність здійснення терористичного нападу (диверсії, реалізації інших злочинних намірів).

Таким чином, інформація про терористичний напад (диверсію) може бути кваліфікована як «достовірна» лише уповноваженими на це органами. Аналіз повноважень, функцій та сфери відповідальності державних органів з цієї точки зору показує, що головну роль тут має відігравати АТЦ при Службі безпеки України як координуюча структура головного органу державної системи протидії тероризму в державі – СБУ.

Водночас слід враховувати, що загрози критичній енергетичній інфраструктурі не обмежуються лише терористичними загрозами. Зазначене вимагає використання комплексного підходу до оцінки загроз – так званого «all hazards approach» [3].

Загрози критичній енергетичній інфраструктури та формування паспортів безпеки об'єктів КІ

Якщо розглядати **загрози КІ за характером їх походження**, то слід виділити загрози техногенного та природного походження, а також загрози, пов'язані зі зловмисними діями [3].

Так, зараз на території України «техногенне навантаження», тобто щільність підприємств, трубопроводів, комунікацій, у декілька разів вище, ніж у більшості країні Європи [4]. Якщо до цього додати ще й той факт, що більшість об'єктів енергетичної інфраструктури більш ніж на 80 % вичерпали свій ресурс, то можна уявити потенційну небезпеку цих об'єктів. За цих умов важливе значення має державна стандартизація з питань безпеки у надзвичайних та кризових ситуаціях, державна експертиза проектів і рішень стосовно техногенної та фізичної безпеки об'єктів, державний нагляд і контроль, **декларування безпеки об'єктів та їх паспортизація**.

Зокрема, відповідно до Закону України «Про об'єкти підвищеної небезпеки» [5] передбачена **декларація безпеки** об'єкта підвищеної небезпеки (документ, в якому наводяться результати аналізу ступеня небезпеки та оцінки рівня ризику цього об'єкту, та який визначає комплекс заходів, що вживаються суб'єктом господарської діяльності з метою запобігання аваріям, а також забезпечення готовності до локалізації, ліквідації аварій та їх наслідків). «Положенням про паспортизацію потенційно небезпечних об'єктів» [6] передбачена ідентифікація таких об'єктів та їх паспортизація – підготовка і надання паспорту потенційно небезпечного об'єкта (ПНО). **Паспорт ПНО** – це документ, в якому наводяться загальні дані про об'єкт, дані про небезпечні природні умови та технологічні процеси, дані щодо основних джерел небезпеки та реципієнтів надзвичайних ситуацій (тобто на які об'єкти та людей скажуться наслідки НС), аварійно-рятувальна документація тощо. Форми паспортів ПНО відповідають певному виду господарської діяльності об'єкту (вугільна шахта,

гідротехнічний об’єкт, магістральний трубопровід, родовище вуглеводнів тощо).

Аналогічні заходи передбачені й у Російській Федерації, зокрема, щодо забезпечення безпеки об’єктів паливно-енергетичного комплексу (ПЕК) [7]. Водночас паспорт безпеки об’єкта ПЕК в РФ відображає не лише характеристики цього об’єкта з точки зору його потенційної небезпеки (категорії небезпеки, отриманої виходячи з властивостей небезпечних речовин, що використовуються на об’єкті, та за впливом уражаючих факторів, що можуть мати місце у разі аварії на об’єкті), але й можливі наслідки в результаті незаконного втручання у функціонування об’єкта, оцінку стану систем інженерно-технічного та фізичного захисту, заходи із забезпечення антитерористичної захищеності. При цьому, інформація, яка міститься у паспорті безпеки, віднесена до інформації з обмеженим доступом.

Щодо антитерористичної захищеності об’єктів ядерно-енергетичного комплексу України, то в рамках Державної системи фізичного захисту [8, 9] за результатами оцінки вразливості [10] готується низка документів, які за своєю сутністю відповідають паспорту ПНО, але є значно ширшими та системними з точки зору оцінки небезпек. Так, Звіт з оцінки вразливості окрім загальних даних про об’єкт та виявлені джерела небезпеки містить ще й опис загроз, сценарії дій правопорушників та аналізує здатність системи фізичного захисту та об’єктового плану взаємодії протистояти цим загрозам.

Державна система фізичного захисту (ДСФЗ) та використання досвіду її функціонування для розбудови в Україні системи захисту критичної енергетичної інфраструктури

Заходи, передбачені в рамках ДСФЗ, включають весь ланцюжок дій – від оцінки загроз та категоризації об’єктів системи, до встановлення конкретних вимог до систем фізичного захисту, оцінки вразливості об’єктів,

ризиків радіаційних наслідків, проведення перевірок систем ФЗ та планів взаємодії. Зазначене врегульовано низкою нормативно-правових актів:

1) проведення оцінки загроз ядерним установкам (ЯУ), ядерним матеріалам (ЯМ), радіоактивним відходам (РАВ), іншим джерелам іонізуючого випромінювання (ДІВ) на державному рівні [11];

2) визначення категорії ЯУ, ЯМ, РАВ та об'єктів, призначених для поводження з ними, категорії ДІВ, а також вимог до фізичного захисту цих об'єктів залежно від їх категорії [12];

3) визначення правил фізичного захисту [13], встановлення вимог до систем фізичного захисту [14] та планів забезпечення фізичного захисту [15];

4) забезпечення охорони [16] (включаючи відомчу [17]), встановлення вимог до інженерно-технічних засобів систем ФЗ [18], зонування території об'єкта та встановлення вимог щодо доступу, виявлення та спостереження, перевірки осіб та транспортних засобів [19];

5) проведення оцінки вразливості ядерних установок та ядерних матеріалів та оцінки ризиків радіаційних наслідків на випадок вчинення акту ядерного тероризму та крадіжки ядерного матеріалу ([10] – включає визначення цілей та завдань правопорушників, сценаріїв їх дій, аналіз радіаційних наслідків, визначення ймовірностей виявлення, переривання та нейтралізації правопорушників, оцінку ризиків та виявлення вразливих цілей, розроблення рекомендацій);

6) розробка та підтримка дієздатності державного та об'єктового планів взаємодії на випадок вчинення диверсії (акту ядерного тероризму) [20, 21];

7) проведення оцінки стану системи фізичного захисту [22], проведення державної перевірки систем фізичного захисту та планів взаємодії у разі вчинення актів ядерного тероризму [23].

Подібні підходи можуть бути використані і при розбудові в Україні державної системи захисту КІ (зокрема, критичної енергетичної інфраструктури). Водночас, на відміну від об'єктів ядерної інфраструктури,

категоризація яких здійснюється, фактично, за одним критерієм – небезпекою, яку несуть ядерні чи радіоактивні матеріали, інші джерела іонізуючого випромінювання, визначення критеріїв, за якими об'єкти мають бути віднесені до критичної інфраструктури, є значно складнішим завданням.

Складність цього завдання багато у чому обумовлено багатовимірністю наслідків та взаємозалежністю об'єктів критичної інфраструктури – тобто каскадними ефектами, коли порушення в роботі одного об'єкту КІ призводять до порушень в роботі інших об'єктів і систем унаслідок їх взаємозалежності. Результатом же каскаду порушень у роботі КІ може стати дестабілізація загальної ситуації в країні. Загальні методологічні підходи до категоризації об'єктів критичної інфраструктури з урахуванням цих факторів викладені в аналітичній записці Національного інституту стратегічних досліджень (НІСД) [24].

На думку НІСД, при формуванні паспортів безпеки об'єктів КІ **загрози КІ слід також розглядати** не тільки з точки зору характеру їх походження, але й **з точки зору виділення елементів КІ, на які ці загрози спрямовані,** за кожною групою об'єктів відповідно до запропонованої у [24] категоризації:

фізичні елементи, зокрема, обладнання та ресурси об'єктів КІ;

системи управління та комунікації, зокрема, системи автоматичного управління та регулювання роботи об'єктів, системи зв'язку тощо;

персонал об'єктів, зокрема, диспетчерський, оперативний персонал, який безпосередньо забезпечує функціонування критичної інфраструктури.

Виділення спрямованості дії загроз методологічно дозволяє більш системно підійти до формування державної політики й організації системи захисту КІ [3]. У планах захисту КІ, розроблених операторами, погоджених і схвалених відповідними державними органами, мають бути докладно описані заходи протидії загрозам за наступними напрямами захисту:

фізичний захист (Physical) – спрямований на забезпечення захищеності об'єктів від несанкціонованого доступу, попередження та

припинення диверсій, крадіжки або будь-якого іншого незаконного вилучення обладнання, пристроїв та матеріалів;

технічний захист (Technical) – забезпечення технологічної безпеки, підвищення відмовостійкості й живучості систем, функціональне резервування;

персонал (Personnel) – підготовка та перевірка персоналу, контроль його здатності до виконання визначених функцій, захищеність персоналу;

інформаційні технології (IT) – захист інформації, систем зв'язку і управління;

юридичний (Legal) – врегулювання питань функціонування інфраструктури у кризових ситуаціях, закріплення розподілу відповідальності у нормативних і правових документах, розробка керівництв й інструкцій для персоналу, у тому числі щодо взаємодії в умовах кризової ситуації;

плани відновлення (Recovery Plans) – створення планів, резервів та сервісів для швидкого відновлення втрачених функцій.

Зазначені напрями захисту та реагування мають бути детально опрацьовані при розробці паспортів безпеки об'єктів КІ. У свою чергу паспорти безпеки мають скласти основу Національного плану захисту КІ, в якому слід визначити систему взаємодії суб'єктів захисту критичної інфраструктури та розподіл ресурсів на загальнодержавному рівні реагування на загрози КІ.

Іншою складовою системи захисту КІ в Україні має стати створення єдиної системи ситуаційних центрів державних органів, що входять до сектору безпеки і оборони, а також інших органів державної та місцевої влади відповідно до Концепції розвитку сектору безпеки і оборони України [25], які мають стати ключовим інструментом інформаційно-аналітичної підтримки процесу прийняття рішень на усіх рівнях управління кризовою ситуацією.

При цьому саме паспорти безпеки (інформація, яка в них знаходиться) мають стати базою для інформаційно-аналітичного забезпечення діяльності державної системи захисту КІ в Україні, зокрема щодо аналізу, прогнозування, розробки заходів з реагування на кризові та надзвичайні ситуації.

Висновки та рекомендації

Терористична небезпека в сучасних умовах України вимагає єдиного системного підходу до забезпечення антитерористичного захисту критичної інфраструктури на державному, відомчому та об'єктовому рівнях.

На даний момент в Україні діють дві основні системи реагування на кризові ситуації, спричинені зловмисними діями щодо об'єктів критичної енергетичної інфраструктури: державна система боротьби з тероризмом (єдина державна система запобігання, реагування і припинення терористичних актів і мінімізації їх наслідків) та державна система фізичного захисту, які мають детально пророблені підходи до реагування у кожній зі своїх сфер. Враховуючи ж небезпеку технологічного тероризму, ці системи мають взаємодіяти і з державною системою реагування на надзвичайні ситуації природного та техногенного характеру (єдиною державною системою цивільного захисту), яка опікується, у т.ч., питаннями аварійної готовності та реагування на надзвичайні ситуації природного та техногенного походження на об'єктах ПЕК, включаючи ядерні установки.

Саме ці три системи разом із державною системою кіберзахисту (яка наразі формується) мають стати основою для розбудови в Україні сучасної системи захисту критичної інфраструктури, одним із ключових механізмів забезпечення функціонування якої є **проведення паспортизації об'єктів критичної інфраструктури,** яка потрібна не лише для виявлення джерел небезпеки, але й для категоризації об'єктів КІ та оцінки здатності систем захисту КІ протистояти усім типам загроз [3]. При цьому, на відміну від діючих вимог до паспорту потенційно небезпечного об'єкту, у паспорті

безпеки об’єкту КІ мають бути враховані загрози усіх типів (будь-якого походження – природного, техногенного, пов’язані зі зловмисними діями, та спрямовані на будь-які елементи КІ – обладнання, матеріали, системи управління, інформацію, персонал тощо) та обґрунтована спроможність системи захисту протистояти усім цим загрозам.

Для міжсистемної взаємодії державних систем реагування та захисту доцільним вбачається **використання національної мережі ситуаційно-кризових центрів** (НМ СКЦ). При цьому одними із ключових елементів НМ СКЦ, з точки зору захисту критичної інфраструктури, мають стати галузевий ситуаційно-кризовий центр Міненерговугілля та Національний центр з питань захисту критичної інфраструктури.

Зважаючи на зазначене, вважається доцільним рекомендувати:

1) Кабінету Міністрів України спільно з СБУ забезпечити розробку:

– проекту Закону України «Про захист критичної інфраструктури», в якому з урахуванням рекомендацій Зеленої книги з питань захисту КІ [3] визначити, зокрема, орган влади, який буде відповідальним за координацію діяльності із захисту критичної інфраструктури;

– проекту акту КМ України щодо встановлення вимог до паспорту безпеки об’єкту КІ, передбачивши врахування загроз усіх типів (будь-якого походження та спрямованих на будь-які елементи КІ), визначення заходів щодо запобігання реалізації загроз, реагування на випадок кризової ситуації та обґрунтування здатності системи захисту протистояти усім цим загрозам;

– проекту Національного плану захисту критичної інфраструктури (за результатами паспортизації об’єктів КІ);

2) Міністерству енергетики та вугільної промисловості:

– розробити вимоги до Паспорту безпеки об’єкту ПЕК;

– провести попередню паспортизацію та категоризацію об’єктів ПЕК з обґрунтуванням віднесення їх до об’єктів критичної інфраструктури;

– із залученням Держатомрегулювання, ДСНС, Мінекономіки розробити проекти змін до відповідних чинних нормативних актів щодо запровадження Паспортів безпеки об’єктів ПЕК.

Відділ енергетичної та техногенної безпеки

(Д. Г. Бобро, О. М. Суходоля)

№ 38, Серія «Національна безпека»

Список використаної літератури

[1] Закон України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV. [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/638-15

[2] Постанова Кабінету Міністрів України від 18.02.2016 № 92 «Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків». [Електронний ресурс]. – Законодавство України. – Режим доступу: http://www.kmu.gov.ua/control/ru/cardnpd?docid=248852549

[3] Зелена книга з питань захисту критичної інфраструктури в Україні. 2015 р. [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/File/2015_nauk_an_rozrobku/Green%20Paper%20-%20dopovid.pdf

[4] Стеблюк М.І. «Цивільна оборона». Підручник. – К.: Знання, 2006 р.

[5] Закон України «Про об’єкти підвищеної небезпеки» від 18.01.2001 № 2245-III. [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/2245-14

[6] Наказ Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 18.12.2000 № 338, зареєстрований в Міністерстві юстиції України 24.01.2001 за № 62/5253 «Про затвердження Положення про паспортизацію потенційно небезпечних об’єктів». [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/z0062-01

[7] Федеральный закон Российской Федерации от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» – ИПС «Закон». [Електронний ресурс]. – Режим доступу: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102149573&rdk=&backlink=1

[8] Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» від 19.10.2000 № 2064-III. [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2064-14

[9] Постанова Кабінету Міністрів України від 21.12.2011 № 1337 «Про затвердження Порядку функціонування державної системи фізичного захисту». [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/1337-2011-%D0%BF

[10] Наказ Держатомрегулювання України від 30.11.2010 № 169, зареєстрований в Міністерстві юстиції України 22.12.2010 за № 1309/18604 «Про затвердження Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів» (НП 306.8.167-2010). [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z1309-10

[11] Про нову редакцію Проектної загрози ядерним установкам, ядерним матеріалам, радіоактивним відходам, іншим джерелам іонізуючого випромінювання в Україні, Указ Президента України від 16.10.2012 № 600/2012 (зі змінами, внесеними згідно з Указом Президента України від 27.08.2015 № 521). [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/600/2012/paran2#n2

[12] Постанова Кабінету Міністрів України від 26.04.2003 № 625 «Про затвердження Порядку визначення рівня фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання відповідно до їх категорії». [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/625-2003-%D0%BF

[13] Наказ Держатомрегулювання України від 04.08.2006 № 116, зареєстрований в Міністерстві юстиції України 21.09.2006 за № 1067/12941 «Про затвердження Правил фізичного захисту ядерних установок та ядерних матеріалів» (НП 306.8.126-2006). [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z1067-06

[14] Наказ Держатомрегулювання України від 28.08.2008 № 156, зареєстрований в Міністерстві юстиції України 21.10.2008 за № 1000/15691 «Про затвердження Загальних вимог до систем фізичного захисту ядерних установок та ядерних матеріалів і Загальних вимог до систем фізичного захисту ядерних матеріалів при їх перевезенні» (НП 306.8.146-2008 та НП 306.8.147-2008). [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/z0999-08

[15] Наказ Держатомрегулювання України від 04.12.2008 № 196, зареєстрований в Міністерстві юстиції України 23.12.2008 за № 1223/15914 «Про затвердження Вимог до змісту та структури плану забезпечення фізичного захисту ядерної установки та ядерних матеріалів і плану забезпечення обліку та контролю ядерних матеріалів» (НП 306.8.150-2008). [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/z1223-08

[16] Наказ Держатомрегулювання України від 23.11.2010 № 164, зареєстрований в Міністерстві юстиції України 15.12.2010 за № 1265/18560 «Про затвердження вимог щодо застосування охорони в системі фізичного захисту ядерних установок, об'єктів, призначених для поводження з радіоактивними відходами, іншими джерелами іонізуючого випромінювання, радіоактивних матеріалів» (НП 306.8.166-2010). [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z1265-10

[17] Наказ Міністерства палива та енергетики України від 08.10.2007 № 480, зареєстрований в Міністерстві юстиції України 12.11.2007 за № 1264/14529 «Про організацію діяльності відомчої воєнізованої охорони Міністерства палива та енергетики України». [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/z1262-07

[18] Наказ Держатомрегулювання України від 05.12.2011 № 176, зареєстрований в Міністерстві юстиції України 23.12.2011 за №1505/20243 «Про затвердження вимог до комплексу інженерно-технічних засобів системи фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання». [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/z1505-11

[19] Наказ Держатомрегулювання України від 05.12.2011 № 177, зареєстрований в Міністерстві юстиції України 23.12.2011 за № 1509/20247 «Про затвердження вимог до зон обмеження доступу, контролю та управління доступом у зони обмеження доступу». [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/z1509-11

[20] Постанова Кабінету Міністрів України від 24.07.2013 № 598 «Про затвердження державного плану взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій щодо ядерних установок, ядерних матеріалів, інших джерел іонізуючого випромінювання у процесі їх використання, зберігання або перевезення, а також щодо радіоактивних відходів у процесі поводження з ними». [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/598-2013-%D0%BF

[21] Наказ Держатомрегулювання України від 22.11.2010 № 163, зареєстрований в Міністерстві юстиції України 15.12.2010 за № 1264/18559 «Про затвердження вимог до об’єктового плану взаємодії у разі вчинення диверсії» (НП 306.8.165-2010). [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z1264-10

[22] Наказ Держатомрегулювання України від 20.12.2010 № 179, зареєстрований в Міністерстві юстиції України 30.12.2010 за № 1443/18738 «Про затвердження вимог до оцінки стану системи фізичного захисту ядерної установки» (НП 306.8.168-2010). [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z1443-10

[23] Постанова Кабінету Міністрів України від 12.03.2003 № 327 «Про затвердження Порядку проведення державної перевірки систем фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання та планів взаємодії у разі вчинення актів ядерного тероризму». [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/327-2003-%D0%BF

[24] Бобро Д. Г. «Удосконалення методології ранжування об'єктів критичної інфраструктури та їх віднесення до критичної інфраструктури». Аналітична записка. [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/2249/

[25] 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». [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/92/2016