УДК: 343:34 Doi: https://doi.org/10.32918/nrs.2019.3(83).07

Проблеми кримінальної відповідальності за посягання на об'єкти критичної інфраструктури в ядерній енергетиці

■ **Таран О. В.**
Національна академія внутрішніх справ, м. Київ, Україна
ORCID: https://orcid.org/0000-0003-4752-9924

■ **Сандул О. Г.**
Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки» м. Київ, Україна
ORCID: https://orcid.org/0000-0002-5640-1482

Наразі в Україні відбувається формування спеціального законодавства щодо кримінальної відповідальності за посягання на об'єкти критичної інфраструктури.

В цьому напрямку Кабінетом Міністрів України схвалена Концепція створення державної системи захисту критичної інфраструктури.

В даній роботі на загальному фоні захисту об'єктів критичної інфраструктури розглянуто цей напрямок законодавства стосовно об'єктів в галузі ядерної енергетики.

Докладно проаналізовано сучасний стан законодавчого регулювання підстав кримінальної відповідальності за злочинну діяльність, що посягає на об'єкти критичної інфраструктури ядерної енергетики. Обговорюється питання на предмет достатності та належності існуючого рівня такої відповідальності.

В роботі, як приклад, наведено перелік деяких основних об'єктів критичної інфраструктури у відповідності до нормативно-правових актів у сфері захисту критичної інфраструктури та надана їх класифікація.

Крім того, розглянуто такі поняття як «критична інфраструктура», що є відносно новим поняттям в національному законодавстві, «акт незаконного втручання», «комп'ютерні злочини», «критична інформаційна інфраструктура» та інші, що мають важливе значення для ядерної енергетики. Проведено аналіз понять, що містяться в різних нормативно-правових документах.

В роботі підкреслюється, що в законодавстві України наразі відсутні спеціальні (окремі) норми стосовно кримінальної відповідальності за посягання на об'єкти критичної інфраструктури. З цього приводу розглянуто також деякі перспективи розгляду цих питань. Особливо це стосується підстав кримінальної відповідальності, щодо захисту об'єктів критичної інфраструктури в галузі ядерної енергетики.

Обговорюється також питання перспективи щодо подальшого розроблення спеціального закону, яким буде визначено напрям розвитку відповідного законодавства про загальне врегулювання цих питань.

В статті також наголошено про необхідність внесення деяких змін і доповнень до Кримінального кодексу України.

К л ю ч о в і с л о в а: об'єкти критичної інфраструктури, нормативно-правові акти, ядерна енергетика

Оприлюднення Урядом України Концепції створення державної системи захисту критичної інфраструктури [1] (далі Концепція) визначило основу та новий етап розвитку законодавства і правозастосовної практики у відповідній сфері.

Зважаючи на мету Концепції якою є визначення основних напрямів, механізмів і строків комплексного правового врегулювання питання захисту критичної інфраструктури та створення системи державного управління у сфері захисту критичної

інфраструктури. Створення державної системи захисту критичної інфраструктури спрямоване на забезпечення стійкості критичної інфраструктури до загроз усіх видів, включаючи загрози природного і техногенного характеру, загрози, спричинені протиправними діями, та інші загрози [1], можна прогнозувати, що зміни та перетворення відбудуться у багатьох галузях права.

У статті розглянуто деякі нормативні положення у сфері захисту критичної інфраструктури, проаналізовано існуючі підстави кримінальної відповідальності щодо захисту об'єктів критичної інфраструктури ядерної енергетики та інших галузей економіки від протиправних посягань. З цією метою розглянуто поняття критична інфраструктура, об'єкти критичної інфраструктури, низку суміжних понять, а також норми Кримінального кодексу (КК) України, якими передбачено відповідальність за посягання на об'єкти критичної інфраструктури, сформульовано висновки щодо поточного стану кримінального законодавства у цій частині.

Поняття «критична інфраструктура» є відносно новим для національного законодавства, правової теорії та правозастосовної практики, проте у деяких нормативних актах і документах надаються його визначення. Так, якщо звернутись до згаданої Концепції, то критична інфраструктура визначається як сукупність об'єктів, які є стратегічно важливими для економіки і безпеки держави, суспільства, населення та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам України [1]. Що стосується складових критичної інфраструктури, то йдеться про системи, об'єкти і ресурси, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки.

У Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури, що затверджений Постановою Кабінету Міністрів № 563 від 23 серпня 2106 року критична інфраструктура визначається як сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних фінансових збитків та людських жертв [2]. До об'єктів критичної інфраструктури віднесено підприємства та установи (незалежно від форми власності) таких галузей, як ядерна енергетика, інформаційні технології та телекомунікації (електронні комунікації), та інших, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення [2]. У цьому документі інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури визначені як критична інформаційна інфраструктура держави.

У проекті Закону України «Про критичну інфраструктуру та її захист» (розроблений Мінекономрозвитку на виконання доручення Кабінету Міністрів України від 21.02.2017 № 1835/4/1–17 до Указу Президента України від 16 січня 2017 року № 8/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури») зазначено, що критична інфраструктура — це об'єкти, які є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

Що стосується об'єктів критичної інфраструктури, то у проекті передбачено, що до них можуть бути віднесені: підприємства, установи, організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, централізованого водовідведення, постачання теплової енергії, гарячої води, електричної енергії і газу, виробництва продуктів, харчування, охорони здоров'я;

3) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави (зокрема ДНТЦ ЯРБ та ДП «НАЕК «Енергоатом»);

4) підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду;

5) є об'єктами підвищеної небезпеки;

6) є об'єктами, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру;

7) є об'єктами, порушення функціонування яких призведе до кризової ситуації регіонального значення [3].

Тобто, із наведених та інших визначень поняття критичної інфраструктури убачається, що його формування відбувається на основі існуючих нормативних визначень та із урахуванням сучасних завдань щодо створення єдиної державної системи захисту критичної інфраструктури.

У контексті досліджуваної проблеми становить інтерес визначення поняття «акт незаконного втручання» як діяння, що створило загрозу безпечному функціонуванню об'єкта критичної інфраструктури та призвело до одного або декількох з таких наслідків: порушило його безперервність і стійкість; створило реальні чи потенційні загрози національній безпеці [3].

Згадані положення в цілому дають уявлення про поняття критичної інфраструктури та її складові, а також можливі загрози її безпеці: природні, техногенні, терористичні, кібератаки, інші протиправні дії.

Чинний КК України не містить спеціальних (окремих) норм, якими передбачена відповідальність за суспільно небезпечні діяння, що посягають на об'єкти критичної інфраструктури, їх визначення та інші суміжні поняття також не згадуються у КК України. Водночас, його системний аналіз показав, що нормативне регулювання підстав кримінальної відповідальності за такі посягання існує.

Мета статті — висвітлення можливої кримінальної відповідальності за посягання на об'єкти критичної інфраструктури.

Перш ніж перейти до розгляду відповідних норм, потрібно наголосити, що наразі лише відбувається формування та становлення згаданого інституту, триває законотворча робота, зокрема з розроблення спеціального закону, яким буде визначено напрями подальшого розвитку законодавства у відповідній сфері, створення переліку об'єктів критичної інфраструктури, тому окремі питання кримінальної відповідальності у цій роботі ми розглядаємо як перспективи удосконалення законодавства.

Отже, як було зазначено, наразі відсутні спеціальні (окремі) норми, у яких передбачено кримінальну відповідальність за посягання на об'єкти критичної інфраструктури. Водночас, кримінально-правовий захист поширюється на низку об'єктів, що можуть бути віднесені до критичної інфраструктури (відповідно до проекту спеціального закону, Концепції та ін. див. вище). Крім того, існує низка нормативних актів, які визначають такі об'єкти (Закон України № 2245-III від 18.01.2001 р. «Про об'єкти підвищеної небезпеки»; Постанова Кабінету Міністрів України № 306 від 29 лютого 2012 р. «Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності та визначається періодичність здійснення планових заходів державного нагляду (контролю) у сфері техногенної та пожежної безпеки»; Постанова Кабінету Міністрів України № 83 від 04.03.2015 «Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави» та ін.).

Норми, якими передбачено відповідальність за злочинні посягання на об'єкти критичної інфраструктури розміщено у різних розділах Особливої частини, що свідчить про те, що законодавець по-різному визначає родовий об'єкт цих злочинів.

Злочини проти основ національної безпеки України. Родовим об'єктом цих злочинів є національна безпека. У Законі України «Про національну безпеку України» національна безпека визначається як захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Загрози національній безпеці України — явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [4].

Злочинні посягання на об'єкти критичної інфраструктури можуть бути вчинені шляхом диверсії (ст. 113 КК України).

Диверсія — це вчинення з метою ослаблення держави вибухів, підпалів або інших

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

дій, спрямованих на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, на зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення, а також вчинення з тією самою метою дій, спрямованих на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій [5].

Серед предметів цього злочину — об'єкти, що мають важливе народногосподарське чи оборонне значення. Цей злочин вчиняється з метою ослаблення держави (спеціальна мета), що відрізняє його від інших злочинів. Поняття «об'єкти, що мають важливе народногосподарське значення чи оборонне значення» не передбачене у законодавстві України і правозастосовувачі при визначенні належності певних об'єктів до згаданих, орієнтуються на поняття, що надаються у нормативних актах, які перераховані вище, а також інші нормативні приписи, наприклад, Закон України «Про національну безпеку України», у якому розкрито поняття громадської безпеки, державної безпеки, національної безпеки, оборонно-промислового комплексу [4].

Злочини проти власності. Родовим об'єктом цих злочинів є право власності, що включає володіння, користування та розпорядження майном.

Злочинне посягання на об'єкти критичної інфраструктури може бути вчинене шляхом умисного пошкодження об'єктів електроенергетики (ст. 194–1 КК України). Для цього злочину додатковим обов'язковим об'єктом є нормальна (стабільна) робота об'єктів електроенергетики.

Умисне пошкодження або руйнування об'єктів електроенергетики є кримінально караним, якщо ці дії призвели або могли призвести до порушення нормальної роботи цих об'єктів, або спричинило небезпеку для життя людей.

Предметом цього злочину є об'єкти електроенергетики. Деякі з них за чинним законодавством належать до особливо важливих об'єктів, які забезпечують функціонування енергетичної системи України. Перелік таких об'єктів визначено у Постанові Кабінету Міністрів України «Про затвердження переліку особливо важливих об'єктів електроенергетики, у тому числі територій забороненої зони та контрольованої зони гідротехнічних споруд, які підлягають охороні відомчою воєнізованою охороною» [6]. Крім того, зазначеною Постановою окремо визначені атомні електростанції ДП «НАЕК «Енергоатом», а також окремо ядерні установки, що охороняються Національною гвардією України.

Злочини проти громадської безпеки. Поняття громадської безпеки, яка є родовим об'єктом цих злочинів визначається в Законі України «Про національну безпеку України» як захищеність життєво важливих для суспільства та особи інтересів, прав і свобод людини і громадянина, забезпечення яких є пріоритетним завданням діяльності сил безпеки, інших державних органів, органів місцевого самоврядування, їх посадових осіб та громадськості, які здійснюють узгоджені заходи щодо реалізації і захисту національних інтересів від впливу загроз [4].

Посягання на об'єкти критичної інфраструктури можуть бути вчинені шляхом терористичного акту (ст. 258 КК України).

Терористичний акт, тобто застосування зброї, вчинення вибуху, підпалу чи інших дій, які створювали небезпеку для життя чи здоров'я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій з тією самою метою [5].

Вчинення терористичного акту здійснюється зі спеціальною метою, що дозволяє відмежувати цей злочин від інших. Задля досягнення зазначеної мети (однієї або декількох) злочинці можуть здійснити терористичний акт на об'єктах критичної інфраструктури, що визначає підвищену суспільну небезпеку таких дій, оскільки порушення нормального функціонування об'єктів критичної

інфраструктури або їх руйнація може вплинути на різні сфери безпеки.

На особливій важливості запобігання терористичним актам на об'єктах критичної інфраструктурі наголошується на міжнародному рівні. Так, 13 лютого 2017 року Рада Безпеки ООН ухвалила резолюцію 2341 щодо захисту критичної інфраструктури від терористичних атак. Ініціатором резолюції виступила Україна, а співавторами були понад 30 держав — членів ООН.

Резолюція має на меті підвищення ефективності міжнародних зусиль з протидії терористичним атакам проти об'єктів критичної інфраструктури, зокрема в рамках Глобальної контртерористичної стратегії ООН [7]. Серед іншого, у цьому документі зазначено, що всі держави-члени повинні кваліфікувати терористичні акти як серйозні кримінальні правопорушення у внутрішньодержавних законах і положеннях, і забезпечити встановлення кримінальної відповідальності за терористичні акти, спрямовані на знищення або дезактивацію критично важливих об'єктів інфраструктури, а також за планування, підготовку, фінансування і матеріально-технічну підтримку таких нападів [8]. Тобто пропонується додатково встановити кримінальну відповідальність за знищення або дезактивацію критично важливих об'єктів внаслідок терористичного акту, а також дії щодо планування, підготовки, фінансування і матеріально-технічної підтримки таких нападів.

Напад на об'єкти, на яких є предмети, що становлять підвищену небезпеку для оточення (ст. 261 КК України) — напад на об'єкти, на яких виготовляються, зберігаються, використовуються або якими транспортуються радіоактивні, хімічні, біологічні чи вибухонебезпечні матеріали, речовини, предмети, з метою захоплення, пошкодження або знищення цих об'єктів [5].

Предметом цього злочину є радіоактивні, хімічні, біологічні чи вибухонебезпечні матеріали, речовини, предмети. Такі предмети зазвичай знаходяться на об'єктах, які можуть бути віднесені до критичної інфраструктури, наприклад, ядерні матеріали на промислових майданчиках атомних електростанцій. Спеціальна мета щодо захоплення, пошкодження або знищення об'єктів, які можуть бути віднесені до критичної інфраструктури дозволяє відмежувати цей злочин від інших.

Умисне знищення або пошкодження об'єктів житлово-комунального господарства (ст. 270–1 КК України), якщо це призвело або могло призвести до неможливості експлуатації, порушення нормального функціонування таких об'єктів, що спричинило небезпеку для життя чи здоров'я людей або майнову шкоду у великому розмірі.

Під об'єктами житлово-комунального господарства в цій статті слід розуміти житловий фонд, об'єкти благоустрою, теплопостачання, водопостачання та водовідведення, а також їх мережі чи складові (кришки люків, решітки на них тощо) [5].

Якість та стабільність послуг щодо водопостачання, водовідведення, теплопостачання — запорука не тільки нормального функціонування різних об'єктів, а й питання їх безпеки. Тому підприємства, які надають такі послуги відносять до об'єктів критичної інфраструктури.

Злочини проти безпеки руху та експлуатації транспорту. Безпека руху та експлуатації транспорту як родовий об'єкт цих злочинів є складовою громадської безпеки. Поняття транспорту, що визначене в Законі України «Про транспорт» як однієї з найважливіших галузей суспільного виробництва і покликаний задовольняти потреби населення та суспільного виробництва в перевезеннях [9] вужче, ніж те, що використовується у КК України. Для його правильного розуміння потрібно звернутись також до Закону України «Про трубопровідний транспорт» [10], у якому розкрито поняття: магістральний трубопровід, промислові трубопроводи, об'єкти трубопровідного транспорту.

Пошкодження шляхів сполучення і транспортних засобів (ст. 277 КК України) ядерної енергетики. Кримінальна відповідальність передбачена за умисне руйнування або пошкодження шляхів сполучення, споруд на них, рухомого складу або суден, засобів зв'язку чи сигналізації, а також інші дії, спрямовані на приведення зазначених предметів у непридатний для експлуатації стан, якщо це спричинило чи могло спричинити аварію поїзда, судна або порушило нормальну роботу транспорту, або створило

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

небезпеку для життя людей чи настання інших тяжких наслідків [5].

Нормальні умови життєдіяльності людей, як складова громадської безпеки, а також стала робота об'єктів ядерної енергетики залежать від стабільного функціонування шляхів сполучення, безпеки руху та експлуатації різних видів транспорту. Тому ці об'єкти можуть бути віднесені до елементів критичної інфраструктури.

Блокування транспортних комунікацій, а також захоплення транспортного підприємства (ст. 279 КК України). У цій статті передбачено відповідальність за блокування транспортних комунікацій шляхом влаштування перешкод, відключення енергопостачання чи іншим способом, яке порушило нормальну роботу транспорту або створювало небезпеку для життя людей, або настання інших тяжких наслідків; захоплення вокзалу, аеродрому, порту, станції або іншого транспортного підприємства, установи або організації.

Деякі предмети злочину, визначені у цій нормі можуть бути віднесені до об'єктів критичної інфраструктури.

Пошкодження об'єктів магістральних або промислових нафто-, газо-, конденсатопроводів та нафтопродуктопроводів (ст. 292 КК України) в енергетичному секторі.

Кримінальна відповідальність передбачена за пошкодження чи руйнування магістральних або промислових нафто-, газо-, конденсатопроводів чи нафтопродуктопроводів, відводів від них, технологічно пов'язаних з ними об'єктів, споруд, засобів обліку, автоматики, телемеханіки, зв'язку, сигналізації, а також незаконне втручання в роботу технологічного обладнання, якщо ці дії призвели до порушення нормальної роботи зазначених трубопроводів або створили небезпеку для життя людей [5].

Із законодавчого визначення поняття «магістральний трубопровід» можна виокремити характеристики цього об'єкта, що вказують на його значення для електроенергетики та багатьох інших галузей економіки та життєдіяльності суспільства. Такі об'єкти очевидно належать до об'єктів критичної інфраструктури.

Зважаючи на те, що порушення нормального функціонування об'єктів критичної інфраструктури як спеціальна мета не визначаються у нормах КК України, у випадках, якщо такою метою є ослаблення держави, кваліфікація може здійснюватись за сукупністю злочинів, одним з яких є диверсія (ст. 113 КК України).

Злочини проти авторитету органів державної влади, органів місцевого самоврядування, об'єднань громадян та злочини проти журналістів. Родовий об'єкт злочинів, які розміщені у частині розділу щодо авторитету органів державної влади, органів місцевого самоврядування, об'єднань громадян — дискусійне питання у теорії кримінального права, проте переважно його визначають як суспільні відносини у сфері діяльності (порядок управління) органів державної влади, органів місцевого самоврядування, об'єднань громадян.

Умисне пошкодження ліній зв'язку (ст. 360 КК України) — умисне пошкодження кабельної, радіорелейної, повітряної лінії зв'язку, проводового мовлення або споруд чи обладнання, які входять до їх складу, якщо воно спричинило тимчасове припинення зв'язку [5].

Предмети злочину, визначені у кримінально-правовій нормі належать до інформаційно-комунікаційних технологій, а підприємства, установи, організації, що надають такі послуги можуть бути визначені як об'єкти критичної інфраструктури.

Державне значення стабільного функціонування ліній зв'язку відзначається будь-якою країною, а також на міжнародному рівні. Наприклад, у Міжнародній конвенції про боротьбу з бомбовим тероризмом зазначено, що об'єкт інфраструктури означає будь-який об'єкт, який знаходиться в державній чи приватній власності та який надає або розподіляє послуги в інтересах населення такі, як водопостачання, каналізація, енергопостачання, постачання палива чи зв'язок [11].

Тут також має значення спеціальна мета учинення злочину. Якщо пошкодження ліній зв'язку вчиняється з метою порушення функціонування, пошкодження або знищення об'єктів критичної інфраструктури задля ослаблення держави, то дії особи можуть бути кваліфіковані або за ст. 113 КК України, або за сукупністю злочинів.

Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Родовим об'єктом цих злочинів визначають інформаційні відносини, засобом забезпечення яких є ЕОМ, системи, комп'ютерні мережі та мережі електрозв'язку [12, с. 373].

Як убачається з положень нормативних актів, до яких ми звертались у цій роботі та інших документів, об'єкти критичної інфраструктури можна класифікувати на фізичні, інформаційні та змішані.

Норми, якими передбачено кримінально-правовий захист інформаційної критичної інфраструктури розміщено у окремому розділі КК України: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут КК України (ст. 361–1 КК України); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361–2 КК України); несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України); порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється (ст. 363 КК України); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (363–1 КК України).

Для загального визначення цих злочинів використовується поняття «комп'ютерні злочини» — суспільно небезпечні, протиправні, кримінально карані, винні діяння, які завдають шкоди інформаційним відносинам, засобом забезпечення нормального функціонування яких є ЕОМ, автоматизовані системи, комп'ютерні мережі або мережі електрозв'язку [12, с. 374].

Не зупиняючись на детальному аналізі складу цих злочинів, зазначимо, що так, як і у злочинах, що посягають на фізичну складову критичної інфраструктури, має значення спеціальна мета учинення злочину. Якщо така мета наявна, кримінально-правова кваліфікація відбуватиметься за сукупністю злочинів, одним з яких може бути диверсія (ст. 113 КК України).

У різний час було здійснено спроби законодавчого врегулювання питань кримінальної відповідальності за посягання на об'єкти критичної інформаційної інфраструктури. Так, у 2014 році було прийнято Закон України «Про внесення змін до Закону України «Про судоустрій і статус суддів» та процесуальних законів щодо додаткових заходів захисту безпеки громадян» (Закон втратив чинність на підставі Закону № 732-VII від 28.01.2014, ВВР, 2014, № 22, ст.811) [13]. Серед іншого було внесено такі зміни до КК України (наразі втратили чинність): Стаття 361–3. Несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури. У статтях 361–3 і 362–1 під критичним об'єктом національної інформаційної інфраструктури пропонувалось розуміти об'єкт, на якому наявна принаймні одна інформаційна (автоматизована), телекомунікаційна або інформаційно-телекомунікаційна система, порушення функціонування якої може призвести до: надзвичайної ситуації техногенного характеру; спричинити негативний вплив на стан екологічної безпеки держави; спричинити негативний вплив на стан енергетичної безпеки держави; спричинити негативний вплив на стан економічної безпеки держави, порушити стале функціонування банківської або фінансової системи держави; порушити стале функціонування транспортної інфраструктури держави; блокувати роботу або спричинити руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

та об'єктів підвищеної небезпеки; блокувати діяльність органів державної влади чи органів місцевого самоврядування; порушити стале функціонування інформаційної або телекомунікаційної інфраструктури держави, у тому числі її взаємодію з відповідними інфраструктурами інших держав; блокувати діяльність військових формувань, інших суб'єктів сектору національної безпеки та оборони, органів військового управління Збройних сил України, систем керування зброєю; призвести до масових заворушень; спричинити розголошення державної таємниці. Стаття 362–1. Несанкціоновані дії з інформацією, що обробляється в державних електронних інформаційних ресурсах або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах критичних об'єктів національної інформаційної інфраструктури, вчинені особою, яка має право доступу до такої інформації. Стаття 361–4. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, що обробляється в державних електронних інформаційних ресурсах.

На теперішній час у Верховній Раді України зареєстровано законопроекти, які передбачають посилення кримінальної відповідальності за злочини, що посягають на об'єкти критичної інформаційної інфраструктури: № 8304 проект Закону про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо розмежування підслідності злочинів, вчинених у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури, внесений Кабінетом Міністрів України та № 8304–1 проект Закону про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за злочини вчинені у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури, та відповідальності за пошкодження телекомунікаційних мереж.

Суть змін до КК України, згідно згаданих проектів, серед іншого, полягає у тому, що пропонується доповнити окремі статті розділу XVI КК України частинами, у яких передбачити кваліфікуючі ознаки злочинів, зокрема у разі вчинення їх стосовно об'єктів критичної інформаційної інфраструктури. Відтак, у разі ухвалення таких змін до КК України буде запроваджено новий термін «критична інформаційна інфраструктура» та посилено відповідальність за такі злочинні посягання.

Отже, ми проаналізували сучасний стан законодавчого регулювання підстав кримінальної відповідальності за злочини, що посягають на об'єкти критичної інфраструктури і підійшли до питання чи є достатнім і належним його існуючий рівень. Зважаючи на те, що наразі тільки відбувається формування спеціального законодавства, триває створення переліку об'єктів критичної інфраструктури, доцільно говорити про перспективи удосконалення КК України.

Такі удосконалення, на нашу думку, мають полягати у запровадженні окремої норми (норм), якою буде передбачено кримінальну відповідальність за посягання на об'єкти критичної інфраструктури. На теперішній час кримінально-правовою охороною охоплюється лише частина таких об'єктів. Звичайно, у кримінально-правовій нормі не доцільно передбачати увесь перелік об'єктів критичної інфраструктури, адже по-перше, він значний за обсягом, а по-друге, зміни і доповнення до цього переліку, які будуть вноситись за результатами його періодичного перегляду, потребуватимуть відповідних змін до КК України. Тому диспозиція правової норми очевидно матиме бланкетний характер. У чинному КК України відповідні норми розміщені у різних розділах КК, а отже мають різний родовий об'єкт, що не відповідає загальній концепції критичної інфраструктури. Отже, доповнення існуючих правових норм відповідними частинами з метою диференціації кримінальної відповідальності за такі злочини не вирішить зазначених проблем. Тому відповідну норму (норми) потрібно передбачити у розділі I Особливої частини КК «Злочини проти основ національної безпеки України».

Список використаної літератури

1. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р. — URL: http://zakon.rada.gov.ua/laws/show/1009–2017-%D1%80.

2. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: Постанова Кабінету Міністрів № 563 від 23 серпня 2106 року. — URL: http://zakon2.rada.gov.ua/laws/show/563–2016-%D0 %BF/paran17#n17.

3. Міністерство економічного розвитку і торгівлі України. Офіційний сайт. — URL: http://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=f6481532-9ec0-4ca5-9832-dcc32e31da3c&title=ProektZakonuUkrainiproKritichnuInfrastrukturuTaYiiZakhis.

4. Про національну безпеку України. Закон України. *Відомості Верховної Ради (ВВР)*. 2018. № 31. С. 241.

5. Кримінальний кодекс України. *Відомості Верховної Ради України (ВВР)*. 2001. № 25–26. С. 131.

6. Про затвердження переліку особливо важливих об'єктів електроенергетики, у тому числі територій забороненої зони та контрольованої зони гідротехнічних споруд, які підлягають охороні відомчою воєнізованою охороною: Постанова Кабінету Міністрів України № 575 від 4 липня 2018 року. URL: http://zakon.rada.gov.ua/laws/show/575–2018-%D0 %BF.

7. РБ ООН щойно ухвалила резолюцію 2341 щодо захисту критичної інфраструктури від терористичних атак, ініційовану Україною. Основні факти. *Permanent Mission of Ukraine to the United Nations*. — URL: https://twitter.com/UKRinUN/status/831161881113014272/photo/1.

8. Резолюція 2341: прийнята Радою Безпеки ООН від 13 лютого 2017 року. — URL: https://undocs.org/ru/S/RES/2341(2017).

9. Про транспорт: Закон України. *Відомості Верховної Ради України (ВВР)*. 1994. № 51. 446 с.

10. Про трубопровідний транспорт: Закону України. *Відомості Верховної Ради України (ВВР)*. 1996. № 29. 139 с.

11. Про приєднання України до Міжнародної конвенції про боротьбу з бомбовим тероризмом: Закон України. *Відомості Верховної Ради України (ВВР)*. 2002. № 10. 72 с. — URL: http://zakon.rada.gov.ua/laws/show/995_374.

12. Кримінальне право (Особлива частина): підручник / за ред. О. О. Дудорова, Є. О. Письменського. Т. 2. Луганськ : «Елтон-2». 2012. 780 с.

13. Про судоустрій і статус суддів та процесуальних законів щодо додаткових заходів захисту безпеки громадян: Закон України. *Відомості Верховної Ради (ВВР)*. 2014. № 22. 801 с. (Закон втратив чинність).

References

1. About the approval of the Concept for the development of a state system for the critical infrastructure protection. Order of the Cabinet of Ministers of Ukraine No. 1009-r dated 6 December 2017. Retrieved from http://zakon.rada.gov.ua/laws/show/1009–2017-%D1%80.

2. On approval of the Procedure for the formation of the list of information and telecommunication systems of critical infrastructure objects of the state. Resolution of the Cabinet of Ministers No. 563 dated 23 August 2016. Retrieved from http://zakon2.rada.gov.ua/laws/show/563–2016-%D0%BF/paran17#n17.

3. Ministry of Economic Development and Trade of Ukraine. Official site. Retrieved from http://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=f6481532-9ec0-4ca5-9832-dcc32e31da3c&title=ProektZakonuUkrainiproKritichnuInfrastrukturuTaYiiZakhis.

4. On National Security of Ukraine. Law of Ukraine. *Bulletin of the Verkhovna Rada of Ukraine*, 2018, No. 31, 241.

5. The Criminal Code of Ukraine. *Bulletin of the Verkhovna Rada of Ukraine*, 2001, No. 25–26, 131.

6. On approval of the list of especially important objects of power industry, including areas of the restricted zone and control area of hydraulic structures, which are subject to the protection of departmental paramilitary security services. Resolution of the Cabinet of Ministers of Ukraine No. 575 dated 4 July 2018. Retrieved from http://zakon.rada.gov.ua/laws/show/575–2018-%D0 %BF.

7. The UN Security Council has just adopted Resolution 2341 initiated by Ukraine on the protection of critical infrastructure against terrorist attacks. Basic facts. *Permanent Mission of Ukraine to the United Nations*. Retrieved from https://twitter.com/UKRinUN/status/831161881113014272/photo/1.

8. Resolution 2341 (2017) adopted by the Security Council on 13 February 2017. Retrieved from https://undocs.org/en/S/RES/2341(2017).

9. About transport. Law of Ukraine. *Bulletin of the Verkhovna Rada of Ukraine*, 1994, No. 51, 446.

10. About pipeline transport. Law of Ukraine. *Bulletin of the Verkhovna Rada of Ukraine*, 1996, No. 29, 139.

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

11. International Convention for the Suppression of Terrorist Bombings. New York, December 15, 1997. The Law of Ukraine "On Ukraine's Accession to the International Convention for the Suppression of Bombing Terrorism". *Bulletin of the Verkhovna Rada of Ukraine*, 2002, No. 10, 72. Retrieved from http://zakon.rada.gov.ua/laws/show/995_374.

12. *Dudorova, O.O., Pismensky, E.O.* (2012). "Criminal Law", Luhansk, Publishing House, Elton-2, 780 p.

13. On the Judicial System and Status of Judges and procedural laws on additional measures to protect citizens. Law of Ukraine. *Bulletin of the Verkhovna Rada of Ukraine*, 2014, No. 22, 801.

Проблеми кримінальної відповідальності за посягання на об'єкти критичної інфраструктури в ядерній енергетиці

Таран О. В.[1], Сандул О. Г.[2]

[1] Національна академія внутрішніх справ, м. Київ, Україна

[2] Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки» м. Київ, Україна

Наразі в Україні відбувається формування спеціального законодавства щодо кримінальної відповідальності за посягання на об'єкти критичної інфраструктури.

В цьому напрямку Кабінетом Міністрів України схвалена Концепція створення державної системи захисту критичної інфраструктури.

В даній роботі на загальному фоні захисту об'єктів критичної інфраструктури розглянуто цей напрямок законодавства стосовно об'єктів в галузі ядерної енергетики.

Докладно проаналізовано сучасний стан законодавчого регулювання підстав кримінальної відповідальності за злочинну діяльність, що посягає на об'єкти критичної інфраструктури ядерної енергетики. Обговорюється питання на предмет достатності та належності існуючого рівня такої відповідальності.

В роботі, як приклад, наведено перелік деяких основних об'єктів критичної інфраструктури у відповідності до нормативно-правових актів у сфері захисту критичної інфраструктури та надана їх класифікація.

Крім того, розглянуто такі поняття як «критична інфраструктура», що є відносно новим поняттям в національному законодавстві, «акт незаконного втручання», «комп'ютерні злочини», «критична інформаційна інфраструктура» та інші, що мають важливе значення для ядерної енергетики. Проведено аналіз понять, що містяться в різних нормативно-правових документах.

В роботі підкреслюється, що в законодавстві України наразі відсутні спеціальні (окремі) норми стосовно кримінальної відповідальності за посягання на об'єкти критичної інфраструктури. З цього приводу розглянуто також деякі перспективи розгляду цих питань. Особливо це стосується підстав кримінальної відповідальності, щодо захисту об'єктів критичної інфраструктури в галузі ядерної енергетики.

Обговорюється також питання перспективи щодо подальшого розроблення спеціального закону, яким буде визначено напрям розвитку відповідного законодавства про загальне врегулювання цих питань.

В статті також наголошено про необхідність внесення деяких змін до кримінального кодексу України стосовно доповнень до окремих статей розділу XIV.

Ключові слова: об'єкти критичної інфраструктури, нормативно-правові акти, ядерна енергетика

Issue of Criminal Liability for Offences Against Critical Infrastructure Objects in Nuclear Industry

Taran O[1]., Sandul O[2].

[1] National Academy of Internal Affairs, Kyiv, Ukraine

[2] State Enterprise "State Scientific and Technical Center for Nuclear and Radiation Safety", Kyiv, Ukraine

A special legislation on criminal liability for offences against critical infrastructure objects is currently under development in Ukraine. The Cabinet of Ministers of Ukraine adopted the Concept for the development of a state system for critical infrastructure protection.

The paper considers this legal area with regard to objects in the nuclear industry in the general context of critical infrastructure protection. It provides the current state in the legal regulation of fundamentals of criminal liability for offences against the critical infrastructure objects in the nuclear industry. The issue on the sufficiency and appropriateness of the existing level of such a liability is discussed further.

The paper presents the list of some main critical infrastructure objects in accordance with the regulatory documents in the sphere of critical infrastructure protection and their classification.

In addition, such concepts as "critical infrastructure" (relatively new notion in the national legislation), "unlawful intrusion", "computer crimes", "critical information infrastructure" and other concepts important to the nuclear industry were considered in this research. The notions presented in different regulatory documents were analyzed.

The paper emphasizes that the legislation of Ukraine does not currently present special (separate) standards on the criminal liability for offences against critical infrastructure objects. Some promising issues related to fundamentals of the criminal liability and protection of critical infrastructure objects in the nuclear industry were also considered.

The research involves the prospect of further development of a special law to define the area for improving relevant legislation on general regulation of these issues.

The paper also stresses on the need to introduce some changes to the Criminal Code of Ukraine with respect to certain articles of section XIV.

Keywords: critical infrastructure objects, regulatory documents, nuclear energy.

Отримано 12.04.2019