УПРАВЛІННЯ МОБІЛІЗАЦІЙНОЇ РОБОТИ, ЦИВІЛЬНОГО ЗАХИСТУ
ТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ МВС УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ № 2 НАВС

РОЗСЛІДУВАННЯ ПОСЯГАНЬ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Методичні рекомендації

Київ 2023

Авторський колектив:

Саковський А.А., д.ю.н., професор, директор ННІ № 2 НАВС, підполковник поліції; **Єфіменко І.М.,** к.ю.н., старший науковий співробітник ННІ № 2 НАВС, капітан поліції; **Хоруженко О.С.,** головний спеціаліст сектору критичної інфраструктури Управління мобілізаційної роботи, цивільного захисту та критичної інфраструктури МВС України; **Радзівон С.М.,** к.ю.н., доцент, доцент кафедри поліцейського права НАВС, підполковник поліції; **Патик А.А.,** к.ю.н., с.н.с., завідувач науково-дослідної лабораторії ННІ № 2 НАВС, підполковник поліції; **Білозьоров Є.В.,** к.ю.н., доцент, заступник директора ННІ № 2 НАВС, підполковник поліції.

Рецензенти:

Вознюк А.А., д.ю.н., професор, завідувач науково-дослідної лабораторії з проблем протидії злочинності ННІ № 2 НАВС, майор поліції;

Шаповалов О.О., к.ю.н., т.в.о. начальника управління документування злочинів учинених в умовах збройного конфлікту головного слідчого управління Національної поліції України, полковник поліції;

Глушак О.М., начальник управління мобілізаційної роботи, цивільного захисту та критичної інфраструктури МВС України.

Розслідування посягань на обєкти критичної інфраструктури : методичні рекомендації / [Саковський А.А., Єфіменко І.М., Хоруженко О.С., Радзівон С.М., Патик А.А., Білозьоров Є.В.]. Київ. НАВС, 2023. 73 с.

Рекомендовано до друку науково-методичною радою
Національної академії внутрішніх справ від 22.12.2023 (протокол №15)

У роботі здійсюється аналіз основних загроз та напрямків розвитку механізмів захисту критичної інфраструктури у частині, що стосується розкриття та розслідування кримінальних правопорушень, що посягають на обєкти критичної інфраструктури. Проводиться оцінка сучасного стану кримінально-правової охорони об'єктів критичної інфраструктури. Досліджується організація діяльності слідчо-оперативної групи при розслідуванні фізичних посягань на обєкти критичної інфраструктури, а також особливості проведення окремих процесуальних дій та експертних досліджень.

Під час підготовки рекомендацій враховувалися нормативно-правові акти, положення яких врегульовують питання національної системи захисту критичної інфраструктури як складової національної безпеки України. Також, бралися до уваги наукові розробки Національної академії внутрішніх справ, Національного інституту стратегічних досліджень з досліджуваної тематики.

Видання розраховане на учасників освітнього процесу закладів вищої юридичної освіти, а також практичних працівників державних органів до повноважень яких належить протидія правопорушенням, що посягають на обєкьти критичної інфраструктури та нагляду за додержанням законності у цій сфері діяльності.

ЗМІСТ

Вступ

Забезпечення безпеки критичної інфраструктури, є складним і довготривалим процесом який потребує організаційно-комплексного підходу. Він притаманний будь-якій цивілізованій країні, та не є виключенням для України, де в умовах повномасштабного російського вторгнення, ключовим пріоритетом державної політики є захист об'єктів критичної інфраструктури від злочинних посягань. До прикладу, за даними Офісу Генерального прокурора, із усіх зафіксованих ракетних ударів, понад 70% були скоординовані саме по критично важливим сферам діяльності держави. За цими фактами, лише Національною поліцією України, було відкрито понад вісімдесят тисяч кримінальних проваджень, у тому числі, передбачених ст. 438 КК України (Порушення законів та звичаїв війни).

Водночас, аналіз науково літератури з правової тематики свідчить про те, що дослідження проблемних аспектів досудового розслідування кримінальних правопорушень, що посягають на обєкти критичної інфраструктури порівняно є новими. Здебільшого вони стосуються питань забезпечення кібербезпеки на критично важливих об'єктах енергетичної галузі.

Поряд з цим, фізичні загрози є не менш небезпечними. До них, можливо віднести ті потенційні небезпеки, які зумовили виникнення на об'єкті критичної інфраструктури кризової ситуації, що загрожує життю і здоров'ю персоналу цього об'єкта та/або місцевому населенню в зоні проживання якого він розташований, а також безпеці інших громадян та/або їх матеріальному становищу.

Оцінюючи фізичні ризики на об'єктах критичної інфраструктури, вони можуть проявлятися у формі диверсій, терористичних актів, викрадення, навмисного знищення та/або пошкодження майна необхідного для їх функціонування тощо. Вкрай важливим є те, що реалізація цих злочинних діянь, на відміну від кібер-деліктів, може спричинити загибель великої кількості людей, заподіяти фізичні чи моральні страждання, завдати значну матеріальну шкоду, нанести непоправиму шкоду довкіллю, що унеможливлює проживання людей на певній території та в кінцевому результаті створює загрозу подальшому існуванню людства.

Незважаючи на актуальність і велику практичну значущість цієї тематики, у відомчих нормативно-правових актах не визначено практичних рекомендацій щодо алгоритму орієнтовних дій уповноважених органів під час реагування на заяви і повідомлення про кримінальні правопорушення вчинені на об'єктах критичної інфраструктури та особливостей методики

розслідування зазначеної категорії деліктів, що зумовила вибір теми методичних рекомендацій.

§ 1. Основні загрози та напрямки розвитку механізмів захисту критичної інфраструктури

Критична інфраструктура складається із об'єктів, систем та їх частин, які забезпечують в державі життєво важливі функції та/або послуги, порушення режиму роботи яких негативно впливає на національну безпеку і оборону країни. До таких функцій та/або послуг національним законодавством були віднесені:

(1) *урядування та надання найважливіших (адміністративних) послуг*. Ця категорія пов'язана з реалізацією владних повноважень. Суб'єктами надання таких послух є органи державної влади (здебільш виконавчої), органи місцевого самоврядування, суб'єкти державної реєстрації уповноважені відповідно до закону надавати адміністративні послуги тощо;

(2) *енергозабезпечення (у тому числі постачання теплової енергії)*. Цей сектор включає такі підсистеми як електроенергетика, нафтова промисловість, газова промисловість та ядерна енергетика, що складаються із сукупності підприємств, установ і організації по виробництву (видобутку і переробки) матеріальних об'єктів, в яких зосереджена енергія придатна для практичного використання людиною;

(3) *водопостачання та водовідведення*. Ця категорія включає системи з виробництва питної та технічної води, а також її водопостачання та водовідведення. До її складу входять підприємства, установи та організації, які здійснюють обслуговування та функціонування систем водообігу;

(4) *продовольче забезпечення*. Ця категорія є важливою складовою загальноекономічної безпеки будь-якої країни. Стан продовольчої безпеки визначає рівень життєзабезпечення населення, його добробут та соціально-економічний розвиток. Вона охоплює системи з вирощування, обробки, виготовлення, пакування, зберігання та поширення (постачання) продуктів рослинного, тваринного, мінерального, синтетичного чи біотехнологічного походження, що використовується для виробництва харчових продуктів;

(5) *охорона здоров'я*. Цей сектор складається із державних та приватних, національних та регіональних (місцевих) закладів охорони здоров'я, лікарень, у тому числі військово-медичних закладів, центрів сімейної медицини, інших медичних установ, оздоровчих комплексів,

психоневрологічних та наркологічних диспансерів, будинків для пристарілих, санітарно-епідеміологічних служб, донорських установ для збору крові, медичних лабораторій, моргів тощо;

(6) *фармацевтична промисловість*. Ця категорія є складовою хімічної промисловість, що пов'язана з дослідженням, розробкою, масовим виробництвом лікарських засобів та виробів медичного призначення переважно для профілактики, полегшення і лікування хворих;

(7) *виготовлення вакцин, стале функціонування біолабораторій*. Вакциною є біологічний лікарський засіб, який застосовуються в медичній практиці з метою специфічної профілактики інфекційних захворювань. Виготовлення вакцин – це результатом складного та тривалого виробничого процесу, що передбачає контроль на віх його етапах. До стадій виробництва вакцин відносять дослідницький етап (розробка вакцин), доклінічні дослідження вакцини-кандидата, клінічні дослідження вакцини-кандидата, розгляд матеріалів на вакцину в Національному регулятивному органі з метою її реєстрації та затвердження нормативних документів, виробництво вакцини, ап також контроль за якістю та застосуванням вакцини в період її масового використання.

(8) *інформаційні послуги*. Ця категорія є об'єктом цивільних правовідносин. Вона направлена на здійснення інформаційної діяльності у визначений законом час і формі з доведення інформаційної продукції до кінцевих споживачів для задоволення інформаційних потреб. Цей сектор також включає ІТ-сферу (інформаційно-телекомунікаційні технології), що охоплюється віртуальними функціями з реалізації ІТ-продуктів і послуг. Важливого значення під час функціонування інформаційно-телекомунікаційні технології набувають служби, які обслуговують спеціальне обладнання і програмне забезпечення ІТ-систем та забезпечують кіберзахист від несанкціонованого втручання в їх роботу;

(9) *електронні комунікації*. Ця системи включають електронно комунікаційні мережі, що складаються із комплексу технічних засобів електронних комунікацій та споруд, призначених для надання електронно комунікаційних послуг, що полягають в прийманні та/або передачі інформації через електронні комунікаційні мережі.

(10) *фінансові послуги*. Фінансовими послугами є операції з фінансовими активами, що здійснюється в інтересах третіх осіб за

власний рахунок чи за рахунок цих осіб, а у випадку, передбачених законодавством – за рахунок залучених від інших осіб фінансових активів, з метою отримання прибутку або збереження реальної вартості фінансових активів. Ця категорія охоплює фінансові установи, тобто, юридичні особи, які надають одну чи декілька фінансових послуг, а також інших послуг (операцій), пов'язаних з наданням фінансових послуг, у випадках визначених законом, та за умов внесення таких установ в установленому законом порядку до відповідного реєстру;

(11) *транспортне забезпечення*. Ця категорія включає транспортні системи, що охоплюються усіма засобами перевозки (авіація, морські шляхи, автомобільні дороги, залізниця, магістральний трубопровідний транспорт), з метою переміщення пасажирів, товарів та послуг. Об'єктами цієї категорії є мережеві системи до якої входять вокзали, аеропорти, морські та річкові порти, вантажні причали, автомобільні шляхи, фарватери, повітряні коридори тощо, а також сукупність служб та технічних засобів та обладнання, що обслуговують та забезпечують їх функціонування тощо;

(12) *оборона, державна безпека*. Ця категорія включає два споріднених сектора. Обороною країни складається із системи політичних, економічних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів держави щодо підготовки до збройного захисту та її захисту у разі збройної агресії або збройного конфлікту.

У свою чергу, державна безпека полягає у захисті державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних чи потенційних загроз невоєнного характеру.

(13) *правопорядок, здійснення правосуддя, тримання під вартою*. Ця категорія включає органи і установи, що забезпечують в державні правопорядок, правосуддя та виконання покарань;

(14) *цивільний захист населення та територій, служби порятунку*. Ця категорія включає сили цивільного захисту, які забезпечують виконання заходів, що реалізуються на території України в мирний час та в особливий період і спрямовані на захист населення, територій, навколишнього природнього середовища, майна, матеріальних і культурних цінностей від надзвичайних ситуацій та інших небезпечних подій, запобігання виникненню таких ситуацій та подій, ліквідацію їх наслідків, надання допомоги постраждалим,

здійснення державного нагляду (контролю) у сфері пожежної та технічної безпеки;

(15) *космічна діяльність, космічні технології та послуги*. До об'єктів космічної діяльності відносяться матеріальні предмети штучного походження, що проєктуються, виготовляються та експлуатуються як у космічному просторі, так і на поверхні Землі з метою дослідження та використання космічного простору. У свою чергу, космічними технологіями та послугами є результати діяльності відповідних наукових установ (конструкторських бюро) та пов'язаних з ними виробництв;

(16) *хімічна промисловість*. Ця категорія виробляє продукцію з вуглеводневої, мінеральної та іншої сировини шляхом її хімічної переробки. Як галузь виробництва, вона відноситься до важкої промисловості;

(17) *дослідницька діяльність*. Об'єктами критичної інфраструктури цієї категорії є наукових установ та закладів вищої освіти, їх структурні підрозділи (університети, академії, інститути тощо), сукупність засобів, ресурсів та пов'язаних з ними послуг, які використовуються науково-педагогічними співробітниками для проведення досліджень, об'єкти наукових устаткувань, обладнання, набори приладів, ресурси, що базуються на знаннях (колекції, архіви, депозитарії та банки даних архівної інформації) тощо.

Дослідницька інфраструктура може бути локально розташованою, віртуальною або розподіленою, державною або приватною. Вона може також мати міжнародний характер та входити до міжнародних мереж.

Формування та реалізація державної політики у сфері захисту критичної інфраструктури здійснюється уповноваженими суб'єктами національної системи захисту критичної інфраструктури. До цих суб'єктів відносяться Кабінет Міністрів України, Апарат Ради національної безпеки і оборони України, Центральна виборча комісія, Національний банк України, Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національна комісія, що здійснює регулювання у сфері енергетики та комунальних послуг, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Фонд Державного майна України, інші центральні органи державні влади із спеціальним статусом, Уповноважений орган у сфері захисту критичної інфраструктури України (ДЗКІ),

Центральний орган виконавчої влади, який забезпечує формування та реалізацію державної політики у сфері цивільного захисту, секторальні та функціональні органи, інші міністерства та центральні органи виконавчої влади, СБУ, правоохоронні та розвідувальні органи, суб'єкти оперативно-розшукової та контррозвідувальної діяльності, Збройні Сили України, інші військові формування, утворені відповідно до законів України, місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення), органи місцевого самоврядування, оператори критичної інфраструктури, підприємства, установи та організації незалежно від форм власності, які проводять діяльність, пов'язану із забезпеченням безпеки та стійкості критичної інфраструктури (див. рис. 1)

Особливе місце серед зазначених суб'єктів займають секторальні та функціональні органи у сфері захисту критичної інфраструктури. Для організації ефективного забезпечення безпеки та стійкості критичної інфраструктури, з урахуванням специфіки забезпечення окремих життєво важливих функцій та/або послуг, секторальними органами у сфері захисту критичної інфраструктури, визначаються сектори критичної інфраструктури у яких, ведеться секторальний перелік об'єктів критичної інфраструктури. У цьому переліку містяться як матеріальні, так й нематеріальні активи порушення режиму роботи яких негативно впливає на функціонування органів державної влади та місцевого самоврядування на державному, регіональному, місцевому чи об'єктовому рівнях.

Під час ідентифікації об'єктів критичної інфраструктури враховується сукупність критеріїв, що визначають їх соціальну, політичну, економічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку. До таких характеристик відносяться:

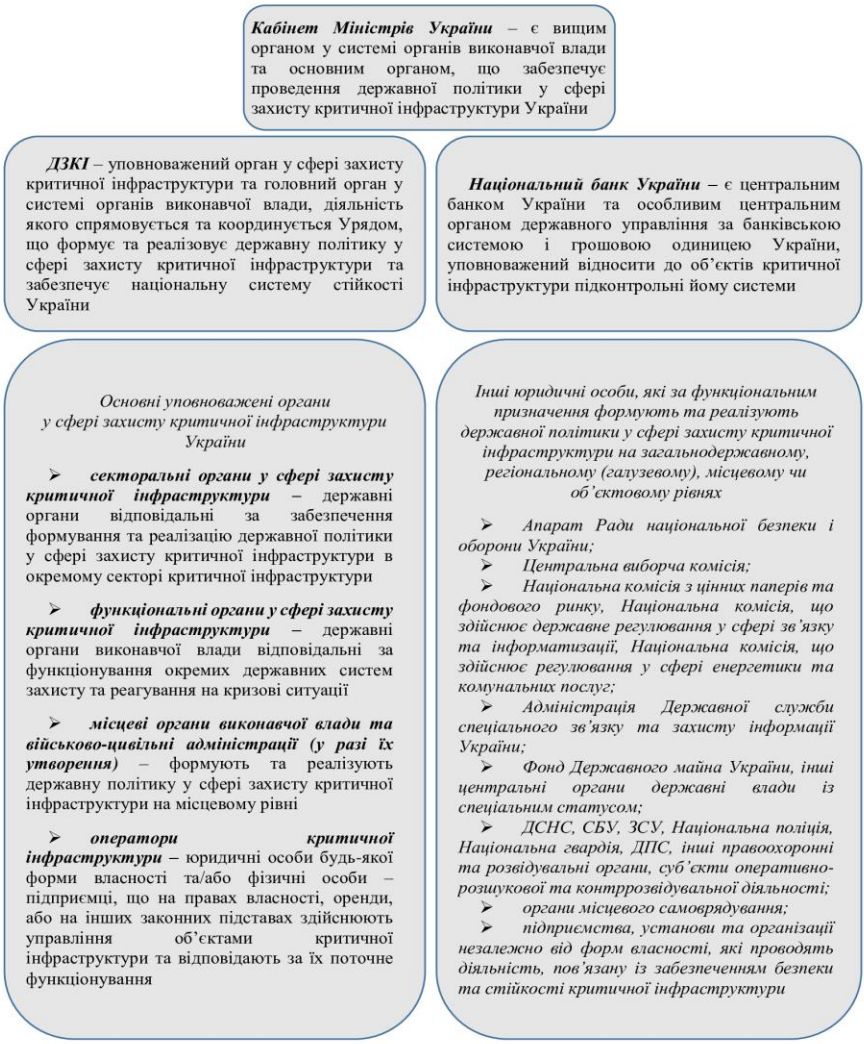
(1) *масштаб заподіяної шкоди* (територіальне поширення наслідків можливої шкоди);

(2) *взаємозв'язок між елементами критичної інфраструктури* (поширення заподіяної шкоди на інші об'єкти чи сектори критичної інфраструктури);

(3) *тривалість та характер впливу заподіяної шкоди* (як саме і на який час проявлятимуться негативні наслідки заподіяної шкоди у разі порушенням штатного функціонування об'єкту критичної інфраструктури);

Рисунок 1.

На рисунку схематично зображені суб'єкти національної системи захисту критичної інфраструктури



(г) *вразливість об'єкту критичної інфраструктури до* пандемій, промислових аварій, терористичних актів, кібератак, стихійних лих та інших прогнозованих і непередбачуваних загроз;

(г) *ступень тяжкості, у тому числі, розмір заподіяних збитків та негативних наслідків, що можуть бути спричинені* економічній безпеці, соціальній (громадській) безпеці, внутрішньополітичній безпеці, екологічній безпеці та державній безпеці.

Основні загрози безпеки критичної інфраструктури поділяються на п'ять категорій, а саме:

(1) *техногенного характеру* (аварії, катастрофи та інциденти на об'єктах критичної інфраструктури, що спричинили людські жертви, матеріальні збитків, негативний вплив на навколишнє середовище тощо);

(2) *природнього характеру* (спричинені метеорологічними, гідрологічними, геологічними та геліофізичними (пожежі) факторами);

(3) *соціального характеру* (спричинені протиправною діяльність окремих осіб та/або відповідних злочинних груп чи угруповань з метою порушення штатного функціонування об'єкта критичної інфраструктури);

(4) *воєнного характеру* (спричинені воєнними діями, що призвело до руйнування об'єкта критичної інфраструктури або порушило його штатне функціонування);

(5) *комбінованого характеру* (спричинені дією каскадного ефекту, коли руйнування одного із об'єктів критичної інфраструктури порушило штатне функціонування інших систем життєзабезпечення).

За територіальним поширенням загрози безпеці критичної інфраструктури прийнято класифікувати на надзвичайні ситуації державного, регіонального, місцевого та/або об'єктового рівнів (див. рис. 2).

Для ефективної протидії цим загрозам:

(а) *на державному рівні* розробляється національний план захисту і забезпечення безпеки та стійкості критичної інфраструктури, який затверджується Кабінетом Міністрів України;

(б) *на секторальному та регіональному рівнях* органи державної влади розробляють та затверджують галузеві, регіональні плани та програми з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії

суб'єктів національної системи захисту критичної інфраструктури, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії суб'єктів національної системи захисту критичної інфраструктури, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань та тренувань тощо;

Рисунок 2.

На рисунку схематично зображена класифікація надзвичайних ситуацій за територіальним поширенням

(в) *на місцевому рівні*, місцеві органи виконавчої влади (військово-

цивільні адміністрації – у разі їх утворення), органи місцевого самоврядування забезпечують розроблення, затвердження і виконання місцевих програм підвищення стійкості територіальних громад до кризових ситуацій. Такі програми включають заходи із забезпечення безпеки та стійкості критичної інфраструктури, взаємодії суб'єктів національної системи захисту критичної інфраструктури, а також відновлення функціонування об'єктів критичної інфраструктури;

(г) *на об'єктовому рівні* розробляються та затверджуються об'єктові плани заходів операторів критичної інфраструктури на кожному окремому об'єкті критичної інфраструктури з метою здійснення його захисту від реальних чи потенційних небезпек. Виконання та реалізація зазначених планів є обов'язковою для усіх суб'єктів захисту критичної інфраструктури.

З метою проведення оцінки стану захищеності об'єктів критичної інфраструктури секторальними та функціональними органами у сфері захисту критичної інфраструктури проводиться моніторинг рівня безпеки об'єктів критичної інфраструктури. Під час здійснення цього моніторингу

по-перше, визначається відповідність стану захищеності об'єкта критичної інфраструктури вимогам законодавства,

по-друге, встановлюється достовірність наданої інформації відповідними суб'єктами національної системи захисту критичної інфраструктури,

по-третє, надається методична допомога операторам об'єктів критичної інфраструктури щодо удосконалення системи захисту критичної інфраструктури.

За результатами проведення моніторингу секторальними та функціональними органами готується звіт про оцінку стану захищеності інспектованих об'єктів критичної інфраструктури та надаються пропозиції щодо удосконалення систем їхнього захисту. Ці відомості та/або дані відносяться до інформацією з обмеженим доступом.

Окреме місце у процесі реалізації безпекових заходів займає взаємодія суб'єктів національної системи захисту критичної інфраструктури з іншими системами захисту у сфері національної безпеки. До цих систем національним законодавством було віднесено: єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків; національну систему

захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах; національну систему кібербезпеки; систему правоохоронних органів, уповноважених здійснювати боротьбу з кримінальними правопорушеннями, а також контррозвідувальні та розвідувальні органи у сфері забезпечення державної безпеки; об'єднану цивільно-військову систему організації повітряного руху України; єдину державну систему цивільного захисту України; державну систему фізичного захисту з питань охорони і оборони важливих державних об'єктів, захищеності та охорони ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання державної власності, запобігання диверсіям, крадіжкам або будь-якому іншому неправомірному вилученню радіоактивних матеріалів та протидії незаконному використанню БпЛА; систему захисту персональних даних.

Окреме місце у системі захисту критичної інфраструктури відведено взаємодії державних органів, які відповідно до Закону України «Про національну безпеку України», входять до структури сектору безпеки і оборони. До основних повноважень цих органів законодавством було віднесено протидію та припинення на об'єктах критичної інфраструктури противоправної діяльності. Реалізація спільних завдань здійснюється шляхом:

(а) оперативного обміну інформацією щодо виконання безпекових заході на об'єктах критичної інфраструктури;

(б) проведення спільних керівництва уповноважених органів у сфері захисту критичної інфраструктури України, центральних та територіальних органів полії, Національна гвардія України, СБУ, Збройних Сил України, Державної служби України з надзвичайних ситуацій та інших державних органів з правоохоронними чи спеціальними функціями;

(в) проведення спільних заходів щодо захисту критичної інфраструктури за планами, які розробляються на відповідному рівні управління та реагування;

(г) проведення спільних командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять із захисту, охорони, оборони, припинення кримінальних правопорушень, інцидентів та кібератак проти об'єктів критичної інфраструктури;

(ґ) регулярного уточнення розрахунків сил та засобів, що залучаються до спільного виконання завдань із захисту об'єктів критичної інфраструктури;

(д) проведення спільних заходів з припинення протиправних дій проти об'єктів критичної інфраструктури, порушення режиму роботи яких загрожує безпеці громадян;

(е) прийняття участі у реагуванні та ліквідації наслідків кризових ситуаціях на об'єктах критичної інфраструктури;

(є) координації дій з підтримання або відновлення правопорядку в місцях розташування об'єктів критичної інфраструктури у разі виникнення кризових ситуацій тощо.

До основних проблем захисту критичної інфраструктури відносять:

(1) *значущість кожного із секторів критичної інфраструктури*. Об'єкти критичної інфраструктури є взаємопов'язаними та взаємозалежними один від одного, а це означає, що від належного функціонування одного із секторів критичної інфраструктури залежить робота іншого взаємопов'язаного з ним сектору;

(2) *управляння безпекою відбувається за умов взаємозалежності діяльності урядових органів, державних та приватних структур, а також регулюючих та економічних чинник*ів. Безпека об'єктів критичної інфраструктури є комплексною категорією, яка залежить не лише від внутрішніх факторів, що забезпечуються державою, а й від інших чинників внутрішнього чи зовнішнього походження, які впливають на функціонування об'єктів критичної інфраструктури;

(3) *неефективна комунікація між суб'єктами захисту критичної інфраструктури*. Державні органи є здебільш вертикально орієнтованими структурами, які переважно накопичують інформацію. Натомість, критична інфраструктура розосереджена по всій території країни значною кількістю та сукупністю державних і приватних суб'єктів, що негативно впливає на своєчасний обмін інформацією між ними;

(4) *неефективний розподіл повноважень із захисту критичної інфраструктури між центральними та місцевими органами державної влади*. Проблема полягає у недосконалості чинного законодавства щодо визначення конкретних функцій кожного із суб'єктів захисту критичної інфраструктури, залежно від рівня управління національної системи захисту критичної інфраструктури;

(5) *відсутність загальної методичної бази для визначення ризиків та властивостей об'єктів критичної інфраструктури*. Вирішення цієї проблеми потребує проведення аналітично-методичних заходів із чіткого формування реєстру об'єктів критичної інфраструктури, визначення існуючих чи/або можливих (потенційних) ризиків та загроз, які впливають на штатне функціонування об'єктів критичної інфраструктури, а також шляхів забезпечення їх захисту на кожному із рівнів функціонування національної системи захисту критичної інфраструктури;

(6) *недостатня участь операторів (власників) критичної інфраструктури у забезпеченні її захисту*. Саме на операторів покладені обов'язки щодо віднесення об'єкта до критичної інфраструктури, тобто його ідентифікації. Ця стадіє є початковою у процесі захисту об'єктів критичної інфраструктури та дозволяє у подальшому провести необхідну його реєстрацію, категоризацію та паспортизацію. З огляду на це, ідентифікація об'єкта критичної інфраструктури відноситься до основного етапу, який впливає на загальний механізм захисту критично важливих сфер діяльності держави та дозволяє систематизувати сукупність елементів критичної інфраструктури і визначити її основні сектори, з метою забезпечення подальшого їх захисту.

Серед ключових напрямки розвитку механізмів захисту критичної інфраструктури розрізняють:

(1) *пасивний захист* (удосконалення нормативно-правових та організаційних механізмів захисту критичної інфраструктури; визначення пріоритетних секторів критичної інфраструктури та органів державної влади, які відповідають за формування та реалізацію державної політики щодо захисту критичної інфраструктури; розроблення та затвердження сучасних критеріїв та методик віднесення об'єктів до критичної інфраструктури (їх ідентифікації); удосконалення системи моніторингу стану захищеності об'єктів критичної інфраструктури, аналізу та прогнозування наявних чи потенційних загроз, визначення шляхів та способів зменшення їх ризиків та унеможливлення виникнення на них надзвичайних ситуацій; розроблення та впровадження стандартів, правил, технічних умов захисту об'єктів критичної інфраструктури; розвиток міжнародного співробітництва з питань захисту критичної інфраструктури; *чітке визначення видів і форм юридичної*

відповідальності за порушення вимог законодавства щодо захисту критичної інфраструктури).

(2) *активний захист* (удосконалення механізмів державно-приватного партнерства із забезпечення безпеки та стійкості критичної інфраструктури; впровадження інноваційних розробок та удосконалення існуючих засобів забезпечення безпеки та стійкості критичної інфраструктури; удосконалення систем та режимів охорони об'єктів критичної інфраструктури; *удосконалення механізмів боротьби з кримінальними правопорушеннями, що посягають на об'єкти критичної інфраструктури;* залучення експертів, громадськості, передових досягнень у забезпечення захисту та безпеки критичної інфраструктури, а також у підготовки кваліфікованих спеціалістів у цій сфері; усунення існуючих загроз шляхом застосування комплексних безпекових заходів; удосконалення системи взаємодії суб'єктів захисту критичної інфраструктури, врегулювання порядку обміну інформацією, збору даних про об'єкти критичної інфраструктури, а також загроз та ризиків пов'язаних з функціонуванням об'єктів критичної інфраструктури; підтримка національного виробника з безпекових послуг; утворення та підтримка функціонування відповідних консультаційних, дорадчих груп з питань захисту критичної інфраструктури; сприяння активній участі операторів критичної інфраструктури у забезпеченні захисту та стійкості критичної інфраструктури; створення єдиної державної системи виявлення і попереджання кібератак на об'єкти критичної інфраструктури).

§ 2. Критична інфраструктура як предмет кримінального правопорушення

Кримінальні правопорушення які посягають на об'єкти критичної інфраструктури умовно можна поділити, на ті, що по-перше, безпосередньо направлені на знищення або пошкодження об'єктів критичної інфраструктури. Тобто, коли винний свідомо вчиняє акт направлений на порушення штатного функціонування об'єктів життєзабезпечення, що є його основною метою. Мотиви у цьому випадку можуть бути різними та на кваліфікацію суспільно небезпечного діяння не впливають. Та по-друге, ті де порушення штатного функціонування об'єктів критичної інфраструктури для

винного не є самоціллю, а засобом досягнення іншої мети, що може перебувати або не перебувати у прямому зв'язку з цими діяннями. До прикладу, якщо взяти до уваги такий склад кримінального правопорушення як диверсія (ст. 114 КК України), то предметом його посягання можуть бути конкретні об'єкти критичної інфраструктури, які забезпечують безпеку та захист держави в економічній, екологічній, воєнній, політичній або будь-якій іншій сфері, незаконне втручання в яку сприяє ослабленню держави. Цими об'єктами можуть бути електростанції, водо-, нафто- та газопроводи, мости, дамби, греблі, водойми, інформаційно-телекомунікаційні системи, вокзали, аеропорти, морські чи річкові порти, а також інші суб'єкти господарювання, незалежно від форм власності, що виробляють чи надають життєво важливі для держави та її населення функції та/або послуги, порушення режиму роботи яких може призвести до непередбачуваних наслідків для національної безпеки, оборони країни та добробуту її громадян. Ураховуючи це, обов'язковою ознакою об'єктивної сторони кримінальних правопорушень об'єктами яких є критична інфраструктура є наявність причинно-наслідкового зв'язку між протиправними діяннями та суспільно небезпечними наслідками.

Залежно від значимості об'єкта, характер спричинених наслідків може мати об'єктовий, місцевий, регіональний (галузевий), державний, а іноді міжнародний рівень небезпеки. До таких об'єктів відносяться підприємства, установи та організації, які забезпечують функціонування та розвиток харчової, хімічної, ядерної промисловості, оборонно-промислового комплексу, фінансового сектору, цивільного захисту населення тощо.

Основними факторами, які впливають на кваліфікацію кримінальних правопорушень, що посягають на штатне функціонування об'єктів критичної інфраструктури є категорія їх критичності, масштаб та характер заподіяних суспільно небезпечних наслідків, кількість задіяних сил та засобів у їх ліквідації, організованість учасників кримінального правопорушення, способи його вчинення, а також мета та мотиви, що спонукали винного (винних) до реалізації протиправних дій.

Кримінальні правопорушення проти безпеки критичної інфраструктури здебільшого мають змішаний або банкетний характер, який відсилає нас до інших нормативно-правових актів, що визначають найбільш важливі для держави та її суспільства об'єкти

інфраструктури, порядок їх ідентифікації, реєстрації, категоризації та паспортизації, а також правила щодо їх експлуатації, захисту та безпеки. Відповідно до Закону України «Про критичну інфраструктуру», перелік цих об'єктів повинен міститись у відповідному автоматизованому реєстрі, формування та ведення якого покладено на уповноважений центральний орган державної влади у сфері захисту критичної інфраструктури (ДЗКІ). Складність цього питання полягає у тому, що до сьогодні в Україні ще не сформований зазначений орган та реєстр.

Не дають відповідей з цього питання й норми закону України про кримінальну відповідальність. Незважаючи на те, що КК України не визначає такого родового об'єкту кримінальних правопорушень як «безпека критичної інфраструктури», близьке за значенням поняття міститься у диспозиціях передбачених статтями 259 (Завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження власності) та 360 КК України (Умисне пошкодження або руйнування телекомунікаційних мереж). Зокрема, частиною 2 статті 259 до кваліфікаційних ознак цього кримінального правопорушення, було віднесено якщо його предметом є «критично важливі об'єкти інфраструктури». Аналогічний термін вживається й у примітці до статті 360 КК України, поєднуючись, з такою оціночною категорію як «тяжкі наслідки». Тобто, наслідки, що спричинили припинення надання телекомунікаційних послуг на критично важливих об'єктах інфраструктури.

Натомість критична інфраструктура може виступати об'єктом, предметом або місцем вчиненні й інших кримінальних правопорушень. Враховуючи особливу значимість для функціонування держави окремих секторів критичної інфраструктури, законодавцем були відокремлені спеціальні види кримінальних правопорушень щодо знищення чи пошкодження майна. Маються на увазі, ті самостійні склади кримінальних правопорушень, об'єктивна сторона яких, характеризується вчиненням суспільно небезпечного діяння, що полягає у знищенні чи пошкодженні окремо визначених об'єктів критичної інфраструктури. До цих об'єктів були віднесені підприємства, установи, організації їх системи та структуровані елементи, що забезпечують діяльність електроенергетичної галузі, природньо-заповідного фонду, житлово-комунального господарства,

ядерної енергетики, транспортних комунікацій, оборонно-промислового комплексу тощо. Власне до них відносяться:

(1) *статті 113 (Диверсія)* щодо об'єктів критичної інфраструктури, які забезпечують безпеку та захист держави в економічній, екологічній, воєнній, політичній або будь-якій іншій сфері відповідно до спрямованості конкретного акту диверсії, головною (спеціальною) метою якої є ослаблення держави. Предметом диверсії можуть бути будівлі, споруди та інші об'єкти критичної інфраструктури, які мають життєво важливе значення для функціонування основних напрямків діяльності держави. Тобто, електростанції, водо-, нафто- та газопроводи, мости, дамби, греблі, водойми, інформаційно-телекомунікаційні системи, вокзали, аеропорти, морські чи річкові порти, військові частини, банкнотно-монетні підприємства, підприємства хімічної та/або металургійної промисловості, а також інші підприємства, установи і організації, незалежно від форм власності, що виробляють чи/або надають життєво важливі для держави та її суспільства товари і послуги;

(2) *статті 194-1 (Умисне пошкодження об'єктів електроенергетики)* щодо об'єктів електроенергетичної галузі держави. Предметом цього кримінального правопорушення можуть бути електроенергетичні підприємства. Зокрема, електричні станції (окрім АЕС), електричні підстанції, електромережі, що підключені до об'єднаної електроенергетичної системи України, а також сукупність інших будівель, споруд та спеціальних технічних засобів, що забезпечують функціонування об'єктів електроенергетики. Основна відмінність цього складу кримінального правопорушення від диверсії полягає у тому, що у його внутрішній (суб'єктивній) стороні, відсутня спеціальна мета, що полягає в ослабленні держави. У той же час, законодавець цією нормою наголошує на особливому значенні захисту об'єктів критично інфраструктури в електроенергетичній сфері чим відмежовує цей склад кримінального правопорушення від умисного знищення або пошкодження майна (ст. 194 КК України);

(3) *статті 252 (Умисне знищення або пошкодження територій, взятих під охорону держави та об'єктів природно-заповідного фонду),* щодо об'єктив, які мають особливу природоохоронну, наукову, естетичну, рекреаційну та іншу цінність.

Безпосереднім об'єктом цього складу кримінального правопорушення можуть бути об'єкти критичної інфраструктури, які

знаходяться під охороною держави та мають особливий екологічний статус. До останніх національне законодавство відносить об'єкти природньо-заповідного фонду (природні та біосферні заповідники, національні природні парки, регіональні ландшафтні парки, пам'ятки природи тощо) та території, взяті під охорону держави (цінні водойми, природні комплекси боліт та лісів тощо, що становлять національне надбання та мають історико-географічну цінність);

(4) *статті 261 (Напад на об'єкти, на яких є предмети, що становлять підвищену небезпеку для оточення)* щодо об'єктив, порушення функціонування яких може викликати загрозу громадській безпеці та безпеці навколишньому середовищу. Об'єктами підвищеної небезпеки є виробництва, сховища, транспортні засоби, наукові установи та інші об'єкти, на яких виготовляються, зберігаються, використовуються та транспортуються радіоактивні, хімічні, біологічні та вибухонебезпечні матеріали, речовини, предмети тощо. У більшості випадків ці об'єкти входять до системи критичної інфраструктури, оскільки від їхнього функціонування залежить економічна, екологічна і соціальна безпека держави та її населення;

(5) *статті 270-1 (Умисне знищення або пошкодження об'єктів житлово-комунального господарства)* щодо об'єктив житлово-комунальної галузі, які забезпечують благоустрій територій і життєдіяльність населених пунктів та суттєво впливають на розвиток різноманітних взаємовідносин в державі. Предметом цього складу кримінального правопорушення є житлово-комунальне господарство, яке складається із сукупності та/або комплексу виробничої і невиробничої інфраструктури, що переважно знаходиться у власності територіальних громад та безпосередньо – у сфері управління органів місцевого самоврядування. Тобто, об'єкти благоустрою, теплопостачання, водопостачання та водовідведення, їх мережі та складові;

(6) *статті 273 (Порушення правил безпеки на вибухонебезпечних підприємствах або у вибухонебезпечних цехах)* щодо окремих об'єктів виробничої галузі, де виробляються вибухонебезпечні речовини, порох і боєприпаси, а також деяких інших підприємств де здійснюється термічне сушіння та подрібнювальні і пресувальні процеси. Місцем вчинення цього діяння можуть бути об'єкти критичної інфраструктури, які входять до системи об'єктів підвищеної небезпеки, на діяльність яких ці правила поширюються;

(7) *статті 274 (Порушення правил ядерної або радіаційної безпеки)* щодо об'єктів, на яких установлена ядерна або радіаційна безпека. Як і в попередньому складі кримінального правопорушення порушення правил безпеки характеризується причинно-наслідковим зв'язком, а також конкретним місцем вчинення кримінального правопорушення. До цих об'єктів відносяться виробничі підприємства, де використовуються ядерні або радіоактивні матеріали (АЕС, експериментальні і дослідні ядерні реактори, сховища радіоактивних відходів тощо).

Поняття ядерних і радіоактивних матеріалів, їх видів, класифікації, а також правил безпеки та поводження з ними, врегульовані окремими національними та міжнародними нормативно-правовими актами. Зокрема, Законом України «Про використання ядерної енергії та радіаційну безпеку», Угодою про Асоціацію між Україною з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами з іншої, Правилами забезпечення збереження ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання, Міжнародною Конвенцією про ядерну безпеку, тощо;

(8) *статті 279 (Блокування транспортних комунікацій, а також захоплення транспортного підприємства)* щодо окремих об'єктив транспортної галузі. Основним безпосереднім об'єктом цього кримінального правопорушення, є безпека функціонування та експлуатації транспортної системи України. З огляду на це, предметом цього складу кримінального правопорушення є транспортні комунікації, вокзали, аеропорти, порти, станції та інші транспортні підприємства, установи та організації, які забезпечують належне функціонування транспортної системи на державному, регіональному та місцевому рівнях;

(9) *статті 292 (Порушення об'єктів магістральних або промислових нафто-, газо-, конденсатопроводів та нафтопродуктопроводів)* щодо окремих об'єктів енергетичної галузі, що охоплюються нафтогазовою промисловістю. Предметом цього кримінального правопорушення є об'єкти критичної інфраструктури, що відносяться до магістральних або промислових нафто-, газо-, конденсатопроводів та нафтопродуктопроводів, відводи від магістральних чи промислових нафто-, газо-, конденсатопроводів чи нафтопродуктопроводів, об'єкти, споруди та системи, що технологічно

пов'язані з магістральними чи промисловими нафто-, газо-, конденсатопроводами та нафтопродуктопроводами, а також входять до системи суб'єктів господарювання, які забезпечують функціонування цих об'єктів;

(10) *статті 298 (Незаконне проведення пошукових робіт на об'єкті археологічної спадщини, знищення, руйнування або пошкодження об'єктів культурної спадщини)* щодо об'єктив, які мають історико-культурну цінність. Основним безпосереднім об'єктом цього делікту є об'єкти критичної інфраструктури, які несуть історичну (археологічну) та культурну цінність та відносяться до пам'яток історії та/або культури (будинки, укріплення, мости, залишки стародавніх поселень, місця битв, музейні експонати, історичні документи тощо);

(11) *статті 341 (Захоплення державних або громадських будівель чи споруд)* щодо об'єктив, які забезпечують функціонування органів державної влади та органів місцевого самоврядування. Основним безпосереднім об'єктом цього кримінального правопорушення є нормальне (штатне) функціонування органів державної влади, органів місцевого самоврядування та об'єднань громадян. Предметом зазначеного складу виступають будівельні об'єкти місцезнаходження цих органів. Зокрема, будівлі і споруди, що забезпечують діяльність Верховної Ради України, Президента України, Ради національної безпеки і оборони України, Кабінету Міністрів України, судової гілки влади, а також інших суб'єктів національної системи захисту критичної інфраструктури;

(12) *статті 361 (Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж)* щодо об'єктив ІТ-інфраструктури. До об'єктів цих кримінально караних діянь відносяться комп'ютерні мережі та їх системи, незаконне втручання в роботу яких загрожує життєво важливим функціям діяльності держави;

(13) *статті 411 (Умисне знищення або пошкодження військового майна)* щодо окремих об'єктив критичної інфраструктури військового призначення. Диспозитивна частина цих деліктів не містить конкретного переліку майна, що є предметом зазначених кримінальних правопорушень. Проте, основна їх відмінність від інших кримінально карних діянь полягає у тому, що це майно має знаходитися у військовій власності. З метою розмежування (структуризації) характеру суспільної

небезпеки і ступенів тяжкості, до кваліфікаційних ознак цих діянь було віднесено загибель людей або спричинення інших тяжких наслідків. Під іншими тяжкими наслідками слід розуміти повне або тимчасове виведення зі строю об'єктів критичної інфраструктури, що мають військове призначення. Зокрема, аеродроми, систем водо- та енергопостачання (водовідведення), системи безпеки, зв'язку тощо;

(14) *статті 438 (Порушення законів та звичаїв війни)* щодо об'єктів критичної інфраструктури, недоторканність яких визначена міжнародними нормативно-правовими актами під час війни. Тобто, ці діяння суперечать (порушують) норми та положення міжнародного гуманітарного права, що закріплені у низці міжнародних нормативно-правових актах. Зокрема, до останніх відносяться Угода про захист культурних, наукових закладів та історичних пам'яток від 15 квітня 1935 року, Женевська конвенція про захист цивільного населення під час війни від 12 серпня 1949 року та додаткові протоколи до неї, Європейська конвенція з прав людини від 04 листопада 1950 року та протоколів до неї, Гаазька конвенція про захист культурних цінностей у випадку озброєного конфлікту від 14 травня 1954 року та додаткові протоколи до неї тощо.

Об'єктивна сторона цього делікту може проявлятися у бомбардуванні чи ракетному обстрілі об'єктів критичної інфраструктури цивільного чи соціального призначення (закладів охорони здоров'я, музеїв, архівів, гідротехнічних споруд, нафтопромислових підприємства, атомних електростанцій та інших об'єктів, пошкодження чи виведення з ладу яких є небезпечним для життя та здоров'я цивільного населення);

(15) *статті 441 (Екоцид)* щодо об'єктив, які забезпечують життєдіяльність екологічної системи в України. Відповідно до Української дипломатичної енциклопедії, «екоцидом» є масове знищення рослинного або тваринного світу, отруєння атмосфери або водних ресурсів, а також вчинення інших дій, що можуть спричинити екологічну катастрофу, у тому числі, спричинену в результаті впливу бойових дій. Предметом цього кримінального правопорушення є рослинний і тваринний світ, атмосфера і водні ресурси, земля, надра та інші компоненти екосистеми і космічного простору.

Поряд з цим, безпека критичної інфраструктури може виступити і як додаткова кваліфікаційна ознака кримінальних правопорушень передбачених статтями 194 (Умисне знищення або пошкодження

майна), 197 (Порушення обов'язків щодо охорони майна), 233 (Незаконна приватизація державного, комунального майна), 258 (Терористичний акт), 258-2 (Публічні заклики до вчинення терористичного акту), 259 (Завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності), 360 КК України (Умисне пошкодження або руйнування телекомунікаційної мережі) тощо.

До загальних особливостей кримінальних правопорушень, що посягають на об'єкти критичної інфраструктури відносяться:

(1) пошкодження чи знищення об'єктів або їх елементів, які є критично важливими для життєдіяльності держави, у тому числі, загальнонебезпечним способом;

(2) заподіяння державі та її громадянам майнової шкоди у великих чи/або особливо великих розмірах;

(3) заподіяння цивільному населенню моральної чи фізичної шкоди, у тому числі, що призвела до непоправних наслідків для життя і здоров'я великої кількості людей;

(4) у деяких випадках відкритість та демонстративність дій, а іноді їх ультимативність;

(5) залежно від значимості об'єкта, характер спричинених наслідків може охоплюватися місцевим, регіональним (галузевим), державним рівнем, а іноді мати міжнародний характер;

(6) наявність причинно-наслідкового зв'язка між діями винного та спричиненими наслідками, які в більшості випадків є тяжкими та/або особливо тяжкими.

З урахуванням критеріїв, що впливають на кваліфікацію протиправних діянь та обрання виду і розміру покарання, ці кримінальні правопорушення можна розгрупувати залежно від заподіяних наслідків, категорії критичності об'єкта інфраструктури, порушення державних функцій, характеру надзвичайної ситуації, кількості та організованості учасників кримінального правопорушення, способу та мотиву вчинення кримінального правопорушення.

Отже, законодавство про критичну інфраструктуру та її захист складають окремі норми та положення національного та міжнародного права. Особи, винні у його порушенні несуть відповідальність, визначену законом. У цьому значенні, критична інфраструктура може виступати об'єктом, предметом або місцем вчинення кримінальних правопорушень не лише на національному рівні, а й бути предметом

розгляду міжнародних інстанцій, у тому числі, Міжнародного кримінального суду. Тому, особливе значення під час розслідування цих кримінальних правопорушень відводиться належному документуванню зазначених діянь.

§ 3. Кримінально-правова характеристика посягань на об'єкти критичної інфраструктури

Стаття 113 (Диверсія).

Підслідність – слідчі органи Служби безпеки України.	
Класифікація кримінального правопорушення – *особливо тяжкий*.	
Об'єкт – відносини, що забезпечують національну безпеку України та є її складовими. *Предмет диверсії* – конкретні об'єкти, на які спрямована диверсія.	*Сфера дії статті* – функціонування життєво важливих об'єктів, які забезпечують життєдіяльність економічної, екологічної, оборонної (воєнної), безпекової, охоронної, інституційної та/або будь-якої іншої сфери діяльності держави. *Суспільна небезпека* полягає у тому, що діяння загрожує суспільно-економічній та воєнно-політичній незалежності країни.
Об'єктивна сторонам – вибух, підпал, інші дії, спрямовані на масове знищення людей, заподіяння тілесних ушкоджень, радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій, руйнування або пошкодження установ органів державної влади, виробничих підприємства, засобів зв'язку та інших об'єктів критичної інфраструктури[1].	Особливість диверсії полягає у вчиненні суспільно небезпечних дій, які проявляються у семи особливо небезпечних формах спрямованих на: 1) масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їх здоров'ю; 2) руйнування або пошкодження життєво важливих об'єктів, систем та їх складових; 3) радіоактивне забруднення; 4) масове отруєння; 5) поширення епідемії; 6) поширення епізоотії; 7) поширення епіфітотій. *Правопорушення вважається закінченим* з моменту вчинення вибуху, підпалу та інших дій незалежно від настання зазначених у диспозиції статті наслідків. Матеріальна шкода враховується при призначенні покарання та на кваліфікацію

[1] *Масове знищення людей* – позбавлення життя багатьох людей в залежності від обставин.

Дії, *спрямовані на радіоактивне забруднення*, можуть бути, наприклад, руйнування чи пошкодження промислових об'єктів ядерної (атомної) енергетики.

Дії, *спрямовані на масове отруєння*, полягають у отруєнні токсичними (отруйними) речовинами води, повітря, продуктів харчування, ліків тощо.

Дії, *спрямовані на поширення епідемії, епізоотії чи епіфітотії*, полягають у розповсюдженні чи у спробі розповсюдження будь-яким способом на території України збудників хвороб, захворювань, інфекцій тощо.

	не впливає. *Склад – матеріальний.*
Суб'єктивна сторона – прямий умисел.	Винний усвідомлює суспільно небезпечний характер своїх дій та бажає настання їх наслідків. *Мотиви* – різні (помста, політична ненависть, користь тощо). *Спеціальна мета* – направлена на ослаблення держави її законодавчої, виконавчої, судової гілок влади.
Суб'єкт – загальний	
Кваліфікаційний склад полягає у вчиненні кримінального правопорушення в умовах воєнного стану або в період збройного конфлікту *(ч. 2).*[1]	

Стаття 194-1 (Умисне пошкодження об'єктів електроенергетики).

Підслідність – органи досудового розслідування Національної поліції.	
Класифікація кримінального правопорушення – *особливо тяжкий.*	При наявності кваліфікаційних ознак передбачених *ч. 3.*
Об'єкт – безпека постачання електроенергії через захист електроенергетичної інфраструктури, а також охорона життя, здоров'я та майна. *Предметом правопорушення* є конкретні об'єкти електроенергетики[2]	*Додатковий об'єкт* – здоров'я, життя та майно незалежно від форм власності[3]. *Суспільна небезпека діяння* має соціально-економічний характер, що полягає, з однієї сторони, у загрозі чи/або заподіянню шкоди життю та здоров'ю громадян, а з іншої – у пошкодженні чи знищенні об'єктів електроенергетичної галузі, від функціонування яких залежить соціально-економічний розвиток країни чи/або окремого її регіону, де постійно проживають люди. *Сфера дії статті* – електроенергетична інфраструктура.
Об'єктивна сторона кримінального правопорушення характеризується	Правопорушення вважається *закінченим* з моменту настання передбачених

[1] *Воєнний стан* – це особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень.

Період збройного конфлікту – певний проміжок часу, на протязі якого триває збройне протистояння, що відбувається між державами, або тривале збройне протистояння між урядовою владою та організованими збройними угрупуваннями, або ж лише між організованими збройними угрупуваннями.

[2] *Об'єктами електроенергетики* є електрична станція (крім ядерної частини атомної електричної станції), електрична підстанція, електрична мережа.

[3] *Майнова шкода* вважається заподіяною у великих розмірах, якщо прямі збитки становлять суму, що в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян, а в особливо великих розмірах - якщо прямі збитки становлять суму, що в тисячу і більше разів перевищує неоподатковуваний мінімум доходів громадян.

сукупністю трьох ознак, що полягають у: *1)* діянні – пошкодженні або руйнуванні об'єктів електроенергетики; *2)* наслідками – у вигляді порушення нормальної роботи цих об'єктів або спричинення небезпеки для життя та здоров'я людей; *3)* причинно-наслідковим зв'язком між діянням та наслідками.	диспозицією статті наслідків, що полягають у порушенні функціонування об'єктів електроенергетики. *Склад – матеріальний.*
Суб'єкт – загальний.	
Суб'єктивна сторона – прямий умисел.	Винний усвідомлює суспільну небезпеку своїх дій, спрямованих на умисне пошкодження або руйнування об'єктів електроенергетики, і бажає настання передбачених наслідків, при цьому мотиви можуть бути різні.
Кваліфікований склад полягає у вчиненні дій передбачених *ч. 1* повторно або загальнонебезпечним способом (підпал, вибух тощо) *(ч. 2)*, або якщо ці дії спричинили загибель людей чи інші тяжкі наслідки *(ч. 3)*.	

Стаття 252 (Умисне знищення або пошкодження територій, взятих під охорону держави, та об'єктів природно-заповідного фонду).

Підслідність – органи досудового розслідування Національної поліції.	
Класифікація кримінального правопорушення – *особливо тяжкий*.	За наявності кваліфікаційних ознак передбачених *ч. 2*. При наявності складу передбаченого *ч. 1* – кримінального правопорушення відноситься до кримінальних проступків *(форма досудового розслідування – дізнання)*.
Об'єкт – відносини, що забезпечують захист територій і об'єктів, взятих під охорону держави, а також охорона життя, здоров'я та майна (ч. 2). *Предметом* кримінального правопорушення є окремі території та об'єкти, які відповідно до нормативно-правових актів взяті під охорону держави.	*Додатковий об'єкт* – здоров'я, життя та майно незалежно від форм власності. *Суспільна небезпека діяння* має екологічний характер, що порушує екологічну рівновагу. До *територій взятих під охорону держави* належать, водно-ботанічні угіддя загальнодержавного значення (цінні природні комплекси боліт, заплавних лук і лісів, а також водних об'єктів), наукові об'єкти, що становлять національне надбання, які не піддаються відтворенню і втрата або руйнування яких матиме серйозні негативні наслідки для розвитку

	науки та суспільства. До *об'єктів природньо-заповідного фонду,* належать, природні території та об'єкти які мають статус заповідників, природніх парків, ландшафтних парків, заказників, пам'яток природи, заповідних урочищ, ботанічних садів, дендрологічних парків, зоологічних парків, пам'яткі садово-паркового мистецтва тощо. *Сфера дії статті* – охоплює території та об'єкти, взяті під охорону держави, у тому числі об'єкти природньо-заповідного фонду.
Об'єктивна сторона полягає у знищенні або пошкодженні будь-яким способом територій, взятих під охорону держави, або об'єктів природньо-заповідного фонду України (ч. 1) ті самі вчинені шляхом підпалу або іншим загальнонебезпечним способом, якщо це спричинило загибель людей або інші тяжкі наслідки (ч.2).	Диспозиція статті – *бланкетна.* *Обов'язкова ознака* – заподіяння шкоди природнім територіям та об'єктам, взятим під охорону держави, а також причинно наслідковий зв'язок між діями та наслідками. *Склад – матеріальний.*
Суб'єктивна сторона характеризується прямим умислом.	
Суб'єкт – змішаний, у більшості випадків загальний, іноді – спеціальний.	Спеціальним суб'єктом може бути посадова особа, до обов'язків якої входить захист територій та об'єктів взятих під охорону держави, у тому числі, природньо-заповідного фонду.
Кваліфікуючими ознаками правопорушення є вчинення дій, передбачених *ч. 1* шляхом підпалу або іншим загальнонебезпечним способом, або якщо в результаті вчинення дій передбачених ч. 1 було спричинено загибель людей або настання інших тяжких наслідків *(ч. 2)*.[1]	

Стаття 258 (Терористичний акт).

Підслідність – слідчі органи Служби безпеки України.	
Класифікація кримінального правопорушення – *особливо тяжкий*.	За наявності кваліфікаційних ознак передбачених *ч. 2, 3*.
Об'єкт – охорона безпеки суспільства,	*Суспільна небезпека діяння* полягає у тому,

[1] *Загибель людей означає* смерті однієї або декількох осіб.

Іншими тяжкими наслідками можуть визначатись, зокрема, заподіяння тяжких тілесних ушкоджень, масове захворювання людей, виведення з ладу об'єктів критичної інфраструктури (гребель, систем водо- та енергопостачання, зв'язку тощо), масова загибель об'єктів тваринного світу, знищення лісових масивів на значних площах, спричинення особливо великих матеріальних збитків, неможливість проживання населення на певній території, у тому числі, вимушене переселення людей тощо.

Підпалом є свідоме спричинення пожежі шляхом застосування джерел вогню.

Інший загальнонебезпечний спосіб полягає у вчиненні вибухів, затоплень, обвалів та інших дій, які є небезпечними для навколишнього середовища.

майна, що становить матеріальну цінність, а також життя та здоров'я людини.	що винні як засіб для досягнення мети намагаються посіяти у оточуючих страх, викликати паніку, паралізувати діяльність органів влади, спровокувати воєнні конфлікти. *Сфера дії статті* – інтереси особи, суспільства і держави.
Об'єктивна сторона характеризується 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, міжнародними організаціями, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій з тією самою метою.	Кримінальне правопорушення вважається *закінченим* з моменту вчинення дій зазначених диспозицією статті, або з загрози їх вчинення. Особа звільняється від кримінальної відповідальності за діяння, передбачене частиною першою цієї статті в частині погрози вчинення терористичного акту, якщо вона до повідомлення їй про підозру у вчиненні нею терористичного акту добровільно повідомила правоохоронний орган про це діяння, сприяла його припиненню або розкриттю, у разі якщо внаслідок цього і вжитих заходів було відвернено небезпеку для життя чи здоров'я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо в її діях немає складу іншого кримінального правопорушення. *Склад* – усічений.
Суб'єктивна сторона – прямий умисел.	Залякування може бути адресоване невизначеному колу осіб та органів державної влади. *Мотиви* можуть бути різні. *Мета* – порушення суспільної безпеки; залякування населення чи вплив на прийняття рішень органами влади.
Суб'єкт – загальний.	Особа, яка досягла 14 років.
Кваліфікуючими ознаками правопорушення є вчинення передбачених *ч. 1* дій повторно або за попередньою змовою групою осіб, або якщо вони призвели до заподіяння значної майнової шкоди чи інших тяжких наслідків *(ч. 2),* або якщо ці дії призвели до загибелі людини *(ч. 3).*	

Стаття 259 (Завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності).

Підслідність – органи досудового розслідування Національної поліції.	
Класифікація кримінального правопорушення –*тяжкий.*	За наявності кваліфікаційних ознак передбачених *ч. 2.*

Об'єкт – громадська безпека, охорона майна, що становить матеріальну цінність, а також життя та здоров'я людини. *Предметом кримінального правопорушення* є майно незалежно від форми власності *(ч.1)* або об'єкти критичної інфраструктури *(ч. 2)*	*Суспільна небезпека діяння* полягає у тому, що поширення неправдивих відомостей створює обстановку загального страху і невпевненості, викликає недовіру до органів влади, може породити паніку, тим самим порушити громадську безпеку. При кваліфікованому складі кримінальне правопорушення може бути *двооб'єктним*, де додатковим об'єктом виступає належне функціонування об'єктів критичної інфраструктури, життя та здоров'я людей або спричинення інших тяжких наслідків. *Сфера дії статті* – інтереси невизначеного кола фізичних та юридичних осіб.
Об'єктивна сторона характеризується єдиною обов'язковою ознакою – суспільно небезпечною дією, яка полягає у *завідомо неправдивому повідомленні* про підготовку вибуху, підпалу або інших дій (вчинення терористичного акту), які загрожують загибеллю людей чи настання інших тяжких наслідків.	*Обов'язковою ознакою є завідомо неправдиве повідомлення*. Тобто, повідомлення зроблене будь-яким способом і доведено до широкого кола осіб чи/або хоча б однієї особі з метою його подальшого поширення. За своїм змістом воно стосується здійснення у майбутньому терористичного акту, або інших суспільно небезпечних дій, які загрожують життю або здоров'ю громадян та/або належному функціонуванню об'єктів критичної інфраструктури. За своїм характером це повідомлення має бути безсумнівно, очевидно неправдивим, а це значить, що винний у подальшому реально не має на меті вчинення цих дій. Кримінальне правопорушення вважається *закінченим* з моменту здійснення повідомлення. *Склад – формальний*.
Суб'єктивна сторона – умисна форма вини. Особа точно знала, що поширена нею інформація є видуманою, розуміла, що такі дії викликають у населення стан страху, тим самим порушувала громадську безпеку. Винний усвідомлював суспільно небезпечний характер своїх дій, передбачав суспільно небезпечні наслідки у вигляді шкоди громадській безпеці.	Бажаючи настання цих наслідків, що виражаються у дезорганізації діяльності життєво важливих для функціонування держави та її суспільства об'єктів інфраструктури чи викликаної паніки у населення – він діяв з прямим умислом. *Мотиви* можуть бути різні (помста, користь, хуліганські, націоналістичні спонукання тощо). *Мета* – ввести в оману фізичних та/або юридичних осіб, які є адресатом цього повідомлення, і тим самим завдати шкоди громадській безпеці, нормальній

	діяльності органів державної влади, правам та інтересам окремих громадян тощо.
Суб'єкт – загальний.	Особа, яка досягла 14 років.
Кваліфікуючими ознаками правопорушення є вчинення передбачених *ч. 1* дій, якщо об'єктами завідомо неправдивого повідомлення стали критично важливі об'єкти інфраструктури або будівлі чи споруди, що забезпечують діяльність органів державної влади, або заклади охорони здоров'я, або заклади освіти або якщо воно спричинило тяжкі наслідки чи вчинені повторно *(ч. 2)*.[1]	

Стаття 261 (Напад на об'єкти, на яких є предмети, що становлять підвищену небезпеку для оточення).

Підслідність – органи досудового розслідування Національної поліції.	
Класифікація кримінального правопорушення – *особливо тяжкий*.	
Об'єкт – забезпечення захисту та безпеки об'єктів, на яких є предмети, що становлять підвищену небезпеку для оточення, громадська та екологічна безпека. *Предметом правопорушення* є конкретні об'єкти, що виробляють, зберігають, транспортують, досліджують, використовують, радіоактивні речовини, хімічні, біологічні та вибухонебезпечні матеріали, предмети тощо.	*Суспільна небезпека діяння* має екологічний характер, що може порушити екологічну рівновагу та завдати значної шкоди навколишньому середовищу. *Сфера дії статті* – виробництва, сховища, транспортні засоби, наукові установи, військові частини та інші об'єкти, на яких виготовляються, зберігаються, використовуються або якими транспортуються радіоактивні, хімічні, біологічні та вибухонебезпечні матеріали, речовини, предмети.
Об'єктивна сторона полягає у нападі на зазначені об'єкти.	Диспозиція статті – *банкетна*. *Обов'язкова ознака* правопорушення полягає у нападі на зазначені об'єкти, тобто, застосування насильства чи створення реальної загрози його застосування до працівників цих об'єктив. *Склад – формальний*.
Суб'єктивна сторона – прямий умисел.	Винний усвідомлює суспільно небезпечний характер своїх дій та передбачає заподіяння шкоди для громадської чи екологічної безпеки. *Мотиви* – різні, у тому числі, порушення штатного функціонування цих обєктів. *Мета* – захоплення, пошкодження або знищення таких об'єктів.
Суб'єкт – загальний.	

[1] *Тяжкі наслідки* є оціночним поняттям, їх наявність визначається у кожному конкретному випадку з урахуванням усіх обставин кримінального провадження (розслідування).

Стаття 270-1 (Умисне знищення або пошкодження об'єктів житлово-комунального господарства).

Підслідність – органи досудового розслідування Національної поліції.	
Класифікація кримінального правопорушення – *особливо тяжкий.*	При наявності кваліфікаційних ознак передбачених *ч. 3.*
Об'єкт – безпека громадян (соціальна безпека) через захист об'єктів, які надають житлово-комунальні послуги, а також охорона життя, здоров'я та майна *(ч. 3).* *Предметом правопорушення* є конкретні об'єкти житлово-комунального господарства[1], які надають житлово-комунальні послуги.	*Додатковий об'єкт* – здоров'я, життя та майно незалежно від форм власності[2]. *Суспільна небезпека діяння* має соціально-економічний характер, що полягає, з однієї сторони, у загрозі чи/або заподіянню шкоди життю та здоров'ю громадян, а з іншої – у пошкодженні чи знищенні об'єктів житлово-комунальної інфраструктури, від функціонування яких залежить соціально-економічний розвиток країни чи/або окремого її регіону, де постійно проживають люди. *Сфера дії статті* – інфраструктура міста.
Об'єктивна сторона кримінального правопорушення характеризується сукупністю трьох ознак, що полягають у: *1)* діянні – знищення або пошкодження об'єктів житлово-комунального господарства; *2)* наслідками – у вигляді припинення надання житлово-комунальних послуг; *3)* причинно-наслідковим зв'язком між діянням та наслідками.	Кримінальне правопорушення вважається *закінченим* з моменту настання передбачених диспозицією статті наслідків, що полягають у порушенні функціонування об'єктів житлово-комунального господарства. *Склад – матеріальний.*
Суб'єктивна сторона – прямий умисел.	Винний усвідомлює суспільну небезпеку своїх дій, спрямованих на умисне знищення або пошкодження об'єктів житлово-комунального господарства, і бажає настання передбачених наслідків, при цьому мотиви можуть бути різними.
Суб'єкт – загальний.	
Кваліфікований склад правопорушення полягає у тому, що дії передбачені *ч. 1*, вчинені повторно, або загальнонебезпечним способом (підпал, вибух тощо) *(ч. 2)*, та	

[1] *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).

[2] *Майнова шкода* вважається заподіяною у великих розмірах, якщо прямі збитки становлять суму, що в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян, а в особливо великих розмірах – якщо прямі збитки становлять суму, що в тисячу і більше разів перевищує неоподатковуваний мінімум доходів громадян.

заподіяли майнову шкоду в особливо великому розмірі або спричинили загибель людей чи інші тяжкі наслідки *(ч. 3)*.[1]

Стаття 273 (Порушення правил безпеки на вибухонебезпечних підприємствах або у вибухонебезпечних цехах).

Підслідність – органи досудового розслідування Національної поліції.	
Класифікація кримінального правопорушення – *тяжкий.*	За наявності кваліфікаційних ознак, передбачених *ч. 2.*
Об'єкт – захист та дотримання спеціальних правил безпеки під час виконання робіт на вибухонебезпечних підприємствах або у вибухонебезпечних цехах, а також охорона життя, здоров'я та майна. *Потерпілий* – будь-яка особа.	*Додатковий об'єкт* – здоров'я, життя та майно людини. *Суспільна небезпека* – полягає у загрозі або заподіянні шкоди життю, здоров'ю та майну великої кількості людей. *Сфера дії статті* – виробнича діяльність у вибухонебезпечних підприємствах або у вибухонебезпечних цехах незалежно від виду їх діяльності та форм власності.
Об'єктивна сторона: *ч. 1* **–** порушення правил безпеки на вибухонебезпечних підприємствах або у вибухонебезпечних цехах, якщо це створило загрозу загибелі людей чи настання інших тяжких наслідків або заподіяло шкоду здоров'ю потерпілого. *ч. 2* – загибель людей або інші тяжкі наслідки. *Місце вчинення кримінального правопорушення* – спеціально визначене (вибухонебезпечне підприємство або вибухонебезпечний цех)	Диспозиція статті – *бланкетна.* *Порушення* правил безпеки може виражатися *дією*, так й *бездіяльністю* або в поєднанні. Обов'язковою ознакою об'єктивної сторони є *місце вчинення кримінального правопорушення*, а також *причинний зв'язок* між допущеними порушеннями і реальними наслідками, що настали, або могли настати[2]. *Кримінальне правопорушення вважається закінченим,* якщо в результаті такого порушення створено реальну загрозу загибелі людей чи настання інших тяжких наслідків або заподіяння шкоди здоров'ю потерпілого *(ч. 1)*, загибель людей або інші тяжкі наслідки *(ч. 2)*[3]. *Склад кримінального правопорушення – формальний* у частині, якщо порушенням створено реальну загрозу загибелі людей чи настанню інших тяжких наслідків *(ч. 1),*

[1] Під збитками в особливо великих розмірах мається на увазі якщо пряма заподіяна шкода в тисячу і більше разів перевищує неоподаткований мінімум доходів громадян.

[2] Особливого значення набуває місце вчинення правопорушення, тому до матеріалів кримінального провадження необхідно долучати копії нормативно-правих актів (наказів, положень, регламентів тощо) про віднесення підприємства (цеху) до певної категорії (класу) вибухонебезпечності.

Для встановлення змісту порушення потрібно також звернутися до спеціальних правил, що передбачають дотримання заходів безпеки на вибухобезпечних підприємствах (цехах) від вибухів і супутніх їх пожеж, отруєнь та інших тяжких наслідків (наприклад: Інструкція з організації безпечного ведення вогневих робіт на пожежонебезпечних та вибухонебезпечних об'єктах, затверджена наказом Міністерства праці та соціальної політики України від 05.06.2011 № 255)

[3] Під *здоров'ям потерпілого та загибеллю людей* слід розуміти наслідки у контексті згаданому в ст. 252 КК України.

Під *іншими тяжкими наслідками* слід розуміти наслідки у контексті згаданому в ст. 270-1 та 274 КК України.

	матеріальний (ч. 1 та 2).
Суб'єктивна сторона – характеризується змішаною формою вини або необережністю.	*Самовпевненість* полягає у *свідомому* порушенні винним правил безпеки на вибухонебезпечних об'єктах, при якому він *передбачав* можливість настання суспільно небезпечних наслідків свого діяння, але *легковажно* розраховував на їх відвернення. При *недбалості* винний не передбачав можливість настання суспільно небезпечних наслідків свого діяння, хоча повинен був і міг їх передбачити.
Суб'єкт – *спеціальний.*	Ним може бути особа, яка зобов'язана дотримувати правил безпеки на вибухонебезпечних підприємствах або у вибухонебезпечних цехах, у тому числі особа, яка є сторонньою для даних виробництв, але яка на законних підставах знаходилися на таких підприємствах та яка була у встановленому порядку ознайомлена з правила безпеки на вибухонебезпечних об'єктах.
Кваліфікований склад правопорушення полягає у діянні, що спричинило загибель людей або інші тяжкі наслідки *(ч. 2).*	

Стаття 274 (Порушення правил ядерної або радіаційної безпеки).

Підслідність – органи досудового розслідування Національної поліції.	
Класифікація кримінального правопорушення – *особливо тяжкий.*	При наявності кваліфікаційних ознак, передбачених *ч. 2.*
Об'єкт – охорона спеціальних правил ядерної або радіаційної безпеки на виробництві, а також охорона життя, здоров'я та майна[1]. *Потерпілий* – будь-яка особа.	*Додатковий об'єкт* – здоров'я, життя та майно людини. *Суспільна небезпека* – полягає у загрозі або заподіянні шкоди життю, здоров'ю та майну великої кількості людей, знищення або пошкодження атомних реакторів та інших експлуатаційних установок, радіоактивне зараження місцевості, опромінювання населення. *Сфера дії статті* – виробнича діяльність підприємств, на яких використовується ядерні або радіаційні матеріали.

[1] *Ядерна безпе*ка – це дотримання норм, правил, стандартів і умов використання ядерних матеріалів, що забезпечують радіаційну безпеку. *Радіаційна безпека* – дотримання допустимих меж радіаційного впливу на персонал, населення і довкілля, що встановлені нормами, правилами та стандартами з безпеки.

Об'єктивна сторона: *ч. 1* – порушення на виробництві правил ядерної або радіаційної безпеки, якщо це спричинило загрозу загибелі людей чи настання інших тяжких наслідків або заподіяло шкоду здоров'ю потерпілого. *ч. 2* – загибель людей або інші тяжкі наслідки.	Диспозиція статті – *бланкетна*[1]. *Порушення* правил ядерної або радіаційної безпеки може виражатися як *дією*, так і *бездіяльністю*. Обов'язковою ознакою об'єктивної сторони є *місце вчинення правопорушення*[2]. *Кримінальне правопорушення закінчене* з моменту порушення правил ядерної або радіаційної безпеки, у тому числі, якщо воно *тривале* і має часовий розрив між самим порушенням правил і його припиненням. *Склад кримінального правопорушення – формальний* у частині, якщо порушенням створено загрозу загибелі людей чи настанню інших тяжких наслідків *(ч. 1), матеріальний (ч. 1, 2).*
Суб'єктивна сторона – характеризується змішаною формою вини або необережністю.	Особливість полягає у *свідомому* порушенні винним правил ядерної або радіаційної безпеки, при якому він *передбачав* можливість настання суспільно небезпечних наслідків свого діяння, але *легковажно* розраховував на їх відвернення.
Суб'єкт – *спеціальний*.	Ним може бути особа, яка зобов'язана дотримувати правил ядерної або радіаційної безпеки.
Кваліфікований склад правопорушення полягає у діянні, що спричинило загибель людей або інші тяжкі наслідки *(ч. 2)*[3].	

Стаття 279 (Блокування транспортних комунікацій, а також захоплення транспортного підприємства).

Підслідність – органи досудового розслідування Національної поліції.	
Класифікація кримінального правопорушення – *особливо тяжкий*.	При наявності кваліфікаційних ознак, передбачених *ч. 3*. При наявності складу передбаченого *ч. 1* – кримінального правопорушення відноситься до кримінальних проступків

[1] Дотримання ядерної і радіаційної безпеки на виробництві регулюється законодавчими й іншими нормативно-правовими актами, зокрема Законом України «Про використання ядерної енергії та радіаційну безпеку».

[2] *До виробництв, де використовуються ядерні матеріали*, належать атомні станції, споруди і комплекси з промисловими, експериментальними і дослідницькими ядерними реакторами і ядерними стендами, інше. *До виробництв, що містять радіоактивні матеріали*, належать, зокрема, сховища радіоактивних відходів. Ядерними матеріалами є: уран, плутоній, торій у вигляді металу, сплаву, хімічного концентрату, інший матеріал, що містить зазначені речовини у визначеній концентрації. *Радіоактивними* – є джерела іонізуючого випромінювання, природного або штучного походження, що знаходяться в будь-якому стані.

[3] Під *іншими тяжкими наслідками* слід розуміти людські жертви, вибухи, знищення або пошкодження атомних реакторів та інших експлуатаційних установок, радіоактивне зараження місцевості, опромінення населення.

	(форма досудового розслідування – дізнання).
Об'єкт – штатне функціонування транспортної галузі, об'єктів, які забезпечують її функціонування, а також безпека функціонування транспортних комунікацій, руху та експлуатації транспорту, безпека експлуатації всієї транспортної системи. *Предметом* правопорушення є транспортні комунікації *(ч. 1)*, вокзали, аеродроми, порти, станції та інші транспортні підприємства, установи та організації *(ч. 2),* загибель людей, або інші тяжкі наслідки *(ч. 3)*[1]	*Додатковий об'єкт* – здоров'я і життя людини, а також приватна, комунальна та державна власність. *Суспільна небезпека* – полягає у загрозі або заподіянні шкоди життю, здоров'ю та майну великої кількості людей, порушення ланцюгів постачання товарів та послуг, порушення логістичних зав'язків, завдання збитків економіці країни чи окремого її регіону. *Предметом* правопорушення є лише ті транспортні підприємства, установи, організації, які забезпечують рух і експлуатацію транспорту, тобто від яких безпосередньо залежить рух та експлуатація транспорту. *Сфера дії статті* – транспортні підприємства, установи та організації, а також об'єкти та їх сукупні елементи, що забезпечують діяльність транспортної галузі.
Об'єктивна сторона: *ч. 1 – блокування* транспортних комунікацій; *ч. 2 – захоплення* вокзалу, аеродрому, порту, станції, або іншого транспортного підприємства, установи або організації; *ч. 3* – якщо дії передбачені ч. 1 та 2 спричинили загибель людей чи наслати інших тяжких наслідків.[2]	Диспозиція статті – *змішана.* Обов'язковою ознакою об'єктивної сторони є *місце вчинення кримінального правопорушення,* а також *причинно-наслідковий зв'язок* між діями та наслідками, який полягає у, по-перше, порушенні нормальної роботи транспорту, по-друге, створенні небезпеки для життя і здоров'я людей або настання інших тяжких наслідків, та по-третє, спричинення загибелі людей, або настання інших тяжких наслідків. Кримінальне правопорушення вважається *закінченим* з моменту настання одного із наслідків визначених в диспозиції статті. *Склад – формальний (ч. 1 та 2), матеріальний (ч. 1 та 3)*
Суб'єктивна сторона	Винний *усвідомлює* суспільно небезпечний

[1] Під *транспортними комунікаціями* слід розуміти шляхи сполучення, споруди на них, засоби сигналізації та зв'язку всіх видів транспорту, включаючи трубопровідний. До комунікацій трубопровідного транспорту належать трубопроводи, а також компресорні станції, лінії сигналізації, зв'язку, пристрої для захисту від корозії тощо.

[2] *Блокування транспортних комунікацій* може здійснюватися шляхом дій або бездіяльності, шляхом перешкоджання у будь-якій спосіб роботи транспортних комунікацій (влаштування перешкод, відключення електропостачання, виставлення пікетів, постів, перекриття шлагбаумів, вимкнення засобів сигналізації, перекриття засувок трубопроводів, влаштування перепон для радіозв'язку тощо).

Під *захоплення об'єктів транспортної інфраструктури* мається на увазі вчинення протиправних дій насильницького або обманного характеру з метою заволодіння цими об'єктами, що як наслідок створює перешкоди щодо вільного використання власником цих об'єктів, або унеможливлює їхнє функціонування в штатному режимі.

характеризується умислом, можлива змішана (подвійна) форма вини *(ч. 3)*.	характер свого діяння та бажає його вчинення. *Мотиви* – різні та не мають значення для кваліфікації, але враховуються при призначенні покарання. *Мета* – бажання заблокувати або захопити об'єкти транспортної інфраструктури.
Суб'єкт – *загальний*.	Суб'єктом кримінального правопорушення можу бути будь-яка осудна особа.
Кваліфікований склад правопорушення полягає у тому, що предметом кримінального правопорушення є об'єкти критичної інфраструктури *(ч. 2),* або в результаті його вчинення було спричинено загибель людей чи інші тяжкі наслідки *(ч. 3)*	

Стаття 292 (Пошкодження об'єктів магістральних або промислових нафто-, газо-, конденсатопроводів та нафтопродуктопроводів).

Підслідність – органи досудового розслідування Національної поліції.	
Класифікація кримінального правопорушення – *особливо тяжкий*.	При наявності кваліфікаційних ознак, передбачених *ч. 3*.
Основний об'єкт – забезпечення енергетичної безпеки, через охорону об'єктів магістральних або промислових нафто-, газо-, конденсатопроводів та нафтопродуктопроводів, що становить матеріальну цінність, а також життя та здоров'я людей. *Предмет* – магістральні або промислові нафто-, газо-, конденсатопроводи чи нафтопродуктопроводи, відводи від них, технологічно пов'язані з ними об'єкти, споруди, технічні засоби та їх елементи, що становлять матеріальну цінність, і пошкодження яких впливає на функціонування зазначених об'єктів інфраструктури.[1]	При кваліфікованому складі правопорушення може бути *двооб'єктовим*, де *додатковим об'єктом* виступає життя та здоров'я людей, власність, довкілля тощо. *Сфера дії статті* – магістральні або промислові нафто-, газо-, конденсатопроводи чи нафтопродуктопроводи, відводи від них, технологічно пов'язані з ними об'єкти, споруди, технічні засоби та їх елементи.
Об'єктивна сторона: *ч. 1* – пошкодження або руйнування об'єктів магістральних або промислових	*Обов'язковою умовою* кримінального правопорушення є причинно-наслідковий зв'язок між діями і наслідками, які є

[1] *Магістральні нафто-, газо- та конденсатопроводи чи нафтопродуктопроводи* – це технологічні комплекси, що функціонують як єдина система і до яких входить окремий трубопровід та пов'язані з ним споруди для транспортування нафти, газу, продуктів їх переробки від місць їх знаходження, видобутку, виготовлення або зберігання в місця їх переробки, споживання, перевантаження чи подальшого транспортування.

Об'єкти і споруди, технологічно пов'язані з магістральними нафто-, газо- та конденсатопроводами чи нафтопроводами – це елементи технологічного комплексу трубопроводу, яким переміщується газ, нафта чи нафтопродукти (сховища, насосні станції, розподільні пристрої, засувки, відстійники тощо).

Відводи від магістральних нафто- , газо-, конденсатопроводів чи нафтопродуктопроводів – це системи чи комплекси об'єкті, які пов'язані з основною системою, але через інженерно-конструктивні особливості відходять від них.

нафто-, газо-, конденсатопроводів та нафтопродуктопроводів, якщо ці дії призвели до порушення нормальної роботи зазначених об'єктів або створили небезпеку для життя людей; *ч. 2* – вчинення дій передбачених частиною першою загальнонебезпечним способом (підпалом, вибухом тощо), або вчинені повторно або за попередньою змовою групою осіб; *ч. 3* – вчинення дій передбачених ч. 1 або 2, якщо вони спричинили загибель людей, інші нещасні випадки з людьми або призвели до аварії, пожежі, значного забруднення довкілля чи інших тяжких наслідків, або вчинені організованою групою.	суспільно небезпечними, оскільки заподіюють значну шкоду власнику майна, ставлять під загрозу безпеку громадян та забруднення довкілля. Діяння може виконуватися шляхом дії або бездіяльності і полягає у пошкодженні чи руйнуванні об'єктів, зазначених диспозицією статті. Кримінальне правопорушення вважається *закінченим* з моменту настання суспільно небезпечних наслідків, передбачених диспозицією статті. *Склад – матеріальний.*
Суб'єктивна сторона характеризується прямим чи/або непрямим (евентуальним) умислом.	Винний усвідомлює, що протиправно знищує чи пошкоджує чуже майно, передбачає неминучість чи реальну можливість заподіяння значної шкоди власнику і навіть бажає чи свідомо допускає настання цих наслідків, або ставиться байдуже до їх настання. *Мета (при прямому умислі) і мотиви* – позбавлені корисливого змісту і можуть бути будь-якими.
Суб'єкт – загальний *(ч. 1)*	Особа, яка досягла 14 років *(ч. 2 та 3).*
Кваліфікований склад правопорушення полягає у тому, що його було вчинено повторно, або за попередньою змовою групою осіб, або загальнонебезпечним способом *(ч. 2),* або якщо в результаті вчинення правопорушення було спричинено загибель людей, настання інших нещасних випадків з людьми, аварій, пожеж, значного забруднення довкілля чи настання інших тяжких наслідків, або якщо діяння було вчинено організованою групою *(ч. 3).*	

Стаття 298 (Незаконне проведення пошукових робіт на об'єкті археологічної спадщини, знищення, руйнування або пошкодження об'єктів культурної спадщини).

Підслідність – органи досудового розслідування Національної поліції.	
Класифікація кримінального правопорушення – *тяжкий.*	При наявності кваліфікаційних ознак, передбачених *ч. 5.* При наявності складу передбаченого *ч. 1* – кримінального правопорушення відноситься до кримінальних проступків *(форма досудового розслідування – дізнання).*

Основний безпосередній об'єкт – охорона пам'яток історії та об'єктів культурної та національної спадщини, що мають особливе значення для збереження національної автентичності, відбивають внесок держави та її народу у розвиток світової цивілізації. *Предметом кримінального правопорушення* є пам'ятки історії та культури, у тому числі національного значення *(ч. 3)*.[1]	*Додатковим об'єктом* є право власності. *Суспільна небезпека діяння* може полягати у завданні непоправимої шкоди для культурної, освітньої, наукової, духовно-релігійної та іншої життєво важливої сфери розвитку українського суспільства, його національної ідентичності та свідомості. *Сфера дії статті* – інтереси невизначеного кола фізичних та юридичних осіб
Об'єктивна сторона – руйнування (знищення) або пошкодження об'єктів культурної спадщини.	Необхідною умовою діяння є *причинно-наслідковий зв'язок*, який характеризується настанням спільно небезпечних наслідків у вигляді шкоди, заподіяної об'єктам культурної спадщини. *Склад – матеріальний.*
Суб'єктивна сторона – умисна вина.	Винний усвідомлює, що знищує чи пошкоджує об'єкти культурної спадщини, передбачає, що може заподіяти шкоду і бажає цього *(прямий умисел)* чи свідомо допускає це *(непрямий умисел)*. При доведенні умислу важливо встановити, що винний знав про те, що відповідний об'єкт відноситься до пам'яткі культурної спадщини.
Суб'єкт – загальний *(ч. 1)* та спеціальний – службова особа *(ч. 5)*.	
Кваліфікований склад правопорушення полягає у тому, що предметом діяння є пам'ятки національного значення (ч. 3), а особливо кваліфікуючий, якщо дії передбачені частиною 2 та 3 вчинені службовою собою з використанням свого службового становища (ч. 5)	

[1] *Культурна спадщина* – сукупність успадкованих людством від попередніх поколінь об'єктів культурної спадщини.

Об'єкт культурної спадщини – визначне місце, споруда (витвір), комплекс (ансамбль), їхні частини, пов'язані з ними рухомі предмети, а також території чи водні об'єкти (об'єкти підводної культурної та археологічної спадщини), інші природні, природно-антропогенні або створені людиною об'єкти незалежно від стану збереженості, що донесли до нашого часу цінність з археологічного, естетичного, етнологічного, історичного, архітектурного, мистецького, наукового чи художнього погляду і зберегли свою автентичність.

Пам'ятка культурної спадщини – об'єкт культурної спадщини, який занесено до Державного реєстру нерухомих пам'яток України, або об'єкт культурної спадщини, який взято на державний облік відповідно до законодавства, що діяло до набрання чинності цим Законом, до вирішення питання про включення (невключення) об'єкту культурної спадщини до Державного реєстру нерухомих пам'яток України.

Нерухомий об'єкт культурної спадщини – об'єкт культурної спадщини, який не може бути перенесений на інше місце без втрати його цінності з археологічного, естетичного, етнологічного, історичного, архітектурного, мистецького, наукового чи художнього погляду та збереження своєї автентичності.

Рухомі предмети, пов'язані з нерухомими об'єктами культурної спадщини – елементи, групи елементів об'єкта культурної спадщини, що можуть бути відокремлені від нього, але складають з ним єдину цілісність, і відокремлення яких призведе до втрати археологічної, естетичної, етнологічної, історичної, архітектурної, мистецької, наукової або культурної цінності об'єкта.

Стаття 341 (Захоплення державних або громадських будівель чи споруд).

Підслідність – слідчі органи Служби безпеки України.	
Класифікація кримінального правопорушення – *нетяжкий*.	
Основний безпосередній об'єкт – функціонування органів державної влади, органів місцевого самоврядування, об'єднань громадян. *Предмет* – будівлі і споруди, які забезпечують діяльність органів державної влади, органів місцевого самоврядування, об'єднань громадян.	*Додатковим обов'язковим об'єктом* є відносини власності, або встановлений порядок використання чи користування будівлями чи спорудами, в яких розміщені ці органи. *Суспільна небезпека* полягає у дестабілізації діяльність владних структур чи/або державних інституцій. *Сфера дії статті* – інституційна інфраструктуру, а також діяльність із забезпечення конституційного ладу та безпеки держави та суспільства.
Об'єктивна сторона – ненасильницьке захоплення державних або громадських будівель чи споруд з метою незаконного користування ними або перешкоджання нормальній роботі підприємств, установ, організацій.	*Кримінальне правопорушення вважається закінченим* з моменту вчинення дій передбачених диспозицією статті, спрямованих на ненасильницьке захоплення державних або громадських будівель чи споруд. Тобто, фактичного захоплення всієї будівлі чи споруди або її окремої частини. При цьому не має значення, чи зайнятий увесь об'єкт, чи окрема його частина. Суттєвим є те, що це захоплення унеможливлює належне функціонування органів державної влади, а також перешкоджає нормальній роботі інших підприємств, установ, організацій, будівлі чи споруди яких незахоплені. *Склад – формальний.*
Суб'єктивна сторона – прямий умисел.	Винний усвідомлює суспільну небезпеку своїх дій, спрямованих на ненасильницьке захоплення зазначених об'єктів, і бажає вчинити ці дії. *Мета* – незаконне користування захопленими об'єктами інфраструктури або перешкодити нормальній діяльності підприємств, установ, організацій.
Суб'єкт – загальний.	

Стаття 360 (Умисне пошкодження або руйнування телекомунікаційної мережі).

Підслідність – органи досудового розслідування Національної поліції.	
Класифікація кримінального правопорушення – *тяжкий.*	При наявності кваліфікаційних ознак, передбачених *ч. 3.* При наявності складу передбаченого *ч. 1* – кримінального правопорушення відноситься до кримінальних проступків *(форма досудового розслідування – дізнання).*
Об'єкт – встановлений порядок забезпечення права на інформацію за допомогою телекомунікаційної інфраструктури (інформаційна безпека). *Предмет* – електронно комунікаційні мережі, технічні засоби, споруди інші об'єкти та їх елементи, що входять до системи електронно комунікаційних мереж та забезпечують діяльність і функціонування з надання електронно-комунікаційних послуг.[1]	*Додатковим об'єктом* є об'єкти критичної інфраструктури, які забезпечують функціонування електронно-комунікаційних послуг. *Сфера дії статті* – телекомунікаційна інфраструктура.
Об'єктивна сторона кримінального правопорушення характеризується сукупністю трьох ознак, що полягають у: *1)* діянні – пошкодженні або руйнуванні телекомунікаційних мереж; *2)* наслідками – у вигляді припинення надання телекомунікаційних послуг; *3)* причинно-наслідковим зв'язком між діянням та наслідками.[2]	Це можуть бути, наприклад, обривання мереж, руйнування обладнання, створення інших перешкод з метою порушення їх роботи в штатному режимі. Кримінальне правопорушення вважається *закінченим* з моменту настання передбачених диспозицією статті наслідків, що полягають у припиненні надання телекомунікаційних послуг.

[1] *Електронна комунікаційна мережа* – комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг.

Електронна комунікаційна мережа загального користування – електронна комунікаційна мережа, доступ до якої відкритий для всіх кінцевих користувачів послуг.

Електронна комунікаційна послуга – послуга, що полягає в прийманні та/або передачі інформації через електронні комунікаційні мережі, крім послуг з редакційним контролем змісту інформації, що передається за допомогою електронних комунікаційних мереж і послуг.

Електронна комунікація (телекомунікація, електрозв'язок) – передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій.

Інфраструктура електронних комунікаційних мереж – технічні засоби та/або споруди електронних комунікаційних мереж (елементи інфраструктури електронних комунікаційних мереж).

Лінія електронних комунікаційних мереж (лінія зв'язку) – елемент інфраструктури електронної комунікаційної мережі, що створює середовище розповсюдження електромагнітних сигналів по радіо, проводових, оптичних чи інших електромагнітних системах між технічними засобами електронних комунікацій, призначеними для передавання та/або приймання електромагнітних сигналів, та/або кінцевим обладнанням.

Мережа Інтернет (Інтернет) – глобальна електронна комунікаційна мережа, що призначена для передачі даних та складається з фізично та логічно взаємоз'єднаних окремих електронних комунікаційних мереж, взаємодія яких базується на використанні єдиного адресного простору та на використанні інтернет-протоколів, визначених міжнародними стандартами.

[2] *Пошкодження телекомунікаційної інфраструктури* полягає у приведення відповідних об'єктів, систем та елементів, що забезпечують діяльність з надання електронних комунікаційних послуг, у непридатний за їх цільовим призначенням стан.

	Склад – матеріальний.
Суб'єктивна сторона – прямий умисел.	Винний усвідомлює суспільну небезпеку своїх дій, спрямованих на умисне пошкодження або руйнування телекомунікаційних мереж, і бажає настання їх наслідків, при цьому мотиви можуть бути різні. Якщо метою припинення електронних телекомунікаційних послуг є ослаблення держави та її інституцій, то дії винного кваліфікуються за ст. 113 КК України (Диверсія). Необережне знищення або пошкодження телекомунікаційних мереж кваліфікується за ст. 196 КК України (Необережне знищення або пошкодження майна).
Суб'єкт – загальний.	
Кваліфікований склад правопорушення полягає в тому, що дії передбачені ч. 1, якщо вони вчинені повторно або за попередньою змовою групою осіб, або загальнонебезпечним способом (підпал, вибух тощо) *(ч. 2)*, та якщо вони заподіяли майнову шкоду у великому розмірі або спричинили припинення надання телекомунікаційних послуг на критично важливі об'єкти інфраструктури *(ч. 3)*.[1]	

Стаття 361 (Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж).

Підслідність – органи досудового розслідування Національної поліції.	
Класифікація кримінального правопорушення – *особливо тяжкий.*	При наявності кваліфікаційних ознак, передбачених *ч. 4 та ч. 5.*
Об'єкт – суспільні відносини, що порушують формування та використання автоматизованих інформаційних систем та ресурсів, а також засобів їх забезпечення (безпека у кіберпросторі особи, суспільства та держави).	Об'єктом несанкціонованого доступу до ІТ інформації є права на інформацію її власника та третіх осіб. Додатковим об'єктом виступає життя та здоров'я людей, екологічна безпека, безпека громадян та національна безпека загалом. *Сфера дії статті* – невизначене коло фізичних та юридичних осіб, а також держава у ІТ сфері.
Об'єктивна сторона – будь-який спосіб несанкціонованого доступу,	Кримінальне правопорушення вважається *закінченим* з моменту настання хоча б

Припинення надання телекомунікаційних послуг означає неможливість протягом певного періоду використовувати лінії і засоби електронного телекомунікаційного зв'язку за їх цільовим призначенням, тобто для передачі та прийому інформації від оператора до користувача.

[1] У цій статті *майнова шкода* визнається заподіяною у великому розмірі, якщо її розмір у тисячу і більше разів перевищує неоподатковуваний мінімум доходів громадян.

знищення, блокування, модифікації та копіювання інформації, а також порушення роботи комп'ютерів, їх систем чи мереж.	одного із наслідків передбачених диспозицією статті. *Склад – матеріальний*
Суб'єктивна сторона – прямий або непрямий умисел.	*Мотив та мета* – на кваліфікацію не впливають, але можуть враховуватися при визначенні розміру та виду покарання.
Суб'єкт – загальний; в окремих випадках – спеціальний *(ч. 3).*	
Кваліфікований склад правопорушення полягає у тому, що дії передбачені ч. 1, якщо вони вчинені повторно або за попередньою змовою групою осіб *(ч. 2)*, якщо вони призвели до витоку втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації *(ч. 3)*, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків *(ч. 4),* якщо дії передбачені ч. 3 та ч. 4 були вчинені під час воєнного стану *(ч. 5).*	

Стаття 411 (Умисне знищення або пошкодження військового майна).

Підслідність – слідчих органів Державного бюро розслідувань.	
Класифікація кримінального правопорушення – *тяжкий.*	При наявності кваліфікаційних ознак, передбачених *ч. 4.*
Об'єкт – порядок застосування та використання військового майна, що становить матеріальну основу для боєготовності та боєздатності Збройних Сил України. *Предмет умисного знищення або пошкодження військового майна* – зброя, боєприпаси, військова техніка, інше майно, що знаходиться у військовій власності.	*Суспільна небезпека* полягає у тому, що вчинення цього діяння негативно впливає, а отже знижує, боєздатність та боєготовність Збройних Сил України. *Сфера дії статті* – місця дислокації військових підрозділів України.
Об'єктивна сторона – знищення чи/або пошкодження майна, що знаходиться у військовій власності.	Кримінальне правопорушення вважається закінченим з моменту вчинення дій, передбачених у диспозиції *(ч. 1);* якщо дії вчинені шляхом підпалу або іншим загальнонебезпечним способом, або якщо вони спричинили загибель людей чи інші тяжкі наслідки *(ч. 2);* якщо дії передбачені частинами 1 та 2 вчинені в умовах особливого періоду (крім воєнного стану) *(ч. 3);* якщо дії передбачені частинами 1 та 2 вчинені в умовах воєнного стану або в бойовій обстановці *(ч. 4).* *Склад – матеріальний.*

Суб'єктивна сторона – *прямий умисел*, можлива змішана (подвійна) форма вини *(ч. 2)*.	Винний *усвідомлює* суспільно небезпечний характер свого діяння та бажає цього. *Мотиви* – невдоволення умовами служби, дій командирів чи/або товаришів по службі. *Мета* – бажання знищити або пошкодити військове майно з метою, наприклад, припинення його робочого стану, ведення військових дій, або помсти будь-кому тощо.
Суб'єкт – спеціальний.	Ним може бути будь-який військовослужбовець.
Кваліфікаційні склад правопорушення полягає у вчиненні діяння, передбаченого частиною першою загальнонебезпечним способом, або якщо ці дії спричинили загибель людей чи інші тяжкі наслідки *(ч. 2)*, або якщо вони вчиненні в особливий період *(ч. 3)*, та якщо вони вчинені під час воєнного стану чи в бойовій обстановці *(ч. 4)*.[1]	

Стаття 438 (Порушення законів та звичаїв війни).

Підслідність – слідчі органи Служби безпеки України.	
Класифікація кримінального правопорушення – особливо тяжкий.	
Об'єкт – встановлені міжнародними угодами (договорами) правила, що забезпечують мінімальний обсяг шкоди, заподіяної в умовах збройного конфлікту (людських жертв, матеріальних збитків, знищення історико-культурної спадщини та іншої цивільної або життєво важливої інфраструктури тощо).	*Суспільна небезпека* цього діяння полягає у реальній загрозі масового знищення людей, тваринного чи рослинного світу на загальнодержавному, регіональному чи місцевому рівні, а також заподіянні моральної та/або матеріальної шкоди в наслідок використання збройних засобів та методів ведення війни. *Сфера дії статті* – має міжнародний характер, тобто, як мінімум торкається інтересів декількох держав (дві і більше).
Об'єктивна сторона – жорстоке	*Диспозиція* – бланкетна.

[1] Під *тяжкими наслідками* слід розуміти знищення або пошкодження дорогого військового обладнання, великої кількості техніки, зброї чи боєприпасів, заподіяння майнової шкоди у великому розмірі, зниження бойової спроможності підрозділу, у тому числі, знищення або пошкодження об'єктів критичної інфраструктури військового призначення тощо.

Воєнний стан – це особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню та органам місцевого самоврядування повноважень, необхідних для відвернення загрози та забезпечення національної безпеки, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень.

Бойова обстановка – стан військових частин, підрозділів (кораблів, літаків) під час здійснення ними тактичних дій по виконанню бойових завдань в обмеженому районі протягом короткого часу.

Особливий період – період, що настає з моменту оголошення рішення про мобілізацію (крім цільової) або доведення його до виконавців стосовно прихованої мобілізації чи з моменту введення воєнного стану в Україні або в окремих її місцевостях та охоплює час мобілізації, воєнний час і частково відбудовний період після закінчення воєнних дій.

Під *іншим загальнонебезпечним способом* мається на увазі наприклад, вчинення вибуху, затоплення, чи організація катастрофи, застосування отруйних речовин, забруднення приміщень небезпечними відходами, а також вчинення інших дій, які несуть небезпеку для життя чи здоров'я оточуючого середовища.

поводження з військовополоненими чи цивільним населенням (комбатантами та некомбатантами), депортація цивільного населення, розграбування національної спадщини та мародерство на окупованих територіях, застосування засобів та методів заборонених міжнародними нормативно-правовими актами, у тому числі зброї масового знищення тощо.	*Перелік заборонених засобів та методів* ведення війни є відкритим на визначений міжнародними нормативно-правовими актами гуманітарного права. Правопорушення вважається закінченим з моменту вчинення будь-якого діяння, визначеного в диспозиції статті. *Настання наслідків* хоча і передбачене, але на кваліфікацію не впливає. *Склад – формальний.*
Суб'єктивна сторона – *прямий умисел.*	*Мотиви* не мають значення для кваліфікації, але враховуються при призначенні покарання (користь, фанатизм, помста за померлих тощо) Передбачення фактичної величини збитків не конкретизовано.
Суб'єкт – *спеціальний.*	Ним може бути лише комбатант (військовослужбовець), як особа, яка віддає неправомірний наказ, що порушує закони і звичаї війни, так і виконавець цього наказу.
Кваліфікаційні склад кримінального правопорушення полягає у вчиненні діяння, поєднаного з умисним вбивством *(ч. 2).*	

Стаття 441 (Екоцид).

Підслідність – слідчі органи Служби безпеки України.	
Класифікація кримінального правопорушення – особливо тяжкий.	
Об'єкт – суспільні відносини, що забезпечують охорону та безпеку навколишнього середовища (флори і фауни). *Предмет екоциду* – рослинний та тваринний світ, водні ресурси, земля, космічний простір та інші компоненти екосистеми.	*Суспільна небезпека* полягає у діянні, що створює загрозу або реально спричиняє шкоду екології та створює екологічну катастрофу, що, як наслідок, негативно впливає на соціально-економічний розвиток суспільства та держави, а також негативно позначається на генофонді населення, тваринного та рослинного світу.[1] *Сфера дії статті* – має міжнародний характер, тобто, як мінімум торкається інтересів декількох держав (дві і більше).
Об'єктивна сторона полягає у масовому знищенні рослинного і тваринного світу, отруєння атмосфери чи водних ресурсів, створення умов, що	Кримінальна відповідальність настає за умов причинно наслідкового зв'язку між діями суб'єкта та настанням негативних наслідків.

[1] У буквальному розумінні екоцид означає вбивство природи. Законом України «Про охорону навколишнього природнього середовища» зазначено, що природа є власністю Українського народу, який має право користуватися нею відповідно в межах визначених Конституцією України та іншими законодавствуймо і підзаконними нормативно-правовими актами.

здатні спричинити екологічну катастрофу.	Правопорушення вважається *закінченим* з моменту настання негативних наслідків, визначених диспозицією статті. Склад – *матеріальний.*
Суб'єктивна сторона характеризується прямим чи опосередкованим (непрямим) умислом.	Винний *усвідомлює* небезпеку своїх дій (бездіяльності), посягаючи на навколишнє середовище, передбачає збитки у вигляді знищення елементів екосистеми та бажає цього (прямий умисел), або передбачає можливість настання шкідливих наслідків в своїй бездіяльності чи вчинення відповідних дій небезпечних для довкілля і байдуже ставиться щодо їх настання (непрямий умисел). *Мотивами* можуть бути недотримання своїх функціональних обов'язків, порушення посадових інструкцій, зловживання владними повноваженнями тощо.
Суб'єкт – *загальний.*	Ними можуть бути посадові особи органів та установ, які забезпечують безпеку навколишнього середовища України.

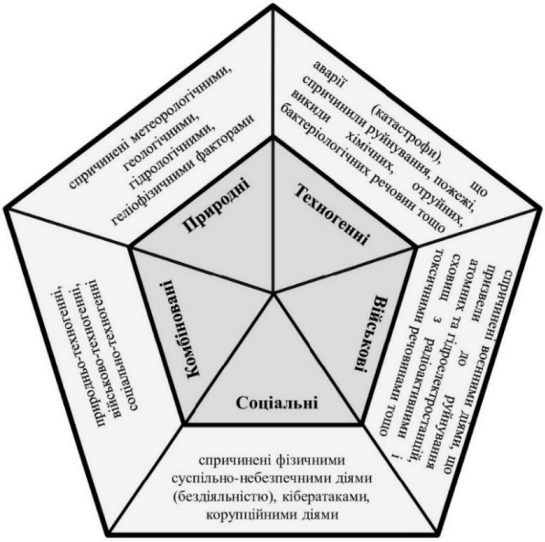
§ 4. Організація діяльності слідчо-оперативної групи під час розслідувань посягань на об'єкти критичної інфраструктури

До основних загроз безпеки критичної інфраструктури відносяться негативні фактори впливу, що були спровоковані потенційними небезпеками природнього, техногенного, соціального, військового та/або комбінованого характеру (див. рис. 3).

У свою чергу, соціальні небезпеки поділяються, по-перше, на фізичні загрози – потенційні небезпеки, які спричинили на об'єкті критичної інфраструктури виникнення кризової ситуації у результаті вчинення диверсійних дій, терористичних актів, викрадення, навмисного знищення та/або пошкодження майна необхідного для їх функціонування тощо. По-друге, кіберзагрози – потенційні небезпеки, які порушили належне функціонування інформаційно-телекомунікаційних систем об'єкту критичної інфраструктури, що в результаті призвело до виникнення позаштатної ситуації, та по-третє, корупційні загрози – потенційні небезпеки, які порушили належне функціонування об'єкту критичної інфраструктури унаслідок вчинення корупційних дій.

Рисунок 3.

На рисунку схематично зображена класифікація потенційних небезпек, які впливають на функціонування критичної інфраструктури



Розглядаючи організацію діяльності слідчо-оперативної групи під час розслідування кримінальних посягань на об'єкти критичної інфраструктури спровокованих фізичними небезпеками, можна виокремити три взаємопов'язаних етапи.

Перший етап. Інформування уповноважених органів у сфері захисту критичної інфраструктури про виникнення на об'єкті критичної інфраструктури надзвичайної ситуації, з метою подальшого проведення невідкладних дій щодо ліквідації її наслідків.

Після виникнення позаштатної ситуації на об'єкті критичної інфраструктури, оператор критичної інфраструктури повинен невідкладно повідомити про це відповідні секторальні та функціональні органи у сфері захисту критичної інфраструктури, а також місцеві органи виконавчої влади та військово-цивільну адміністрацію у разі її утворення. Інформація у повідомленні має містити дані про час та місце події, її обставини, наслідки, передбачену або вже відому причину, організацію надання медичної допомоги постраждалим особам, їх число, орієнтовну кількість жертв тощо.

Організація аварійно-рятувальних робіт повинна проводитися невідкладно з одночасним вжиттям заходів щодо обмеження доступу до місця події сторонніх осіб. Місце події, обов'язково має бути оціненим щодо ймовірного розташування на його території потенційно небезпечних предметів. Це дозволить забезпечити безпеку осіб, які беруть участь у ліквідації наслідків надзвичайної ситуації та проведенні процесуальних дій.

Враховується й комплекс небезпечних факторів, які виникають після вибуху чи пожежі, шляхом визначення небезпечної та аварійної зони . Знаходження людей в межах «небезпечної зони» та проведення в ній будь-яких робіт забороняється.

Ліквідація наслідків надзвичайної ситуації проводиться лише після остаточного усунення небезпечних чинників у зоні проведення аварійно-рятувальних робіт. Якщо є інформація про можливе радіаційне, хімічне або бактеріологічне (біологічного) зараження навколишнього середовища, проведення робіт повинне відбуватися за участю кваліфікованих фахівців у відповідній галузі знань з дотриманням усіх існуючих об'єктових чи відомчих інструкцій.

Другий етап: Організація охорони місця події та залучення до його проведення необхідних учасників.

Отримавши повідомлення про виникнення на об'єкті критичної інфраструктури надзвичайної ситуації, на місце події, терміново направляється відповідна слідчо-оперативна група. Залежно від характеру надзвичайної ситуації та категорії критичності об'єкта, на місце події, можуть прибувати представники різних правоохоронних органів, що ускладнює процес прийняття уповноваженими суб'єктами національної системи захисту критичної інфраструктури оперативних рішень. Тому, наразі залишається відкритим питання щодо нормативно врегулювали формування та діяльності постійно діючих відомчих та міжвідомчих слідчо-оперативних груп з розслідування кримінальних правопорушень об'єктами яких є критична інфраструктура. У подальшому, це надавсь можливість організовувати та проводити спільні навчання для відпрацювання схеми оповіщення, системи негайного виїзду та координації дій кожного із її удачників на місці події.

До складу такої слідчо-оперативної групи мають входити прокурор, слідчий (група слідчих), спеціаліст-криміналіст та працівники відповідних оперативних підрозділів залежно від підслідності

кримінального правопорушення. У випадках коли порушення функціонування об'єктів критичної інфраструктури було спричинено вибухом, до проведення огляду долучається спеціаліст-вибухотехнік відповідної експертної служби. Також, можуть залучатися й фахівці піротехнічних підрозділів Державної служби з надзвичайних ситуацій, проте, необхідно враховувати відсутність у них практичних навичок щодо виявлення, фіксації та вилучення об'єктів, які мають криміналістичне значення. Під час виявлення на місці події загиблих, до проведення огляду долучається спеціаліст в галузі судової медицини. Залежно від обставин та кількості жертв, до участі в огляді доцільно залучати лікарів швидкої медичної допомоги та психологів. У разі необхідності використання службово-розшукових собак, до проведення огляду запрошуються спеціалісти-кінологи. Компетентну допомогу можуть надати й працівники об'єкту критичної інфраструктури, яким відомі його конструктивні особливості.

Перед початком огляду, кожен із учасників СОГ, має бути забезпечений спеціальними засобами індивідуального захисту (респіраторами, касками, рукавичками, комбінезонами тощо) та необхідним технічним обладнанням для його проведення (фото- та відеокамери, дозиметри, далекоміри тощо). З метою полегшення процесу пізнання до огляду доцільно залучати спеціаліста-оператора безпілотного літального апарату, що надасть можливість учасникам огляду проаналізувати місце події зверху вниз та краще змоделювати обставини події. Окрім цього, використання БпЛА значно пришвидшить проведення огляду, що позитивно вплине на час проведення відновлювальних робіт. Не порушуючи принципу єдиноначальності, залежно від обсягу проведення необхідної роботи, у складі слідчо-оперативної групи також рекомендується організаційно виокремити відповідні підгрупи слідчих, спеціалістів та оперативних працівників, а також окрему групу, яка б забезпечувала безпеку на місці події та здійснювала комунікацію із засобами масової інформації.

Третій етап: Проведення огляду місця події.

У кримінальних провадженнях об'єктами яких є критична інфраструктура огляд місця події є однією з найбільш складних і важливих слідчих (розшукових) дій з чітко вираженою специфікою його проведення. Зволікання з оглядом неминуче веде до втрати доказів і зміни первинної обстановки в силу нестійкості окремих слідів і умов, в результаті яких сталася ця подія. Поряд з цим, важливість

функціонування об'єктів критичної інфраструктури вимагає якнайшвидшої ліквідації наслідків надзвичайної ситуації. Тому, з прибуттям на місце події слідчо-оперативної групи, аварійно-рятувальні роботи можуть бути ще незавершені. На цьому етапі усі зусилля мають бути скоординовані на ретельну відео- та фотофіксацію тієї обстановки, яка спостерігається на момент прибуття.

За умов якщо багато криміналістично значущих слідів можуть буди втрачені, огляд доцільно проводити паралельно з аварійно-рятувальними роботами. За можливістю слідчому необхідно відразу скоординувати свої дії так, щоб забезпечити збереження криміналістично значимих слідів розташованих поруч з проведенням відновлювальних робіт. Насамперед, мають бути оглянуті ті об'єкти, які потребують негайного відновлення чи евакуації.

Прибувши на місце події, учасникам слідчо-оперативної групи необхідно оцінити ступінь та масштаби надзвичайної ситуації, а також наявність та кількість постраждалих осіб. Якщо на місці події є постраждалі, необхідно з'ясувати, чи надавалася їм допомога та за необхідності вжити невідкладних заходів для її надання. Після чого, проводяться заходи щодо охорони місця події, її посилання та за необхідності розширення.

Перед початком огляду має бути забезпечена безпека осіб, які беруть у ньому участь. Вживаються усі необхідні заходи щодо унеможливлення появи на місці події сторонніх осіб, у тому числі, в «небезпечній зоні». Слідчо-оперативна група також знаходиться поза її межами. Учасники групи мають бути проінструктовані щодо дотримання заходів особистої безпеки. Якщо є небезпека вибуху, огляд не розпочинається без залучення до його проведення відповідних спеціалістів вибухотехнічної служби. З виявленням на місця події вибухових пристроїв чи нерозірваних боєприпасів, керівник групи спільно з відповідним фахівцем, приймають рішення щодо їх знешкодження на місці події або поза її межами. Знешкодження вибухонебезпечних предметів здійснює кваліфікованим фахівцем з дотриманням усіх існуючих правил та інструкцій для виконання подібних робіт.

У зв'язку з можливими масштабними руйнуваннями та великою кількістю об'єктів, які мають бути оглянуті, збільшується час проведення огляду, а іноді навіть до декількох тижнів. У такому разі територія місця події розбивається на менші ділянки, огляд яких

доручається конкретному слідчому цієї групи. Взаємодія слідчого з іншими учасниками огляду має бути організована таким чином, щоб він мав можливість постійно підтримувати комунікацію з ними. Слідчому також потрібно враховувати й те, що на місці події, паралельно може проводити службове розслідування відповідна (відомча) комісія. Предметом службового розслідування є матеріальна обстановка на місці поді, виявлення свідків, збереження необхідної документації та слідів, які можуть бути пошкоджені чи/або знищені, складання схем, наявних пошкоджень чи руйнувань, актів огляду, здійснення фото- та відеофіксації. Тобто, завдання процесуального розслідування схожі із завданнями службового розслідуванням. Тому, слідчому необхідно ознайомитися із функціональними обов'язки голови цієї комісії та її складом. Результати службового розслідування можуть слугувати як допоміжні матеріали для планування та проведення подальших процесуальних дій.

Окрема увага в ході проведення огляду звертається на місця руйнувань чи пошкоджень об'єктів критичної інфраструктури їх систем та елементів, а також знаходження в їх межах сторонніх предметів. У випадку якщо їх складно описати, до протоколу долучаються схеми, плани, фотозображення, а при їх протоколюванні запрошуються компетентні працівники. У випадку виявлення на місці події особливо небезпечних об'єктів (ядерних, хімічних, термобаричних боєприпасів тощо) проведення огляду негайно зупиняється до прибуття відповідних фахівців. Якщо об'єкт повністю знищений та являє собою купу будівельного сміття, необхідно провести його розбирання, попередньо оглядаючи знищені фрагменти.

Одночасно з оглядом доцільно проводити й інші слідчі (розшукові) дій. Оперативним працівникам доручається встановлення очевидців та потерпілих, організація охорони місця події та слідів, що не були оглянуті, збирання відомостей про осіб, які опинилися в межах події, збереження технічної документації, що характеризує діяльність об'єкта критичної інфраструктури та від якої залежить належне функціонування об'єкту критичної інфраструктури, допомога у проведенні рятувальних робіт тощо.

§ 5. Особливості проведення окремих процесуальних дій під час розслідування посягань на об'єкти критична інфраструктура

Допит. При підготовці до проведення допитів потерпілих чи свідків необхідно враховувати психоемоційний стан допитуваних осіб. Тактика проведення допитів у переважній більшості відбувається з урахуванням загальних рекомендацій, розроблених криміналістичною наукою. Водночас, очевидцями кримінального правопорушення на об'єкті критичної інфраструктури здебільшого є його працівники, які можуть бути не свідками, а потерпілими. У цьому разі, мають бути поставлені питання щодо технологічного чи виробничого процесу на об'єкті, особливості його функціонування та експлуатації тощо. Наприклад:

(а) які функції виконував допитаний до, під час і після надзвичайної ситуації;

(б) якими інструкціями або іншими нормативно-правовими документами регламентується його діяльність;

(в) яка робоча зміна працювала на момент виникнення надзвичайної ситуації;

(г) яким чином забезпечувалась безпека об'єкта;

(ґ) хто із працівників володів знаннями, які могли бути використані для підготовки і реалізації кримінального правопорушення;

(д) що було пошкоджено в результаті вчинення кримінального правопорушення;

(е) що було пошкоджено в результаті проведення аварійно-рятувальних робіт;

(є) які предмети і документи зникли чи з'явилися до, під час або після виникнення надзвичайної ситуації.

Особливості допитів у кримінальних провадженнях, де об'єктами злочинних посягань є критична інфраструктура, передусім проявляються в змісті специфічних питань, які слідчий задає допитуваним. У цьому контексті, до процесу допиту доцільно залучати кваліфікованих спеціалістів. Не слід також ігнорувати й ті обставини, що допитуваними особами вже надавалися пояснення в межах службового розслідування.

У ході проведення допитів акцентується увага й на встановленні

обставин кримінального правопорушення. У цьому випадку необхідно з'ясувати, чи не зверталася увага допитуваних на підозрілих осіб, чим саме ці особи звернули їхню увагу, їх прикмети, маршрут пересування тощо.

Під час підготовки до проведення допиту підозрюваного потрібно враховувати можливу його схильність до психічних або поведінкових розладів. Тому, перед початком допиту береться до уваги психічний стан підозрюваного, його біографічні данні та враховується його свідоме ставлення до вчиненого кримінального правопорушення. Мається на увазі, наприклад, чи усвідомлював він важливість об'єкта критичної інфраструктури для життєдіяльності держави, регіону, міста, населення тощо.

У разі потреби беруться до уваги матеріали службового розслідування, огляду місця події, або вилучені відеозаписи з камер спостереження. Ця інформація може містити дані про спосіб вчинення кримінального правопорушення, його співучасників, а також роль та функції кожного із них. Також вона може бути використана в якості тактичних прийомів проведення допиту, наприклад:

(1) поступове пред'явлення доказів вини підозрюваного від менш переконливого до більш вагомого;

(2) несподіване пред'явлення самого значного доказу;

(3) тримання в постійній напрузі підозрюваного, натякаючи на те, що слідству відомо факти його причетності до кримінального правопорушення або затримано його співучасників;

(4) замовчування до певного часу відомих фактів, а потім несподіване їх пред'явлення;

(5) застосування певної послідовності питань, пред'явлення доказів, показань інших осіб;

(6) використання прийомів, що активізують емоційні переживання підозрюваного (встановлення психологічного контакту з привернення позитивного іміджу до співрозмовника);

(7) демонстрація науково-технічних можливостей встановлення обставин, незалежно від показань допитуваного.

Загалом тактика допиту підозрюваного залежить від позиції допитуваного та обставин події. В ході допиту підлягають з'ясуванню такі обставини як:

(а) коли, за яких обставин, з ким і з якою метою він опинився на місці події;

(б) хто може підтвердити його свідчення;

(в) коли, з ким і за яких обставин було вчинено ним кримінальне правопорушення;

(г) яка роль і функції кожного із учасників групи на стадіях підготовки, вчинення і приховання кримінального правопорушення;

(ґ) які були дії кожного із учасників кримінального правопорушення після його вчинення;

(д) яку мету та мотиви учасники групи переслідували під час підготовки, вчинення і приховання кримінального правопорушення.

Якщо мета допиту полягає у з'ясуванні причин вибуху чи, наприклад, послідовності виготовлення вибухових пристроїв, то для участі у його проведенні доцільно запрошувати спеціаліста у відповідній галузі знань.

Підозрювані, у яких при обшуку були виявлені вибухові речовини, пристрої або їх частини, зазвичай посилаються на те, що вказані предмети опинилися у них випадково, або призначалися для інших цілей. У зв'язку з цим, слідчому важливо правильно обрати необхідну тактику допиту. Загальноприйнятою рекомендацією щодо допиту підозрюваного є спочатку встановлення фактів, що відносяться до об'єктивної сторони кримінального правопорушення, а потім тих, які стосуються суб'єктивної сторони кримінального правопорушення (намір, мета, мотив тощо).

Огляд документів. Поряд з оглядом місця події слідчий проводить виїмку і огляд документів, а саме: технічної документації, що відноситься до виконання тих чи інших видів робіт, документів про технічний стан устаткування, документів, що характеризують організацію робіт, документів, що свідчать про підготовку потерпілого і підозрюваного в галузі техніки безпеки та їх кваліфікації, документів, що відображають стан безпеки та стійкості об'єкта критичної інфраструктури тощо.

Вилучення і огляд документів проводиться за участю фахівців, з урахуванням забезпечення безперервності виробничого процесу. Мається на увазі те, що оперативна документація від якої залежить належне функціонування об'єкта критичної інфраструктури не вилучається, а у випадку необхідності її отримання з неї робляться засвідчені копії.

При огляді технічних проектів, описів технологічних процесів, технологічних карт, посадових інструкцій і подібних матеріалів

звертається увага не тільки на їх ведення, а й на факт наявності необхідних підписів, печаток відповідних посадових осіб, дотримання необхідного порядку їх узгодження з відповідними органами тощо.

Під час огляду графіків ремонтних робіт обладнання фіксуються зазначені в них терміни і характер їх проведення. Якщо в документації відображаються ті чи інші дії конкретних осіб по виконанню покладених на них обов'язків (наприклад, вахтові журнали механізмів, журнали реєстрації інструктажів з техніки безпеки), то ретельно досліджуються зміст записів, повнота відображення проведених заходів, наявність дат і підписів відповідальних осіб.

Під час проведення огляду свідоцтв та посвідчень на право керування механізмами або проведення певних робіт, досліджуються реквізити цих документів, звертається увага на термін їх дії. При виникненні сумнівів в достовірності записів вони можуть зіставлятися з іншою документацією, що відображає супутні факти, а за необхідності – експертно досліджуватися.

Затримання, обшук. Затримання підозрюваного здійснюються невідкладно за правилами визначними кримінальним процесуальним законодавством України. Після затримання підозрюваного, уповноважена службова особа повинна здійснити його особистий обшук та огляд його речей з дотриманням правил, передбачених КПК України.

Оглядаючи руки, інші частини тіла чи одягу підозрюваного можливо виявити сліди кіптяви, які можуть вказати на вид вибухової речовини, а також інші сліди, що свідчать про перебування підозрюваного на місці вчинення кримінального правопорушення.

Усі дії учасників огляду детально фіксуються у відповідному протоколі. У разі необхідності, особистий одяг та взуття підозрюваного вилучаються і направляються для окремого експертного дослідження. Окрім цього, криміналістично значима інформацію може міститись й у особистих речах підозрюваного, які були при ньому під час затримання. Як приклад, такими речами є мобільний телефон. За необхідності можливо провести огляд ділянки місцевості, де було затримано підозрювану особу.

Докази, які були отримані в результаті проведення досудового розслідування, надають підстави для подальшої організації та проведення обшуків підозрюваного за місцем його проживання, реєстрації, роботи тощо. Під час проведення цієї слідчої (розшукової)

дії необхідно звертати увагу на фактичні дані, що можуть вказувати на причетність підозрюваного до вчиненого кримінально правопорушення. Ці данні можуть міститись у електронних листуваннях, фотографіях, відеозаписах, соціальних мережах тощо. Тому, при підготовці до обшуку слідчий має заздалегідь визначитись з колом учасників, які будуть приймати у ньому участь.

З метою встановлення причетності підозрюваного до виготовлення вибухових пристроїв, під час обшуку, з підлоги чи меблів, що знаходяться у приміщені вилучаються фрагменти пилу. Також сліди вибухових речовин можуть зберігатися на інструментах чи одязі підозрюваного.

Для пошуку металевих предметів доцільно використовувати металошукачі. Важливі речові докази можуть бути закопані на присадибних ділянках або знаходиться у приміщеннях для господарського користування. При виявленні вибухових пристроїв або схожих на них предметів обшук призупиняється, а його учасники евакуюються у безпечне місце до прибуття відповідних фахівців.

§ 6. Особливості проведення окремих експертних досліджень під час розслідування посягань на об'єкти критична інфраструктура

Проведення експертиз. Досудове розслідування кримінальних правопорушень, що посягають на об'єкти критичної інфраструктури, зумовлене проведенням різних видів експертних досліджень. Зокрема, до останніх відносяться традиційні криміналістичні, інженерно-технічні, економічні, судово-медичні та судово-психіатричні експертизи. Наприклад, предметом судової вибухотехнічної експертизи та експертизи вибухових речовин є встановлення фактичних обставин вибуху на об'єкті критичної інфраструктури, приналежність досліджуваних речовин і виробів до певного класу, оцінка їх вражаючої дії, а також встановлення рівня спеціальних знань у осіб, що їх виготовили. У проведенні цієї експертизи беруть участь експерти з різних галузей знань та спеціальностей (фізики, хіміки, технологи), тому вона є комплексною.

Окрім цього, об'єктами вибухотехнічної експертизи та експертизи вибухових речовин є фрагменти вибухових пристроїв, вибухові речовини, боєприпаси, саморобні вибухові пристрої, сліди вибуху тощо.

При виявленні на місці події зазначених об'єктів та їх направлення на експертне дослідження слідчому необхідно знати, що:

(1) до експертної установи направляються лише заздалегідь знешкоджені вибухонебезпечні предмети, які упаковуються в прозорі полімерні пакети. У іншому випадку, ці об'єкти безпосередньо після їх виявлення знешкоджуються. Тимчасово для зберігання цих об'єктів можуть використовуватися дерев'яні бліндажі з піском, або інші спеціальні контейнери (сейфи);

(2) детонатори (електродетонатор) направляються в упаковках виготовлених з діелектричних матеріалів (картон, пінопласт, полімер), оголені дроти електродетонаторів необхідно герметизувати ізоляційною стрічкою;

(3) транспортування вибухонебезпечних об'єктів відбувається окремо у невеликій кількості у спеціальних контейнерах у супроводі уповноважених працівників;

(4) продукти вибуху вибухових речовин мають властивість випаровуватися, тому вини повинні зберігатися у герметичній упаковці і направлятися на експертне дослідження не пізніше ніж через дві доби після вибуху.

Перед експертом можуть бути поставлені питання, що відносяться до підготовки і процесу вибуху, вибухового пристрою, вибухових речовин, наслідків вибуху тощо.

Також, можуть призначатися трасологічні, матеріалознавчі, біологічні, почеркознавчі, авторознавчі, фоноскопічні та інші експертизи. Наприклад, на деталях вибухових пристроїв можуть бути виявлені сліди пальців залишені підозрюваним, а на місці події – сліди підошви його взуття.

Якщо в результаті виникнення надзвичайної ситуації на об'єкті критичної інфраструктури є постраждалі чи загиблі особи, слідчий призначає судово-медичну експертизу, на вирішення якої можуть бути поставлені питання про причину смерті, час її настання, механізм заподіяння і тяжкість тілесних ушкоджень. Залежно від конкретних обставин вчинення кримінального правопорушення, експерту можуть бути поставлені також питання про те, чи не перебував потерпілий на момент смерті в стані алкогольного сп'яніння, чи не було у нього медичних протипоказань до виконання певних видів робіт, чи могли наявні у потерпілого тілесні ушкодження виникнути при обставинах, зазначених потерпілим тощо.

При відпрацюванні версій щодо порушення на об'єкті критичної інфраструктури інструкцій з охорони праці призначається судово-технічна експертиза. Здебільшого, на її розгляд ставляться питання про причини нещасного випадку, чи мало місце порушення правил безпеки або інших правил охорони праці та яких саме, хто відповідальний за їх дотримання, чи є з технічної точки зору причинний зв'язок між порушеннями і наслідками тощо.

Якщо кримінальне провадження відкрите за фактом порушення правил безпеки, в результаті яких була створена лише загроза загибелі людини або настання інших тяжких наслідків, передбачених законом, перед експертом можуть бути поставлені питання про ступінь ймовірності настання цих наслідків та розвиток подальших подій. За необхідності можуть ставитися й інші питання, зумовлені конкретними обставинами розслідування, наприклад, про механізм події, про відповідність технологічним процесам, виробничим операціям або окремим діям працівника підприємства, про умови, що сприяли вчиненню кримінального правопорушення тощо. За необхідності отримання фахової консультативної допомоги до проведення експертних досліджень також доцільно залучати представників секторальних та функціональних органів фізичного захисту об'єкту критичної інфраструктури, на якому сталася надзвичайна подія.

У справах про кримінальні правопорушення проти безпеки виробництва можуть проводитися й інші види експертних досліджень. Так, наприклад, для виявлення підробок в документах, встановлення виконавця записів або підписів від імені певних осіб, призначаються техніко-криміналістичні експертизи документів та почеркознавчі експертизи. Для встановлення механізму і технічних причин пошкодження деталей і вузлів агрегатів проводиться металознавча експертиза металів і сплавів. З метою встановлення механізму утворення слідів, ідентифікації знарядь (наприклад, робочого інструменту використаного постраждалим) по слідах на оброблених деталях проводяться трасологічні дослідження тощо.

Перелік рекомендованих джерел:

Нормативно-правові акти:

1. Деякі питання об’єктів критичної інфраструктури. Постанова Кабінету міністрів України від 09.10.2020 № 1109. Верховна Рада України. URL: https://zakon.rada.gov.ua;
2. Договір про захист художніх і наукових закладів та історичних пам'яток (Пакт Реріха) від 1935 року. Верховна Рада України. URL: https://zakon.rada.gov.ua;
3. Другий протокол до Гаазької конвенції про захист культурних цінностей у разі збройного конфлікту 1954 року. Верховна Рада України. URL: https://zakon.rada.gov.ua;
4. Європейська конвенція з прав людини від 1950 року. Верховна Рада України. URL: https://zakon.rada.gov.ua;
5. Звід принципів захисту всіх осіб, які підлягають затриманню або ув’язненню у будь-якій формі, затвердженому Резолюцією 43/173 Генеральної Асамблеї ООН від 09.12.1988 року. URL: https://zakon.cc;
6. Інструкція з організації діяльності слідчих підрозділів Національної поліції України. Наказ МВС України від 06.07.2017 № 570. Верховна Рада України. URL: https://zakon.rada.gov.ua;
7. Інструкція про призначення та проведення судових експертиз та експертних досліджень. Наказ Міністерства юстиції України від 08.10.1998 № 53/5. Верховна Рада України. URL: https://zakon.rada.gov.ua;
8. Кодекс цивільного захисту України. Закон України від 02.10.2012 № 5403-VI. Верховна Рада України. URL: https://zakon.rada.gov.ua;
9. Конвенція про захист воєнного або будь-якого іншого ворожого використання засобів вплину на природнє середовище. Верховна Рада України. URL: https://zakon.rada.gov.ua;
10. Конвенція про захист цивільного населення під час війни від 1949 року. Верховна Рада України. URL: https://zakon.rada.gov.ua;
11. Конституція України. Закон України від 26.06.1996. Верховна Рада України. URL: https://zakon.rada.gov.ua;
12. Кримінальний кодекс України. Закон України від 05.04.2001 № 2341-III. Верховна Рада України. URL: https://zakon.rada.gov.ua;
13. Кримінальний процесуальний кодекс України. Закон України від 13.04.2012 № 4651-VI-III. Верховна Рада України. URL: https://zakon.rada.gov.ua;

14. Кримінально-виконавчий кодекс України. Закон України від 11.11.2003 № 1129-IV. Верховна Рада України. URL: https://zakon.rada.gov.ua;

15. Положення про Єдиний державний вебпортал електронних послуг. Постанова Кабінету Міністрів України від 04.12.2019 № 1137. Верховна Рада України. URL: https://zakon.rada.gov.ua;

16. Положення про єдину державну систему цивільного захисту. Постанова Кабінету Міністрів України від 09.01.2014 № 11. Верховна Рада України. URL: https://zakon.rada.gov.ua;

17. Про адміністративні послуги. Закон України від 06.09.2012 № 5203-VI. Верховна Рада України. URL: https://zakon.rada.gov.ua;

18. Про вивезення, ввезення та повернення культурних цінностей. Закон України від 21.09.1999 № 1068-XIV. Верховна Рада України. URL: https://zakon.rada.gov.ua;

19. Про державну службу спеціального зв'язку та захисту інформації України. Закон України від 23.02.2006 № 3475-IV. Верховна Рада України. URL: https://zakon.rada.gov.ua;

20. Про затвердження Інструкції з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України. Наказ МВС України від 27.04.2020 № 357. Верховна Рада України. URL: https://zakon.rada.gov.ua;

21. Про затвердження категорій об'єктів державної форми власності та сфер державного регулювання, які підлягають охороні органами поліції охорони на договірних засадах. Постанова Кабінету Міністрів України від 21.11.2018 № 975. Верховна Рада України. URL: https://zakon.rada.gov.ua;

22. Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави. Постанова Кабінету Міністрів України від 04.03.2015 № 83. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

23. 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 від 04.07.2018 № 575. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

24. Про затвердження переліку особливо важливих об'єктів нафтогазової галузі. Розпорядження Кабінету Міністрів України від 27.05.2009 № 578-р. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

25. Про затвердження порядку класифікації надзвичайних ситуацій за їх рівнем. Постанова Кабінету Міністрів України від 24.03.2004 № 368. Верховна Рада України URL: https://zakon.rada.gov.ua;

26. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Постанова Кабінету Міністрів України від 23.08.2016 № 563. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

27. Про інформацію. Закон України від 02.10.1992 № 2657-XII. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

28. Про космічну діяльність. Закон України від 15.11.1996 № 502/96-ВР. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

29. Про критичну інфраструктуру. Закон України від 16.11.2021 № 1882-IX. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

30. Про наукову і науково-технічну діяльність. Закон України від 26.11.2015 № 848-VIII. *Верховна Рада України.* URL: https://zakon.rada.gov.ua;

31. Про національну безпеку України. Закон України від 21.06.2018 № 2469-VIII. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

32. Про Національну систему конфіденційного зв'язку. Закон України від 10.01.2002 № 2919-III. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

33. Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури. Рішення Ради національної безпеки і оборони України від 16.02.2017 введене в дію Указом Президента України від 16.02.2017 № 37/2017. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

34. Про об'єкти підвищеної небезпеки. Закон України від 18.01.2001 № 2245-III. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

35. Про оборону України. Закон України від 06.12.1991 № 1932-XII. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

36. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII. *Верховна Рада України.* URL: https://zakon.rada.gov.ua;

37. Про охорону культурної спадщини. Закон України від 08.06.2000 № 1805-III. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

38. Про платіжні послуги. Закон України від 30.06.2021 № 1591-IX. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

39. Про попереднє ув'язнення. Закон України від 30.06.1993 № 3352-XIII. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

40. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». Указ Президента України від 14.09.2020 № 392/2020. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

41. Про систему екстреної допомоги населенню за єдиним телефонним номером 112. Закон України від 13.03.2012 № 4499-VI. *Верховна Рада України.* URL: https://zakon.rada.gov.ua;

42. Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури. Рішення Ради безпеки і оборони України від 29.12.2016 введене в дію Указом Президента України від 16.01.2017 № 8/2017. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

43. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України. Постанова Кабінету Міністрів України від 12.11.2022 № 787. *Верховна Рада України.* URL: https://zakon.rada.gov.ua;

44. Про фінансові послуг та державне регулювання ринків фінансових послуг. Закон України від 12.07.2001 № 2664-III. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

45. Про фінансові послуги та фінансові компанії. Закон України від 14.12.2021 № 1953-IX. Верховна Рада України URL: https://zakon.rada.gov.ua;

46. Рішення Конституційного Суду України у справі за конституційним поданням Верховного Суду України щодо відповідності Конституції України (конституційності) положень частини третьої статті 120, частини шостої статті 234, частини третьої статті 236 Кримінально-процесуального кодексу України (справа про розгляд судом окремих постанов слідчого і прокурора). Рішення Конституційного Суду України Іменем України від 30.01.2003 № 3-рп/2003. *Верховна Рада України*. URL: https://zakon.rada.gov.ua;

47. Стратегія забезпечення державної безпеки. Затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України від 30.12.2021 «Про Стратегію забезпечення державної безпеки» від 16.02.2022 № 56/2022. Верховна Рада України. URL: https://zakon.rada.gov.ua;

48. Стратегія національної безпеки України «Україна у світі, що змінюється». Указ Президента України від 12.02.2007 № 105. Верховна Рада України. URL: https://zakon.rada.gov.ua;

49. Стратегія національної безпеки України. Рішення Ради національної безпеки і оборони України від 06.05.2015 введене в дію Указом Президента України від 26.05.2015 № 287/2015. Офіційний сайт Президента України. URL: https://www.president.gov.ua;

50. Типове положення про функціональну підсистему єдиної державної системи цивільного захисту. Постанова Кабінету Міністрів України від 11.03.2015 № 101. Верховна Рада України. URL: https://zakon.rada.gov.ua;

51. Угода про Асоціацію між Україною з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншою від 30.11.2015. Верховна Рада України. URL: https://zakon.rada.gov.ua.

Науково-методична література:

1. (2020). Investigation of crimes against production safety: Method. rec. / O. Taran, V. Sushchenko, I. Yefimenko and others; in general ed. Doctor of Law, Prof. S. Chernyavskyi. Kyiv: National. Acad. of Internal Affairs, 2020. 110;

2. (2020). Organization of emergency and rescue work: training manual / R. Ratushnyi, V. Loyik, O. Synel′nikov, V. Koval′chuk. Lviv. 394;

3. (2023). Scientific and practical commentary on the Criminal Code of Ukraine / According to general ed. I. Kopotun. Kyiv: «KNT». 932;

4. Alabassi, et al. (2022). A Self-Tuning Cyber-Attacks' Location Identification Approach for Critical Infrastructures. Ieee transactions on industrial informatics. 18 (7). 5018-5027. Doi: 10.1109/TII.2021.3133361;

5. Alcaraz, C. & Sherali, Z. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection. 8, 53-66. Doi: 10.1016/j.ijcip.2014.12.002;

6. Arkhipova, E., & Klevchuk, O. (2021). State regulation in the field of cultural heritage protection of Ukraine. Investments: Practice and Experience, 13(14), 51–57. Doi: 10.32702/2306-6814.2021.13-14.51;

7. Batiuk, O. & Yevtushenko, I. (2022). The importance of the science of forensics in ensuring countermeasures against crimes at critical infrastructure facilities. Honor and law. 2022. 2 (81). 42-47. Doi: 10.33405/2078-7480/2022/2/81/263764;

8. Batiuk, O. (2021). Forensic support for combating crimes at critical infrastructure facilities: Monograph. Lutsk: Volyn Polygraph. 450;

9. Belousov, D. (2023). We consider enemy attacks on critical infrastructure as a component of the crime of genocide. The official portal of the Office of the Prosecutor General. Retrieved from: https://www.gp.gov.ua/ua/posts/yurii-bjelousov-ataki-voroga-na-kriticnu-infrastrukturu-mi-rozglyadajemo-yak-skladovu-zlocinu-genocidu;

10. Biryukov, D. (2015). Protection of critical infrastructure in Ukraine: from scientific understanding to the development of policy principles. Scientific and information bulletin of the Academy of National Security. 3 (4). 155-170;

11. Biryukov, D. & Kondratov, S. (2012). Protection of critical infrastructure: problems and prospects of implementation in Ukraine. Kyiv: National Institute of Strategic Investigations;

12. Chowdhury, N. & Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security: a systematic literature review. Information and computer security. 29 (5). 697-723. Doi: 10.1108/ICS-07-2020-0121;

13. Chumachenko, S., & Trotsko, V. (2017). Assessment of threats to critical infrastructure facilities. Scientific Bulletin: Civil Protection and Fire Safety, 1, 41-47;

14. Chumakova, T. (2022). Current problem issues regarding the qualification of subjects of illegal privatization of state, communal property. Bulletin of Mariupol State University. Series: Right, 23-24, 176-183. Doi: 10.34079/2226-3047-2022-12-23-24-176-183;

15. Davchenko, T. (2020). Grounds for the opening of criminal proceedings. Legal Scientific Electronic Journal, 4, 299-302. Doi: 10.32782/2524-0374/2020-4/72;

16. David, M. (2018). Cyber risk of coordinated attacks in critical infrastructures. Winter Simulation Conference. Sweden, Gothenburg. PublisherInstitute of Electrical and Electronics Engineers Inc. 2759-2768. Retrieved from https://experts.illinois.edu/en/publications/cyber-risk-of-coordinated-attacks-in-critical-infrastructures/;

17. Denisiuk, S. & Kotsar, O. (Eds.). (2016). Energy efficiency of Ukraine. Best project ideas: Project "Professionalization and stabilization of energy management in Ukraine" (pp. 79). Kyiv: KPI named after Igor Sikorskyi;

18. Dontsov, D. (2020). Civil legal framework for privatizing state property. Entrepreneurship, Economics and Law: Civil Law and Process Series, 12, 17-21. Doi: 10.32849/2663-5313/2020.12.03;

19. Dreis, Y. (2017). Analysis of basic terminology and negative consequences of cyberattacks on information and telecommunication systems of critical infrastructure of the state. Protection of Information, 19(3), 214-222. Doi: 10.18372/2410-7840.19.11900;

20. Dubnytskyi, V., Fedulova, O. & Vasyliuk, V. (2017). Regional infrastructure: modernization, priorities and development prospects. Economic problems: Regional Economy, 2, 167-168;

21. Ducaru, S. (2017). The security of critical energy infrastructure in the age of multiple attack vectors: nato's multi-faceted approach. Europolity-Continuity and Change in European Governance. 11 (1). 5-20. Doi: 10.25019/europolity.2017.11.1.01;

22. Dudorov, O. & Dudorova, K. (2011). Illegal privatization of state and municipal property: Problems of qualification and law improvement. Scientific Bulletin of the International Humanitarian University, 2, 104-110;

23. Fediuk, V. (2022). The law of Ukraine «on critical infrastructure»: Issues of criminal law. In International Scientific Conference (pp. 229-233). Riga: Baltija Publishing. Doi: 10.30525/978-9934-26-229-6-59;

24. Franchuk, V., Pryhunov, P. & Melnyk, S. (2021). Security of critical infrastructure facilities in Ukraine: Organizational and regulatory problems and approaches. Social and Legal Studies, 3 (13), 142-148. Doi: 10.32518/2617-4162-2021-3-142-148;

25. Frintova, D. & Frinta, O. (2022). Legal capacity in the Civil Code and its recent development. Acta Universitatis Carolinae Iuridica, 68(2), 27-34. Doi: 10.14712/23366478.2022.14;

26. Gusarev, S. & Tikhomirov, O. (Eds.). (2017). Theory of the state and law: education. manual. Kyiv: NAIA, Education of Ukraine;

27. Guseva, V. (2019). Forensic classification of crimes: current state of scientific support and prospects for further research. National Law Journal: Theory and Practice. 3 (1). 151-156. Retrieved from: http://dspace.univd.edu.ua/xmlui/handle/123456789/6079;

28. Hankevich, K. et al. (2021). Peculiarities of the formation of the legal basis for the existence of critical infrastructure objects of Ukraine in the system of the Ministry of Defense of Ukraine. Legal Scientific Electronic Journal. Doi: 10.32782/2524-0374/2021-11/15;

29. Hasegawa, A., Ohira, T., Maeda, M., Yasumura, S. & Tanigawa, K. (2016). «Emergency Responses and Health Consequences after the Fukushima Accident; Evacuation and Relocation». Clinical Oncology. 28 (4). 237-244. Doi: 10.1016/j.clon.2016.01.002.;

30. Higton, N. & Clark, S. (2010). Using Public Private Partnerships to deliver successful rail projects. Proceedings of the ASME Joint Rail Conference, 2, 479-486. Doi: 10.1115/JRC2010-36198;

31. Humin, O. & Pryakhin, E. (2020). The person of the criminal as an element criminal characteristics illegal privatization of the state and communal property. Bulletin of the Lviv Polytechnic National University. Series: «Legal Sciences», 7(27), 199-205. Doi: 10.23939/law2020.27.199;

32. Iksarova, N. (2010). Transport infrastructure as a component of economic security of Ukraine. Economic Space, 36, 55-61;

33. Kachur, I., Lepushynskyi, V. & Zammit, R. (2016). The balance sheet of the National Bank of Ukraine: Before, during and after the crisis. Bulletin of the

National Bank of Ukraine. Retrieved from https://journal.bank.gov.ua/uploads/articles/237_1_ukr.pdf;

34. Klymas, R. (2022). Inspection of the fire site in the presence of explosive objects by specialists of the research and testing laboratories of the State Emergency Service under martial law. The European choice of Ukraine, the development of science and national security in the realities of large-scale military aggression and global challenges of the 21st century: in 2 volumes: materials International scientific-practical conf. (June 17, 2022). Odesa: «Helvetyka» Publishing House, 2. 440-444;

35. Kolinets, L. (2018). The effects of the global crisis on the economy of Ukraine. Scientific Bulletin of the Uzhhorod National University: Series: International Economic Relations and World Economy, 18 (2), 54-57;

36. Komisarchuk, R. (2017a). The mechanism of economic crime and his forensic analysis: Problem. Scientific Works of the National University "Odesa Law Academy", 19, 206-213;

37. Komisarchuk, R. (2017b). Forensic model of the mechanism of criminal activity in the sphere of economic activity: Concepts and conditions of formation. Actual Problems of the State and Law, 79. 58-65;

38. Komisarov, O., Batyuk, O. & Pavlov, S. (2022). Forensic and military combat support against terrorist and sabotage threats at critical infrastructure facilities. Honor and law. 4 (79). 33-39. Doi: 10.33405/2078-7480/2021/4/79/251498;

39. Krasnoshlyk, A. (2020). Forensic analysis of crimes related to the privatization of communal property. Retrieved from http://dspace.onua.edu.ua/handle/11300/12670?show=full;

40. Krykh, T. (2008). The subject of illegal privatization of state, communal property. University Scientific Notes, 3, 272-275;

41. Kucherina, S. & Olejnikov, D. (2021). Current state of criminal and legal protection critical infrastructure facilities. Information and law. 1 (36). 90-98;

42. Lazari, A. & Mikac, R. (2022). The External Dimension of the European Union's Critical Infrastructure Protection Programme: From Neighbouring Frameworks to Transatlantic Cooperation. Taylor & Francis Group, 336. Doi: 10.4324/9781003273769;

43. Leschuk, G. (2017). Conceptual determinants of investment infrastructure of the region. Scientific Bulletin of the International Humanitarian University. Series: Economics and management, 24 (2), 20-24;

44. Li, S., Cai, J. & Cai, H. (2019). Infrastructure privatization analysis: A public-private duopoly game. Transport Policy, 83, 80-87. Doi: 10.1016/j.tranpol.2019.09.005;

45. Lordan-Perret, R. et al. (2019). Attacks on energy infrastructure targeting democratic institutions. Energy policy, 132. 915-927. Doi: 10.1016/j.enpol.2019.06.025/;

46. Melnyk, M. & Leschuh, I. (2019). Development of the institutional infrastructure of business support in the region: trends and prospects. Efficient Economy, 10. Doi: 10.32702/2307-2105-2019.10.14;

47. Mudretskyi, R. (2019). Forensic classification of methods of countermeasures against judicial review of criminal proceedings. Entrepreneurship, economy and law, 6. 306-312. Doi: 10.32849/2663-5313/2019.6.57;

48. Nicol, D. (2018). Cyber risk of coordinated attacks in critical infrastructures. 2018 Winter Simulation Conference. Sweden, Gothenburg. PublisherInstitute of Electrical and Electronics Engineers Inc. 2759-2768. Retrieved from: https://experts.illinois.edu/en/publications/cyber-risk-of-coordinated-attacks-in-critical-infrastructures;

49. Perinić, J. & Mikac R. (2021). Protection of the Critical Infrastructure from Terrorism: Case Study of the Republic of Croatia. IOS Press. Series: NATO Science for Peace and Security: Information and Communication Security, Comprehensive Approach as «Sine Qua Non» for Critical Infrastructure Protection, 39, 235-250. Doi: 10.3233/978-1-61499-478-7-235;

50. Potip, M. & Negodchenko, V. (2019). Administrative services in the field of housing privatization provided by local self-government bodies. Law and Society: Economic Law and Process, 3, 188-196. Doi: 10.32842/2078-3736-2019-3-1-32;

51. Potip, M. (2019). State of scientific development of the problem administrative and legal principles of the public privatization management in Ukraine. Academic Notes of TNU Named After V.I. Vernadskyi. Series: Legal Sciences, 30(5), 164-170. Doi: 10.32838/2707-0581/2019.5/28;

52. Priakhin, Ye. (2019). Forensic characterization of the illegal privatization of state and municipal property. Bulletin of the Lviv University of Trade and Economics. Legal Sciences, 8, 174-183. Doi: 10.36477/2616-7611-2019-08-19;

53. Rekunenko, I. (2012). Scientific and methodological aspects of the study of the concept of "infrastructure" as an economic category. Economics and management, 3, 57-62;

54. Reznik, O. & Bondrenko, O. (2021). Organizational and legal aspects of the creation of special anti-corruption institutions: A comparative legal study. Law. State. Technology, 3, 92-97. Doi: 10.32782/LST/2021-3-14;

55. Romanenko, E. & Shtokin, R. (2017). Main stages of privatization in Ukraine. Public administration, 5(10), 248-258;

56. Sakhanyuk, O. (2020). Types of vaccines and their development. Vaccination as the most effective method of protecting the population from infectious diseases. State expert center of the Ministry of Health of Ukraine. Kyiv. Retrieved from: https://www.dec.gov.ua/wp-content/uploads/Conference/2020/6/section/9/s9f3.pdf;

57. Selyukov, V. (2022). Prospects for improving legal regulation in the field of canine activity in Ukraine. Entrepreneurship, economy and law. 11. 153-158. Doi: 10.32849/2663-5313/2020.11.26;

58. Shueh, S. (2020). Silicon Valley. Charleston, SC: Arcadia Publishing. 8. Retrieved July 28. URL: https://www.google.com/books/edition/Silicon_Valley/kQj9sq1ktn0C?hl=en &gbpv=1&pg=PA8&printsec=frontcover;

59. Syvodyed, I. (2023). Investigating genocide and ecocide in wartime conditions. Scientific works of the Interregional Academy of Personnel Management. Legal Sciences, 2 (62), 59-64. Doi: 10.32689/2522-4603.2022.2.9;

60. Taran, O. & Sandul, O. (2019). Issue of Criminal Liability for Offences Against Critical Infrastructure Objects in Nuclear Industry. Scientific and technical magazine «Nuclear and radiation safety». 3 (83). 58-67. Doi: 10.32918/nrs.2019.3(83).07;

61. Ted, G. Lewis. (2020). Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, 3rd Edition. 464;

62. Telenyk, S. (2020). The concept and content of the state critical infrastructure protection system. Carpathian Legal Gazette, 2(31), 112-120. Doi: 10.32837/pyuv.v0i2(31).577;

63. Tertyshnyk, V. (2022) Constitution of Ukraine. Scientific and practical commentary. Kyiv: Alerta. 430;

64. Tkalya, O. (2022). National interests and values as the basis for the existence and development of the national state. Legal scientific electronic journal. 4, Doi: 10.32782/2524-0374/2022-4/12;

65. Van Buuren, A; Ellen, G.J. & Warner, J.F. (2016). «Path-dependency and policy learning in the Dutch delta: toward more resilient flood risk management in the Netherlands?». Ecology and Society. 21 (4). Doi:10.5751/es-08765-210443;

66. Vasyutynska, L. (2021). Theoretical aspects of infrastructure research in the context of the project approach. Problems of innovation and investment development. 25. 16-22. Doi: 10.33813/2224-1213.25.2021.2;

67. Vergolyas, O. (2018). Reforming the protection system and increasing the stability of Ukraine's critical infrastructure in terms of current threats. Retrieved from https://coolyanews.info.htm;

68. Yaremechuk, O. & Stakhnitskyi, Y. (2022). Theoretical approaches to defining the definition of critical infrastructure as an object of public administration. Public Administration and Customs Administration, 1 (32), 76-82. Doi: 10.32836/2310-9653-2022-1.13;

69. Yefimenko, I. (2022). Modern possibilities of using unmanned aerial vehicles by Police authorities and units: Analysis of foreign and Ukrainian experience. Scientific Journal of the National Academy of Internal Affairs, 27 (3), 65-77. Doi: 10.56215/0122273.65;

70. Yefimenko, I. (2022). Unmanned aerial vehicle as a forensic technical tool and object of forensic research. Law Journal of the National Academy of Internal Affairs, 12 (4), 61-71. Doi: 10.56215/04221204.61;

71. Yefimenko, I. & Sakovskyi, A. (2022). History, current state, and prospects of development of unmanned aerial vehicles as a technical and forensic tool and object of forensic research. Scientific Journal of the National Academy of Internal Affairs, 27(2), 75-86. Doi: 10.56215/0122272.75;

72. Yefimenko, I., Sakovskyi, A. & Bilozorov, Ye. (2023). Protection of critical infrastructure as a component of Ukraine's national security. Law Journal of the National Academy of Internal Affairs, 13(2), 74-85. Doi: 10.56215/naia-chasopis/2.2023.74;

73. Yefimenko, I., Slipchenko, V. & Vaško, A. (2023). Critical infrastructure as an object of criminal encroachment: General characteristics and features of the investigation organisation. Scientific Journal of the National Academy of Internal Affairs, 28(2), 41-51. Doi: 10.56215/naia-herald/2.2023.41;

74. Yefimov, M. & Pyrig, I. (2022). Methods of investigation of certain types of criminal offenses: Textbook. Dnipro: Bila K.O. Publisher. 271;

75. Yermenchuk, O. (2017). Normative and legal regulation of activity in the sphere of protection of national critical infrastructure: analysis and generalization of the US rule-making practice. Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs, 3, 135-140;

76. Yermenchuk, O. (2018). Basic approaches to the organization of critical infrastructure protection in European countries: experience for Ukraine. Dnipro;

77. Yin, M. (2022). Privatization and accountability in Australian immigration detention: A case of state-corporate symbiosis. Punishment and Society, 4 (25), 1119-1137. Doi: 10.1177/14624745221135175;

78. Zabzaliuk, D., & Besaha, I. (2023). Legal aspects of protection of rights to land plots that were transferred to private ownership based on the provisions of Decree of the Cabinet of Ministers of Ukraine. Social and Legal Studies, 6 (2), 17-24. Doi: 10.32518/sals2.2023.17;

79. Zadorozhny, O. (2018). Some problematic aspects of the amendments to the Law of Ukraine "On Privatization of State and Communal Property". Entrepreneurship, Economy and Law: Civil law and Process, 5, 30-35;

80. Zhu, H., Zhang, C., Ramirez-Marquez, J.A., Wu, S., & Monroy, R. (2021). The Integration of Protection, Restoration, and Adaptive Flow Redistribution in Building Resilient Networked Critical Infrastructures Against Intentional Attacks. Ieee Systems Journal, 15(2), 2959-2970. Doi: 10.1109/JSYST.2020.3039466.

РОЗСЛІДУВАННЯ ПОСЯГАНЬ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Методичні рекомендації