УДК 342.951:351.85

В. В. Косинський
здобувач кафедри адміністративного права,
процесу та адміністративної діяльності
Дніпропетровського державного університету внутрішніх справ

КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ ЯК ОБ'ЄКТ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ

Вступ. У сучасному світі національна безпека країни, її стійкість стосовно усього комплексу загроз і небезпек значною мірою залежать від рівня захищеності та стійкості критичної інфраструктури держави. Навпаки проблеми із забезпеченням населення, суб'єктів господарювання та органів влади електроенергією, зв'язком, послугами з транспортних перевезень, водопостачання, водовідведення, каналізації тощо, припинення надання таких послуг та товарів, в деяких випадках навіть суттєве підвищення вартості тарифів, може призводити до соціально-політичної нестабільності, загострення внутрішньополітичних конфліктів, значних економічних втрат, послаблення інститутів влади.

Поширення різноманітності загроз з кожним роком являє усе більшу реальну небезпеку під час захисту об'єктів критично важливої інфраструктури. Уразливість таких об'єктів усе більше проявляється з розвитком інформаційних технологій, які пронизують усі сфери життя і, в першу чергу, діяльність економічно активного населення. Тому захист (в першу чергу засобами адміністративного права) життєво важливих суспільних структур та інститутів є пріоритетним завданням державних інституцій в контексті забезпечення національної безпеки країни.

Традиційно в поняття інфраструктури в першу чергу включаються великі автомагістралі, дороги, мости, мережі громадського транспорту, аеропорти, мережі постачання води, обробку та ліквідацію відходів, поводження з небезпечними відходами, виробництво і подачу електроенергії, телекомунікації. Однак цим переліком не слід обмежуватися. В умовах, коли на суші і на морі, в повітрі, космосі і кіберпросторі держави готові вести війни гібридні і проксі-війни, асиметричні війни і війни, які тепер називають «конфлікт», власне поняття «інфраструктура» і «критична інфраструктура» зазнають змін, точніше – наповнюються новим змістом.

Відсутність чітко визначеної понятійно-термінологічної основи в цій галузі так само заважає створенню ефективно діючої системи підтримання належного рівня функціонування критичної інфраструктури, навіть попри те, що вперше поняття «критична інфраструктура» почало вживатися у другій половині 1990-х років переважно стосовно розподілених великомасштабних інформаційних систем (центрів обробки даних, об'єднаних комунікаційних мереж тощо) [1, с. 55–57].

Стан наукової розробки проблеми. Проблема створення ефективної системи адміністративно-правового забезпечення безпеки критичної інфраструктури не нова для української правничої науки. Чимало вчених, політиків, громадських діячів зверталися до широкого кола питань цієї тематичної ніші, зокрема слід згадати наукові праці В.Б. Авер'янова, Л.С. Анохіна, О.М. Бандурки, Д.М. Бахраха, В.М. Бевзенка, О.І. Безпалової, Ю.П. Битяка, І.Л. Бородіна, І.А. Галагана, В.В. Галунька, В.М. Гаращука, І.П. Голосніченка, С.Т. Гончарука, Є.В. Додіна, О.І. Дрозда, В.В. Зуй, Р.В. Ігоніна, Д.П. Калаянова, Р.А. Калюжного, Л.В. Коваля, Т.О. Коломоєць, В.К. Колпакова, А.Т. Комзюка, О.В. Кузьменко, С.О. Кузніченка, М.В. Лошицького, Д.М. Лук'янця, Р.С. Мельника, Т.П. Мінки, Р.В. Миронюка, С.О. Мосьондза, О.М. Музичука, В.Я. Настюка, В.І. Олефіра, О.І. Остапенка, В.П. Пєткова, С.В. Пєткова, Д.В. Приймаченка, Р.А. Сербина, А.О. Собакаря, М.М. Тищенка, О.І. Харитонової, О.С. Юніна та ін. Водночас вчені тлумачать окреслені питання, виходячи із власних політичних уподобань, що унеможливлює об'єктивне висвітлення досліджуваних проблем, зумовлює потребу аналітичного узагальнення здобутків попередників на теоретичному рівні. Проблематика адміністративно-правового забезпечення безпеки критичної інфраструктури докладно не досліджувалась, оскільки переважна більшість вчених у своїх доробках висвітлюють її фрагментарно.

Тому **метою статті** є з'ясування сутності та змісту критичної інфраструктури як особливого об'єкта адміністративно-правового захисту, а також визначення чинників, якими зумовлено необхідність постійного та цілеспрямованого його здійснення.

Виклад основного матеріалу. Для українського законодавства поняття «критична інфраструктура» є відносно новим, хоча і визначається у деяких нормативно-правових актах різної юридичної сили та цільового спрямування. Одним з таких, насамперед, є Концепція створення державної системи захисту критичної інфраструктури, в якій остання розуміється як сукупність об'єктів, які є стратегічно важливими для економіки і безпеки держави, суспільства, населення та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам України [2].

Майже аналогічне визначення критичної інфраструктури містить проект Закону України «Про критичну інфраструктуру та її захист», розроблений Мінекономрозвитку на виконання доручення Кабінету Міністрів України від 21.02.2017 № 1835/4/1–17 до Указу Президента України від 16 січня 2017 року № 8/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» [3], згідно якого критична інфраструктура – це об'єкти, які є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [3].

Більш розширеним є визначення критичної інфраструктури, як сукупності об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних фінансових збитків та людських жертв, наведене у Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури, що затверджений постановою Кабінету Міністрів України № 563 від 23 серпня 2016 року [4].

Повного розкриття на законодавчому рівні поняття «критична інфраструктура», як бачимо, не має, проте окремі його елементи зустрічаються в Директиві Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту [5], постанові Кабінету Міністрів України від 14.03.2018 р. № 309 «Про затвердження Кодексу системи передачі» [6] тощо.

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

Наявність у будь-якій країні об'єктів критичної інфраструктури ставить на порядок денний актуальне питання їх захисту, підвищення безпеки та стійкості такої системи до всього спектру загроз і ризиків, оскільки саме критична інфраструктура забезпечує життєво важливі для населення, суспільства та держави послуги та функції, без яких неможливі їх безпечне існування та добробут, а також належний рівень національної безпеки [7] особливо в нинішніх умовах, коли спостерігається загальносвітова тенденція до різкого посилення екстремізму та тероризму, небувале зростання організованої злочинності тощо.

Однією з головних проблем стійкості критичної інфраструктури є високий рівень зношеності основних фондів промислових підприємств, що в середньому становить 60,3%. Значний ризик техногенних аварій пов'язаний із наявністю на території України численних об'єктів підвищеної небезпеки, що використовують в діяльності значні обсяги небезпечних речовин. При цьому аварії на більшості з них можуть призвести до виникнення надзвичайних ситуацій державного або регіонального рівня.

В житлово-комунальному комплексі протяжності ветхих та аварійних водопровідних мереж в середньому по Україні становить понад 34%, а теплових і парових мереж – понад 18% від загальної протяжності таких мереж, що впливає на втрати води та теплової енергії при їх доставці споживачам, підвищення тарифів, і як наслідок провокує соціальну нестабільність.

До типових прикладів порушення умов безпечного функціонування об'єктів критичної інфраструктури, їх безперервності та стійкості, що створює реальні чи потенційні загрози національній безпеці, вчені відносять:

по-перше, фізичне захоплення об'єктів при збереженні їх функціональності (наприклад, захоплення енергетичних активів Криму);

по-друге, припинення функціонування об'єктів, у тому числі внаслідок фізичного захоплення, для завдання збитків попередньому власнику чи обміну на «потенційні» переваги в інших сферах (задоволення політичних чи економічних вимог, як-от умови постачання вугілля до України, викуп активів, вплив на ринкову вартість компаній та сировини тощо);

по-третє, розукомплектування окремих елементів інфраструктури з метою отримання кримінального доходу (масові факти різання критичної інфраструктури на окупованих територіях Донбасу для продажу у вигляді металобрухту);

по-четверте, фізичне знищення об'єкта для завдання критичної шкоди, збільшення витрат на подолання стану порушення функціонування інфраструктури (наприклад, неможливість доставити ресурси);

по-п'яте, перешкоджання діяльності з відновлення функціональності енергетичної інфраструктури та формування суспільно-політичного невдоволення;

по-шосте, використання транспортної інфраструктури (зокрема повітряного простору України) для провокацій (як у випадку із трагедією авіарейсу MH178), блокування відновлення критичної інфраструктури в зоні бойових дій, блокування транзиту товарів через російський кордон [8, с. 62-76];

по-сьоме, несанкціоновані втручання в роботу не лише енергетичної, але й інформаційно-комунікаційної, комунальної інфраструктури тощо.

В групі загроз природні лиха та небезпечні природні явища слід виділити: метеорологічні або

надзвичайні погодні умови (снігопади, ожеледь, хуртовини, зливи, градобій, заморозки, посухи, спека, урагани, шквали, смерчі), гідрологічні (повені, селі, паводки, підтоплення, цунамі), геологічні (небезпечні екзогенні геологічні процеси – зсуви, просідання та карст), епідемії та пандемії. Поміж зазначених видів загроз варто виділити метеорологічні, частота яких в Україні значно збільшилася останніми десятиліттями, зокрема таких як обледеніння, підтоплення, посухи тощо. Найнебезпечнішими гідрологічними загрозами за наслідками для критичної інфраструктури є паводки [9].

Іншими словами постає необхідність виявлення небезпек, оцінювання ризиків та прогнозування надзвичайних ситуацій, що можуть завдати непоправної шкоди охоронюваним суспільним інтересам шляхом створення відповідних загроз національній безпеці країни в цілому.

На сьогодні можна сказати, що загрозами критичної інфраструктури є:

недостатній розвиток організаційно-технічного забезпечення захисту об'єктів критичної інфраструктури і державних електронних інформаційних ресурсів;

брак спроможностей суб'єктів сектору безпеки і оборони для забезпечення захисту об'єктів критичної інфраструктури та боротьби з кіберзагрозами, кібершпигунством, кібертероризмом та кіберзлочинністю, які негативно впливають на їх стале функціонування;

запізнення та неефективність дій органів державної влади та силових структур з реагування на загрозу пошкодження критичної інфраструктури та забезпечення її відновлення тощо.

Крім цього, найбільш небезпечними джерелами та передумовами загроз безпеці критичної інфраструктури можуть бути наступні чинники та явища:

– інституційна слабкість органів державної влади та місцевого самоврядування, що робить відповідні критично важливі об'єкти вразливими до впливу деструктивних чинників;

– природні катаклізми, кліматичні зміни, технологічні катастрофи та надзвичайні події, пов'язані з діяльністю людини;

– внутрішні і транскордонні кризові явища політичної, економічної, фінансової, демографічної природи;

– тероризм, наркоторгівля, організована злочинність;

– обмежені ресурси (природні, економічні, соціальні), брак або недосконалість норм і правил користування ними, корупція, що провокують небажані форми конкуренції за доступ до ресурсів тощо.

На стан захищеності об'єктів критичної інфраструктури впливає й економічна ситуація, що склалася в країні, адже, якщо у державі спостерігаються розвиток та економічне зростання, то безпека зміцнюється і закріплюється, а її граничні значення зміщуються у бік вищих значень або вводяться нові індикатори, котрі відображають новий рівень національної економічної системи. Однак криза супроводжуються, як правило, загрозами стабільності соціально-економічній ситуації та призводять до наближення показників до неприпустимого рівня безпеки [10, с. 54].

З урахуванням викладеного необхідність адміністративно-правового захисту критичної інфраструктури не викликає сумнівів, що може бути зроблено на декількох рівнях, а саме:

фізичний захист ресурсів, об'єктів, технологій, що використовуються, а також управлінських технологій;

програмно-технічний рівень передбачає здійснення ідентифікації і перевірки дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності;

управлінський рівень передбачає управління, координацію і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління критичною інфраструктурою;

технологічний рівень – здійснюється реалізація стратегії безпеки критичної інфраструктури держави шляхом застосування комплексу сучасних автоматизованих інформаційних технологій;

оперативний рівень (рівень оператора об'єкта критичної інфраструктури) передбачає вжиття комплексу заходів щодо створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем та кібербезпеки;

рівень інформаційно-телекомунікаційних мереж реалізується у форматі координації дій суб'єктів системи безпеки критичної інфраструктури, які пов'язані між собою однією метою.

процедурний рівень передбачає вжиття заходів, що реалізуються відповідними суб'єктами, серед яких: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування відновлювальних робіт тощо.

З урахуванням загроз нормальному функціонуванню об'єктів критичної інфраструктури запобігання та протидія ним вбачається шляхом застосування комплексу заходів залежно від сукупності таких складових як: а) об'єкт загрози; б) носій загрози; в) причини її виникнення; г) спосіб впливу; д) динаміка ескалації; е) можливі наслідки впливу загрози [11].

Детальний аналіз загроз за такою схемою дає можливість, по-перше, формалізувати та деталізувати їх розгляд, по-друге, розробити сукупність базових сценаріїв на випадок можливих конфлік-

тних ситуацій, по-третє, оцінити реальність загроз та визначити їх пріоритети і, нарешті, приступити до формування функцій захисту не взагалі, а насамперед, маючи за мету запобігти деструктивному впливу конкретної загрози на різних етапах її ескалації. Розгляд наведених прикладів загроз дає підстави стверджувати, що їх виявлення та протидія їхньому впливу на національні інтереси України мають бути турботою не тільки спеціальних органів безпеки, а й практично всіх державних органів у всіх сферах життєдіяльності. Ця робота має починатися на етапах планування діяльності, формування концепцій, стратегій, державних програм соціально-економічного розвитку і продовжуватися під час їх виконання [11].

Безперечно, захист критичної інфраструктури повинен враховувати особливості кожної групи критично важливих об'єктів залежно від певних загроз та вразливих місць. Це необхідно для захисту всіх частин критичної інфраструктури, в тому числі її фізичного захисту шляхом охорони, блокадами або виокремленням виробництва процесів через ефект доміно.

Висновок. Таким чином, підсумовуючи викладене, слід підкреслити важливість критичної інфраструктури як особливого об'єкта адміністративно-правового захисту, необхідність постійного та цілеспрямованого здійснення якого зумовлено різними чинниками, основними з яких є:

по-перше, визнання критичної інфраструктури та її захисту як одного із пріоритетних завдань суб'єктів публічного адміністрування у сфері забезпечення національної безпеки в Україні;

по-друге, широке використання автоматизованих інформаційних систем управління виробництвом та інших нових технологій у важливих галузях економіки;

по-третє, зростання небезпеки та інтенсивності загроз техногенного та природного характеру для об'єктів критичної інфраструктури;

по-четверте, збільшення кількості потенційно небезпечних об'єктів, багато з яких розташовані у великих містах і найбільш заселених регіонах;

по-п'яте, наростання терористичної активності, політичного і релігійного екстремізму в світі тощо.

Література:

1. Гнатюк, С. О. Критерії визначення елементів критичної інфраструктури держави / С. О. Гнатюк, В. М. Лядовська // «Інноваційний потенціал світової науки XXI сторіччя»: матеріали XXIII всеукраїнської наук.-практ. конф., 10–15 грудня 2013 р. Запоріжжя: Вид-во ПГА, 2013. С. 55–57.

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

3. Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури : рішення Ради національної безпеки і оборони України від 29 грудня 2016 року URL: https://zakon.rada.gov.ua/laws/show/n0014525-16#Text

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

5. Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту. URL: https://zakon.rada.gov.ua/laws/show/984_002-08/ed20081208#n41

6. Про затвердження Кодексу системи передачі: Постанова від 14.03.2018 р. № 309. URL: https://zakon.rada.gov.ua/laws/show/v0309874-18/ed20180314#n72

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

8. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети*. 2016. № 3 (40). С. 62-76.

9. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки) (аналітична записка) URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/zagrozi-kritichniy-infrastrukturi-ta-ikh-vpliv-na-stan-nacionalnoi

10. Кулінська А. В. Кризові ситуації, які викликають загрозу індикаторам економічної безпеки України. *Економіка та держава*. 2016. № 1. С. 53-55.

11. Економічна безпека як складова національної безпеки держави URL: http://bibl.com.ua/pravo/5488/index.html.

Анотація

Косинський В. В. **Критична інфраструктура України як об'єкт адміністративно-правового захисту.** – Стаття.

У статті з'ясовано сутність та зміст критичної інфраструктури як особливого об'єкта адміністративно-правового захисту, а також визначено чинники, якими зумовлено необхідність постійного та цілеспрямованого його здійснення.

Окреслено типові приклади порушення умов безпечного функціонування об'єктів критичної інфраструктури, їх безперервності та стійкості, що створює реальні чи потенційні загрози національній безпеці.

Розглянуто найбільш небезпечні джерела та передумови загроз безпеці критичної інфраструктури.

Охарактеризовано рівні адміністративно-правового захисту критичної інфраструктури, а саме: фізичний захист ресурсів, об'єктів, технологій, що використовуються, а також управлінських технологій; програмно-технічний рівень передбачає здійснення ідентифікації і перевірки дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності; управлінський рівень передбачає управління, координацію і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління критичною інфраструктурою; технологічний рівень – здійснюється реалізація стратегії безпеки критичної інфраструктури держави; рівень інформаційно-телекомунікаційних мереж реалізується у форматі коор-

динації дій суб'єктів системи безпеки критичної інфраструктури, які пов'язані між собою однією метою; процедурний рівень передбачає вжиття заходів, що реалізуються відповідними суб'єктами.

Підкреслено важливість критичної інфраструктури як особливого об'єкта адміністративно-правового захисту, необхідність постійного та цілеспрямованого здійснення якого зумовлено різними чинниками, серед яких названо: визнання критичної інфраструктури та її захисту як одного із пріоритетних завдань суб'єктів публічного адміністрування у сфері забезпечення національної безпеки в Україні; широке використання автоматизованих інформаційних систем управління виробництвом та інших нових технологій у важливих галузях економіки; зростання небезпеки та інтенсивності загроз техногенного та природного характеру для об'єктів критичної інфраструктури; збільшення кількості потенційно небезпечних об'єктів, багато з яких розташовані у великих містах і найбільш заселених регіонах; наростання терористичної активності, політичного і релігійного екстремізму в світі тощо.

Ключові слова: критична інфраструктура, об'єкт, адміністративно-правовий захист, національна безпека, загрози безпеці, джерела небезпеки, публічне адміністрування.

Аннотация

Косинский В. В. **Критическая инфраструктура Украины как объект административно-правовой защиты.** – Статья.

В статье выяснено сущность и содержание критической инфраструктуры как особого объекта административно-правовой защиты, а также определены факторы, которыми обусловлено необходимость постоянного и целенаправленного его осуществления.

Определены типичные примеры нарушения условий безопасного функционирования объектов критической инфраструктуры, их непрерывности и устойчивости, создает реальные или потенциальные угрозы национальной безопасности.

Рассмотрены наиболее опасные источники и предпосылки угроз безопасности критической инфраструктуры.

Охарактеризованы уровни административно-правовой защиты критической инфраструктуры, а именно: физическая защита ресурсов, объектов, технологий, используемых, а также управленческих технологий; программно-технический уровень предусматривает осуществление идентификации и проверки подлинности пользователей, управление доступом, протоколирование и аудит, криптография, экранирование, обеспечение высокой доступности; управленческий уровень предполагает управление, координацию и контроль организационных, технологических и технических мероприятий на всех уровнях управления критической инфраструктурой; технологический уровень осуществляется реализация стратегии безопасности критической инфраструктуры государства; уровень информационно-телекоммуникационных сетей реализуется в формате координации действий субъектов системы безопасности критической инфраструктуры, которые связаны между собой одной целью; процедурный уровень предусматривает принятие мер, реализуемых соответствующими субъектами.

Подчеркнута важность критической инфраструктуры как особого объекта административно-правовой защиты, необходимость постоянного и целенаправленного осуществления которого обусловлено различными факторами, среди которых названо: признание критической инфраструктуры и ее защиты как одного из приоритетных задач субъектов публичного администрирования в сфере обеспечения национальной безопасности в Украине; широкое использование автоматизированных информационных систем управления производством и других новых технологий в ведущих отраслях экономики; рост опасности и интенсивности угроз техногенного и природного характера для объектов критической инфраструктуры; увеличение количества потенциально опасных объектов, многие из которых расположены в крупных городах и наиболее заселенных регионах; нарастания террористической активности, политического и религиозного экстремизма в мире и тому подобное.

Ключевые слова: критическая инфраструктура, объект, административно-правовая защита, национальная безопасность, угрозы безопасности, источники опасности, публичное администрирование.

Summary

Kosinsky V. V. **Critical infrastructure of Ukraine as an object of administrative and legal protection.** – Article.

The article clarifies the essence and content of critical infrastructure as a special object of administrative and legal protection, as well as identifies the factors that determine the need for constant and purposeful implementation.

Typical examples of violations of the conditions of safe operation of critical infrastructure, their continuity and resilience, which poses real or potential threats to national security.

The most dangerous sources and preconditions for threats to the security of critical infrastructure are considered.

The levels of administrative and legal protection of critical infrastructure are characterized, namely: physical protection of resources, objects, technologies used, as well as management technologies; software and hardware level provides for the identification and verification of users, access control, logging and auditing, cryptography, shielding, ensuring high availability; management level involves the management, coordination and control of organizational, technological and technical activities at all levels of critical infrastructure management; technological level – the implementation of the security strategy of the critical infrastructure of the state is carried out; the level of information and telecommunication networks is realized in the format of coordination of actions of subjects of security system of critical infrastructure, which are interconnected by one purpose; procedural level involves the implementation of measures implemented by the relevant actors.

The importance of critical infrastructure as a special object of administrative and legal protection is emphasized, the need for constant and purposeful implementation of which is due to various factors, including: recognition of critical infrastructure and its protection as one of the priority tasks of public administration in national security in Ukraine; extensive use of automated production management information systems and other new technologies in important sectors of the economy; increasing danger and intensity of man-made and natural threats for critical infrastructure facilities; increasing the number of potentially dangerous objects, many of which are located in large cities and the most populated regions; the growth of terrorist activity, political and religious extremism in the world, etc.

Key words: critical infrastructure, facility, administrative and legal protection, national security, security threats, sources of danger, public administration.