2. Про затвердження Указу Президента України «Про введення воєнного стану в Україні»: Закон України від 24 лютого 2022 року № 2102-IX. URL:https://zakon.rada.gov.ua/laws/show/2102-20#Text.

3. Про оборону України: Закон України. Відомості Верховної Ради України. – 1992, № 9, Ст.106. URL:https://zakon.rada.gov.ua/laws/show/1932-12#Text

4. Про затвердження Порядку залучення працездатних осіб до суспільно корисних робіт в умовах воєнного стану: Постанова Кабінету Міністрів України від 13 липня 2011 року № 753. URL: https://zakon.rada.gov.ua/laws/show/753-2011-%D0%BF#Text

5. Гуцу С. Ф. Особливості дистанційної праці і її впровадження в надзвичайних умовах//Український дослідницький простір в умовах війни: адаптація й перезавантаження технічних і юридичних наук: збірник матеріалів доповідей учасників міжнародної науково-практичної конференції. (Харків-Рига, 31 травня 2022 р.). Харків, 2022. С. 70-73

УДК 342

Дмитро РАСПУТНІЙ
здобувач вищої освіти ступеня доктора філософії (PhD)
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
ORCID: 0000-0002-2920-4854

ЗАГАЛЬНІ ТА ГАЛУЗЕВІ ЗАСАДИ БЕЗПЕКИ ТА СТАЛОГО РОЗВИТКУ В СЕКТОРАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: У даній статті розглядається вплив воєнного стану на процес трансформації, розвитку та реалізації безпекових функцій при забезпеченні безпеки об’єктів критичної інфраструктури. Основні принципи, та основоположні документи для формування безпеки на об’єктах критичної інфраструктури. Тенденції розвитку, та трансформація наявної системи.

Ключові слова: Критична інфраструктура, Кадрова безпека, Економічна безпека Інформаційна безпека, Фізична безпека, інженерно-технічні споруди.

GENERAL AND SECTOR-SPECIFIC PRINCIPLES OF SECURITY AND SUSTAINABLE DEVELOPMENT IN CRITICAL INFRASTRUCTURE SECTORS

Abstract: This article explores the impact of a state of war on the process of transformation, development, and implementation of security functions in ensuring the safety of critical infrastructure objects. It delves into the fundamental principles and key documents shaping security on critical infrastructure sites. The trends in development and the transformation of the existing system are also examined.

Keywords: Critical infrastructure, Personnel security, Economic security, Information security, Physical security, Engineering structures.

Вступ

Значення критичної інфраструктури для суспільства та економіки полягає у її ключовій ролі у забезпеченні функціонування суспільства та підтриманні економічної стійкості країни.

Згідно з «Законом україни про критичну інфраструктуру» об’єкти критичної інфраструктури - об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [1].

Тобто Критична інфраструктура об'єднує різноманітні сектори, такі як енергетика, транспорт, водопостачання, телекомунікації, охорона здоров'я, фінанси та інші, які є життєво важливими для суспільства та економіки.

А отже, критична інфраструктура є основою суспільства та економіки, і її безпека та сталий розвиток є важливим завданням для забезпечення добробуту громадян та стійкості держави особливо під час війни.

Основна частина

Термін КІ- далі, критична інфраструктура, вперше з’явився у директиві PDD-63 (Presidential Decision Directive), яка була підписана президентом Сполучених Штатів Америки Б. Клінтоном у 1996 році. [4]

Зазначеною Директивою критичну інфраструктуру було віднесено до національних життєво важливих інтересів, визначено цілі та сформовано концепцію зменшення її уразливості в громадському і приватному секторі.

КІ– це системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки» [2, с. 7].

З огляду на зазначене, видається логічним та доцільним поняття «критичну інфраструктуру України» розглядати як сукупність об’єктів незалежно від форми власності.

Європейський підхід формування архітектури безпеки

Згодом з формуванням Європойської асоціації сталі та вуглю, а пізніше трансформації її до «ЕС» питанням критичної інфраструктури та її безпеки почали приділяти увагу в інших країнах, зокрема: Німеччина, Велика Британія, Нідерланди, Чеська Республіка, Словаччина, Польща, Угорщина та інші. В подальшому така зацікавленість країн учасниць у об’єднанні трансформувалась до утворення низки політичних наднаціональних проєктів, та затвердження організації **European Programme for Critical Infrastructure Protection** (**EPCIP**)

На данний момент, країни європейського союзу формують консультативний оргна разом з іншими країнами НАТО, **Цільова група НАТО - ЄС з питань стійкості критично важливої інфраструктури.**

Це викликано тим, що дедалі більшу загрозу КІ становить диверсійна діяльність та використання саме організованої злочинності (далі – ОЗУ), як інструмент для впливу на діяльність КІ.

Це видозмінює принцип побудування архітектури безпеки навколо об'єкту критичної інфраструктури.

Розвиток забезпечення безпеки об'єктів критичної інфраструктури в Україні

Основоположним документом, для розвитку принципів організації безпеки критичної інфраструктури, тим паче враховуючи безперестанний рух нашої країни до заходу це "ЗЕЛЕНА КНИГА З ПИТАНЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ"

Однак не дивлячись на принципи що були закладені в цьому документі. Теорія зазвичай, стикається з проблемами реалізації на практиці.

Досліджуючи дану тему необхідно зауважити, що те на скільки великим пластом є сама критична інфраструктура, на стільки і обширним є перелік загроз для неї. Тому передбачити все, майже не можливо.Через це багато об'єктів критичної інфраструктури, адаптуються під умови сьогодення на прикладах аналогічних підприємств що зазнали ураження від ворожих дій.

На разі достеменно невідомо повний перелік усіх організаційних засад та дій що використовується для захисту безпеки критичної інфрасткутури органами безпеки, розвідки та контррозвідки, армії та генеральним штабом.

Однак перш за все на підприємствах такого типу не враховуючи в приватній властності вони знаходяться або в державній, як правило використовують наступні підходи із забезпечення безпеки:

- Кадрова безпека,
- Економічна безпека,
- Інформаційна безпека,
- Фізична безпека.

Багато проблем було утворено особами що були залучені до дій проти нашої держави. А саме під впливом третіх осіб або організацій такі особи передавали данні про стан наших критично важливих об'єктів, що й призводило в подальшому до влучань по таким об'єктам.

З моменту початку війни, багато підприємств дедалі більше приділяють уваги саме фізичній безпеці, через постійну, потенційну, небезпеку ураження, а враховуючи досвід отриманий того річ, така загроза повністю реальна.

В першу чергу підприємства, почали підсилювати свої інженерно-технічні споруди, та вдосконалювати системи фізичного захисту.

Почались розбудови та зміни устрою підприємств. Подекуди на деяких підприємствах було прийнято ряд дій за для перенесення уразливих до ворожих дій елементі під землю, а подекуди критично важливі вузли тепло та енерго постачання прийнято було рознести та децентралізувати.

Прикладом такого підходу слугує Проект Закону про внесення змін до Закону України "Про комбіноване виробництво теплової та електричної енергії (когенерацію) та використання скидного енергопотенціалу" щодо розвитку високоефективної когенерації.

Основною проблемою сталого функціонування органів забезпечення безпеки повстала проблема закриття багатьох баз даних.

Зараз завдяки роботі та доволі швидкій адаптації органів розвідки, та правоохоронних органів, взаємодії багатьох профільних міністерств. Доступ до деякої частини таких баз було відновлено, або була знайдена заміна. Тому безпекові органи підприємств відновили в більшій мірі свої дії, та набули нового досвіду з принципів рекрутингу нових робітників.

З приводу економічної безпеки відбулося теж немало змін, органи безпеки підприємст повинні були моніторити економічну діяльність підприємств за відсутності електронних баз даних що безперечно ускладнювало роботу. Це подекуди блокувало дію таких органів, а іноді примушувала відкочуватись до досвіду минулих поколінь та співпрацювати через своїх інформаторів та перевірених контрагентів, хоч і співпрацюючи на невигідних умовах.

А це в свою чергу призводило до завищення цін за товари або послуги, та махінацій у торгах. Однак з плином часу, доступ до більшої половини таких інформаційних баз було відновлено. А навички нового досвіду використовуються навіть з відновленням доступу до таких баз.

Тенденції розвитку та інтеграції

Українськими законотворцями було ухвалено план зі сталого розвитку підприємств критичної інфраструктури, де було вказано на доктринальному рівні план розвитку підприємств, та нових підходів з реалізації безпеки.

В якому здебільшого була акцентована увага саме на подальшій співпраці з міжнародними безпековими органами та консультативними нарадами. Це тим більше крокує нога в ногу з новим підходом до розбудови нової системи захисту критичної інфраструктури, а саме обрати власну стратегію забезпечення національної стійкості та визначити при цьому єдиний комунікаційний пункт для обміну інформацією для контактів з іншими об’єктами КІ регіону та іншими країнами-членами.

Що дасть змогу реагувати саме на актуальні проблеми того регіону, де розташовується об’єкт КІ, та діяти в залежності від ситуації і вже в другу чергу опиратись на дії партнерів.

Все це приводить до роздумів що до того, як буде далі інтегруватись критична інфраструктура України у європейський економічний простір.

Такі зміни в цілому будуть плекати інтерес до інвестицій у об’єкти такого плана. Що надалі буде стимулювати зростання обсягів енергетики, транспортних хабів та інших об’єктів у нашій державі, адже економіка та ринок не терплять пустоти. А Україна свого часу була величезним хабом та брамою до Европи на шляху з Азії.

Однак не дивлячись на все це, на скільки буде приємним інвестеційний клімат, залежить вже саме від нас, та реалізації концепцій що закладуються в законодавстві.

Висновок

Дедалі більше з розглядом нормотворчих актів та документів що використовуються як основоположні для розвитку безпеки КІ ми можемо бачити розвиток у напрямку взаємодії та подальшої інтеграції до системи сумісної взаємодії з Европою. Дедалі більше будуть інтегруватись на підприємствах саме стандарти НАТО та формування сумісного безпекового контуру такого типу об’єктів.

Однак необхідно не забувати і про те що країни НАТО ніколи не зтикалися з прямим протистоянням таким країнам агресорам як наш супротивник.

Тож це нова ступінь в розвитку забезпечення безпеки. Де Українські органи безпеки, та українські спеціалісти зможуть трансформовувати загальний підхід до забезпечення безпеки

На скільки реальним є поняття сталого розвитку критичної інфраструктури в умовах війни дуже важко оцінити, не дивлячись на це я міг би мовити про те що, однозначно наша держава, та критична інфраструктура вийде видозміненою з цих всіх подій.

Логічним буде уявити формування єдиного консультативного органу, та комунікаційної системи з формування оборони та безпеки. Ліричним відступом було б мовити про формування бастіонів навколо, або з таких об’єктів.

Вивчення способів та методів ураження, вивчення витрати на безпеку, та співвідношення їх з потенційними втратами об’єктів. Аналіз ризиків та внесення коректив до вже реалізованих проектів та нововведення вже з отриманих даних.

Список використаних джерел:

1. Про критичну інфраструктуру та її захист : проєкт Закону України. URL: https://zakon.rada.gov.ua

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

3. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпекова діяльність: системний підхід. Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна. 2017. Вип. 1. С. 154–163.

4. Presidential Decision Directive (PDD NSC-63) May 22, 1998, [Електронний ресурс]. – Режим доступу: https://fas.org/irp/offdocs/pdd/pdd-63.htm.