УДК 351.746:355.01(477)
DOI https://doi.org/10.32844/2618-1258.2025.4.34

ЖАЛУБАК В.М.

ТРАНСФОРМАЦІЯ КОНТРРОЗВІДУВАЛЬНОГО ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВІЙНИ В УКРАЇНІ

TRANSFORMATION OF COUNTERINTELLIGENCE PROTECTION OF CRITICAL INFRASTRUCTURE IN THE CONDITIONS OF WAR IN UKRAINE

У статті досліджено трансформацію контррозвідувального захисту критичної інфраструктури України в умовах повномасштабної війни, що супроводжується якісною зміною характеру та інтенсивності безпекових загроз. Обґрунтовано, що воєнні дії на території держави зумовили необхідність переосмислення традиційних підходів до організації контррозвідувального захисту та формування нової моделі реагування на комплексні, гібридні та асиметричні загрози. У статті встановлено, що одним із ключових напрямів трансформації контррозвідувального захисту є поєднання заходів фізичної безпеки з інструментами кіберзахисту, що зумовлено одночасним застосуванням противником засобів кінетичного ураження та методів інформаційно-кібернетичного впливу. Особливу увагу приділено вразливості об'єктів критичної інфраструктури енергетичного та транспортного секторів, які зазнають систематичних атак із використанням ракетного озброєння, керованих авіаційних боєприпасів, безпілотних літальних апаратів різних типів, а також масштабних кібератак, що фактично свідчить про ведення кібервійни як складової сучасного збройного протистояння. Доведено, що застосування противником різноманітних тактичних прийомів і стратегій обумовлює необхідність індивідуалізації контррозвідувального захисту кожного об'єкта критичної інфраструктури. Такий підхід передбачає розроблення спеціалізованих стратегій і тактик, заснованих на оцінці конкретних ризиків, уразливостей та сценаріїв загроз, а також впровадження механізмів управління ризиками і відновлення функціонування об'єктів у разі їх пошкодження або виведення з ладу. Окремо наголошено, що ефективний контррозвідувальний захист у воєнних умовах має будуватися як багаторівнева система, що охоплює загальнодержавний, секторальний та об'єктовий рівні. Така модель передбачає посилену координацію між суб'єктами сектору безпеки і оборони, органами державної влади, операторами критичної інфраструктури та міжнародними партнерами, а також високий рівень адаптивності до змін у воєнній тактиці та динаміки загроз. Зроблено висновок, що подальший розвиток контррозвідувального захисту критичної інфраструктури в умовах війни має ґрунтуватися на принципах комплексності, гнучкості та випереджального реагування, що є необхідною умовою забезпечення стійкості держави та її національної безпеки.

Ключові слова: *диверсія, загроза, критична інфраструктура, кібербезпека, кіберзахист, національна безпека, підривна діяльність, тероризм, трансформація.*

The article examines the transformation of counterintelligence protection of Ukraine's critical infrastructure under conditions of full-scale war, which is accompanied by a qualitative change in the nature and intensity of security threats. It is substantiated that military hostilities on the territory of the state have necessitated a rethinking of traditional approaches to the organization of counterintelligence protection and the formation of a

© ЖАЛУБАК В.М. – кандидат юридичних наук, старший викладач кафедри захисту об'єктів критичної інфраструктури (Національна академія Служби безпеки України) https://orcid.org/0000-0002-7812-7103

new response model to complex, hybrid, and asymmetric threats. The article establishes that one of the key directions in the transformation of counterintelligence protection is the integration of physical security measures with cybersecurity instruments, which is обусловлено the simultaneous use by the adversary of kinetic means of destruction and methods of information and cyber influence. Particular attention is paid to the vulnerability of critical infrastructure facilities in the energy and transport sectors, which are subjected to systematic attacks using missile weapons, guided aerial munitions, unmanned aerial vehicles of various types, as well as large-scale cyberattacks, which in fact indicates the conduct of cyberwarfare as a component of modern armed confrontation. It is demonstrated that the use by the adversary of diverse tactical techniques and strategies necessitates the individualization of counterintelligence protection for each critical infrastructure facility. This approach involves the development of specialized strategies and tactics based on the assessment of specific risks, vulnerabilities, and threat scenarios, as well as the implementation of risk management mechanisms and measures aimed at restoring the functioning of facilities in the event of their damage or disruption. Special emphasis is placed on the fact that effective counterintelligence protection under wartime conditions should be built as a multilevel system encompassing the national, sectoral, and facility-specific levels. Such a model presupposes enhanced coordination among security and defense sector actors, public authorities, critical infrastructure operators, and international partners, as well as a high degree of adaptability to changes in military tactics and the dynamics of threats. It is concluded that the further development of counterintelligence protection of critical infrastructure in wartime should be based on the principles of comprehensiveness, flexibility, and anticipatory response, which is a necessary condition for ensuring state resilience and national security.

Key words: *sabotage, threat, critical infrastructure, cybersecurity, cyber protection, national security, subversive activities, terrorism, transformation.*

Актуальність теми. В умовах повномасштабного російсько-українського збройного конфлікту, коли рф на практиці реалізовує власну військову доктрину ведення так званої «гібридної» війни, критична інфраструктура України, стійкість функціонування якої є невід'ємною складовою забезпечення національної безпеки держави, стала першочерговою ціллю як для військових формувань рф із застосуванням при цьому усього наявного у них арсеналу засобів ураження, так і об'єктом для ведення стосовно них різнопланової підривної діяльності спецслужбими держави-агресора.

В умовах ведення повномасштабної війни на порядок денний постають нові загрози для критичної інфраструктури України, які вимагають відповідного реагування усіх суб'єктів державної системи її захисту. Виняткового значення та особливої ваги за подібних умов набуває питання саме контррозвідувальної компоненти в організації протидії новітнім загрозам, зокрема, в частині недопущення отримання ворогом доступу до інформації як про окремі об'єкти критичної інфраструктури, так і про систему організації захисту критичної інфраструктури в цілому, яка могла б у подальшому бути використана ворогом як для коригування цілей для враження, так і для організації та проведення спецслужбами ворога на найбільш важливих об'єктах вітчизняної інфраструктури диверсій, терористичних актів та інших підривних акцій.

Однією з умов побудови системи ефективного контррозвідувального захисту критичної інфраструктури є належне правове регулювання даної сфери у відповідності до динаміки змін та трансформації раніше існуючих та появи нових небезпек та загроз.

З лютого 2022 року на законодавчому рівні було прийнято ряд нормативно-правових актів, які стосуються діяльності суб'єктів захисту критичної інфраструктури в умовах дії правового режиму воєнного стану, у тому числі і Служби безпеки України як «спеціально уповноваженого органу державної влади у сфері контррозвідувальної діяльності» (стаття 5 Закону України «Про контррозвідувальну діяльність») [1].

Нові умови функціонування критичної інфраструктури, нові загрози та виклики, особливості завдань, які вирішуються органами Служби безпеки України в своїй практичні діяльності, об'єктивно впливають і на організацію самого контррозвідувального захисту критичної інфраструктури, трансформуючи його до нових умов та викликів.

Аналіз наукових досліджень і публікацій. Теоретико-правові засади організації захисту критичної інфраструктури України у загальному безпековому вимірі після початку фази

повномасштабного російсько-українського збройного конфлікту у лютому 2022 року були предметом дослідження таких науковців як Р.Л. Балакін [2], Б.В. Богдан [3], Д.А. Затонацький [4], Г.Ю. Каніщев [5], М.О. Кизим [6], Ю.В. Кузьменко [7], Д.С. Мельник [8], Р.В. Плахотнюк [9], Я.О. Страхніцький [10], О.Л. Шпатакова [11] та інші.

Питання побудови системи антитерористичної та антидиверсійної захищеності критичної інфраструктури досліджували В.В. Крутов [12], Б.Д. Леонов [13] та В.М. Форноляк [12].

Проблематику організації інформаційної безпеки та кіберзахисту об'єктів критичної інфраструктури висвітлювали у своїх наукових працях С.Г. Гордієнко [14], С.Д. Казьмірук [15], А.П. Качаровський [16], О.М. Кучма [17], Я.С. Мануілов [18], В.Г. Пядишев [19], О.І. Скіцько [20] та ряд інших науковців.

У системі відомчої наукової школи вагомий внесок у дослідження саме контррозвідувальної компоненти захисту критично інфраструктури та її генези в умовах війни внесли, Ю.А. Іванов [21, 22, 23], Є.О. Меленті [24], І.І. Осипчук [25], І.В. Слюсарчук [26], Стрельбицький М.П. [27], Тарнавський Ю.Є. [28] та інші.

Однак, враховуючи важливість побудови ефективної системи протидії новим загрозам для критичної інфраструктури України в умовах повномасштабної війни, зважаючи на форми і методи її ведення державою-агресором, в загальній конструкції цієї системи контррозвідувальна складова відіграє надзвичайно важливе, особливе значення. Без належної організації саме контррозвідувального захисту критичної інфраструктури забезпечити стабільність і стійкість функціонування як окремих її об'єктів так і системи в цілому неможливо. З урахуванням зазначеного, питання трансформації контррозвідувального захисту критичної інфраструктури відповідно до реальних і потенційних загроз, які в умовах сьогодення постійно змінюються, потребує подальшого теоретичного опрацювання

Мета статті полягає у комплексному дослідженні процесу та визначенні ключових особливостей трансформації контррозвідувального захисту критичної інфраструктури в умовах ведення на території України повномасштабної війни. Досягнення поставленої мети передбачає аналіз положень загального і спеціального законодавства у сфері національної безпеки та захисту критичної інфраструктури, узагальнення наукових позицій вітчизняних учених, а також вивчення практики діяльності суб'єктів державної системи її захисту, насамперед Служби безпеки України як спеціально уповноваженого органу у сфері контррозвідувальної діяльності. У межах дослідження ставиться завдання з'ясувати напрями, механізми та рівні трансформації контррозвідувального захисту, оцінити їх ефективність в умовах сучасних воєнних і гібридних загроз, а також обґрунтувати можливі шляхи подальшого вдосконалення системи захисту критичної інфраструктури з урахуванням динаміки безпекового середовища.

Виклад основного матеріалу. Стан захищеності об'єктів критичної інфраструктури є однією з ключових складових системи національної безпеки України та водночас необхідною передумовою її сталого функціонування. Ефективний захист таких об'єктів безпосередньо впливає на здатність держави забезпечувати безперервність життєво важливих функцій, зокрема у сферах енергетики, транспорту, зв'язку, водопостачання, охорони здоров'я, фінансової системи та державного управління, а також на спроможність протидіяти сучасним загрозам гібридного характеру.

Процес формування в Україні державної системи захисту критичної інфраструктури відбувався в умовах підвищеної складності та динамічних трансформацій. Значний вплив на нього мали масштабні реформи системи органів державної влади, поява нових інституцій та зміна функціонального призначення вже існуючих органів. Наслідком цих процесів став перерозподіл повноважень між суб'єктами публічного управління, що супроводжувався необхідністю визначення нових компетенцій, механізмів координації та відповідальності у сфері захисту критичної інфраструктури.

Водночас суттєвим стримувальним чинником виступали проблеми законотворчої діяльності. Формування нормативно-правової бази, яка мала б комплексно регулювати питання створення, функціонування та розвитку системи захисту критичної інфраструктури, відбувалося фрагментарно та без належної системності. Окремі нормативні акти ухвалювалися з різним рівнем узгодженості між собою, що ускладнювало чітке визначення кола суб'єктів відповідної системи, їхніх повноважень, зон відповідальності та механізмів взаємодії між державними органами, органами місцевого самоврядування і приватними операторами об'єктів критичної інфраструктури.

Таким чином, процес становлення державної системи захисту критичної інфраструктури в Україні характеризувався інституційною нестабільністю, нормативною непослідовністю та

потребою постійної адаптації до внутрішніх реформ і зовнішніх безпекових викликів. Це зумовлює актуальність подальшого наукового осмислення зазначеної проблематики та необхідність удосконалення правових і організаційних засад захисту критичної інфраструктури як одного з пріоритетних напрямів забезпечення національної безпеки держави.

Так, у грудні 2017 року було прийнято Концепцію створення державної системи захисту критичної інфраструктури [29], і лише у листопаді 2021 року було прийнято базовий для даної сфери забезпечення національної безпеки законодавчий акт [29].

Лише після прийняття профільного Закону в Україні були сформовані відповідні умови для планомірної розбудови національної системи захисту критичної інфраструктури, однак окремі положення потребують певного доопрацювання, що є наслідком непослідовності процесу формування національного законодавства у сфері функціонування критичної інфраструктури на протязі попередніх років. На дану обставину звертає увагу у своїх працях Іванов Ю.А. [22, с. 104].

До недоліків базового законодавчого акту у сфері захисту критичної інфраструктури Тарнавський Ю.Є. відносить той факт, що в Законі не визначено повноваження, завдання та відповідальність суб'єктів національної системи захисту критичної інфраструктури, до яких належить і Служба безпеки України, а також права, обов'язки та відповідальність власників об'єктів критичної інфраструктури.

Крім того, Тарнавський Ю.Є. звертає увагу на те, що визначаючи поняття «життєво важливі функції та/або послуги» (п. 2 ч. 1 статті 1 Закону), законодавець не розкриває ні зміст таких функцій та/або послуг, ні термін «негативний результат» від збоїв, переривань та порушень їх надання визначеними суб'єктами [28, с. 108].

Однак з урахуванням того, що предметом нашого розгляду є трансформація саме контррозвідувального захисту критичної інфраструктури, відповідальність за організацію якого у відповідності до діючого законодавства несе саме Служба безпеки України, розглянемо практичні аспекти та проблемні питання діяльності саме за даним напрямом.

Іванов Ю.А. зазначає, що першочерговою умовою організації ефективного контррозвідувального захисту об'єктів критичної інфраструктури є власне чітке визначення самого переліку цих об'єктів [21, с. 19].

Згідно із Законом України «Про критичну інфраструктуру» захист критичної інфраструктури є складовою частиною забезпечення національної безпеки України (пункт 1 статті 4), а Службу безпеки України визначено як суб'єкт національної системи захисту критичної інфраструктури (пункт 11 статті 14). Діяльність Служби безпеки України у сфері захисту критичної інфраструктури здійснюється в рамках, визначених цим Законом та у порядку, встановленому законами України, що регламентують правові засади організації та діяльності вітчизняної спецслужби. Також зазначається, що Служба безпеки України у межах компетенції здійснює планування відповідних заходів із захисту критичної інфраструктури [30].

У грудні 2022 року Кабінетом Міністрів України до переліку секторів критичної інфраструктури, з урахуванням нових загроз та необхідності організації ефективної протидії цим загрозам, було додано сектор «Національна безпека», секторальним органом до якого цілком логічно було визначено Службу безпеки України [31]. Таким чином, компетенцію Служби в системі захисту критичної інфраструктури було суттєво розширено, додавши до контррозвідувальної складової функцію секторального органу. При цьому важливо відзначити, що в Законі України «Про Службу безпеки України» питання захисту критичної інфраструктури взагалі не відображено, що, на нашу думку, потребує відповідного коригування шляхом внесення відповідних змін до самого Закону.

Слід відзначити, що в структурі самої Служби виокремлено самостійний підрозділ, який безпосередньо опікується вирішенням завдань у сфері захисту критичної інфраструктури та реалізації державної політики у даній сфері у визначеному чинним законодавством порядку – Головне управління контррозвідувального забезпечення об'єктів критичної інфраструктури та протидії фінансуванню тероризму Департаменту захисту національної державності Служби безпеки України.

Щодо інших складових організації контррозвідувального захисту критичної інфраструктури слід також відзначити певну ієрархічну структуризацію з часу початку повномасштабної війни секторів критичної інфраструктури в залежності від їх впливу на здатність функціонування економіки держави в цілому. Саме ці сектори критичної інфраструктури є першочерговою ціллю для держави-агресора, саме вони зазнають найбільш масштабних руйнувань та потребують постійних фінансових вливань для відновлення власної функціональності. До таких секторів

у першу чергу слід віднести сферу енергетики, транспорту та об'єкти життєзабезпечення. Об'єкти у даних сферах вирізняються масштабністю та значно вищою у порівнянні з іншими секторами концентрацією на певних територіях, що робить їх досить вразливими для ракетно-бомбових ударів ворога. Окрім цього, зважаючи на їх значимість для підтримання стійкості усієї критичної інфраструктури країни, подібні об'єкти постійно перебувають у полі зору спеціальних служб ворога, які із застосуванням специфічних засобів і методів роботи намагаються порушити стабільність їх функціонування.

Відтак, постає питання щодо протидії органами СБ України безпосередньо підривній діяльності спецслужб ворога відносно об'єктів критичної інфраструктури саме у цих сферах.

Враховуючи тенденції розвитку ситуації на світових енергетичних ринках та реалії повномасштабної війни на території України, захист вітчизняної енергетики слід розглядати як пріоритетний для Служби безпеки України напрямок контррозвідувального захисту критичної інфраструктури

Воєнні дії викликають в енергетичній сфері ряд проблем, кожна з яких є самостійною загрозою, а в комплексі вони сьогодні вимагають надзвичайних міжнародних зусиль для організації роботи і належного функціонування галузі. Енергетичну безпеку, так само як ядерну й техногенну, слід розглядати в сучасних умовах як міжнародну категорію. Особливість енергетичної безпеки України полягає в тому, що її питому вагу значною мірою складає атомна енергетика, оскільки в попередні роки Україна невпинно нарощувала свій енергетичний потенціал за рахунок збільшення виробничих потужностей атомних електростанцій, співпрацюючи при цьому із рф. На сьогодні в Україні діючими є чотири атомних електростанції, на яких працюють 15 енергоблоків: Запорізька АЕС – 6; Рівненська АЕС – 4; Південноукраїнська АЕС – 3; Хмельницька АЕС – 2. Ними виробллялося більше половини електроенергії в Україні. В умовах повномасштабної війни ці енергоблоки в будь-який час можуть стати загрозою для населення України й світу в результаті враження або пошкодження. В першу чергу це стосується Запорізької АЕС, територія якої опинилася окупованою і ізольованою від енергосистеми України [27].

Загалом, форми та методи ведення війни, які застосовує російська федерація, характеризуються комплексністю, асиметричністю та широким використанням інструментів гібридного впливу. Це зумовлює принципову зміну підходів до забезпечення безпеки держави та актуалізує питання всебічного захисту об'єктів критичної інфраструктури як одного з пріоритетних напрямів національної безпеки. У сучасних умовах збройної агресії загрози таким об'єктам носять не лише воєнний, а й диверсійний, терористичний, інформаційний та кібернетичний характер, що вимагає системного застосування контррозвідувальних, контртерористичних і контрдиверсійних заходів.

Особливої уваги потребує сфера енергетики, насамперед ядерна, з огляду на її стратегічне значення та потенційно катастрофічні наслідки у разі порушення безпеки відповідних об'єктів. Не менш уразливими є підприємства військово-промислового комплексу, функціонування яких безпосередньо пов'язане з обороноздатністю держави та спроможністю Збройних Сил України ефективно протидіяти агресії. Цілеспрямований вплив противника на ці об'єкти може призвести до суттєвого ослаблення військового потенціалу та ускладнення забезпечення потреб сектору безпеки і оборони.

В умовах війни підвищену загрозу також зазнають об'єкти нафтогазової, харчової та агропромислової промисловості, які забезпечують енергетичну, продовольчу та економічну безпеку держави. Порушення їх стабільної роботи може мати довготривалі соціально-економічні наслідки та спричинити гуманітарні кризи. Окрему групу ризику становлять інформаційні технології, мережі електронних комунікацій і системи зв'язку, які є основою сучасного державного управління, функціонування економіки та координації дій у секторі безпеки. Кібератаки, інформаційно-психологічні операції та втручання в роботу телекомунікаційних мереж розглядаються противником як ефективний інструмент дестабілізації внутрішньої ситуації в країні.

Крім того, об'єктами підвищеної уваги з боку ворожих спецслужб і диверсійних груп є мережі життєзабезпечення, транспортна інфраструктура, заклади охорони здоров'я та банківський сектор. Порушення їх функціонування здатне негативно впливати на життєдіяльність населення, фінансову стабільність та рівень суспільної довіри до державних інституцій. У сукупності це створює передумови для внутрішньої дестабілізації та ослаблення стійкості держави до зовнішніх загроз.

Отже, характер сучасної війни обумовлює необхідність формування комплексної та багаторівневої системи захисту об'єктів критичної інфраструктури, що поєднує правові, організаційні,

оперативні та технічні заходи. Провідну роль у цій системі мають відігравати контррозвідувальні, контртерористичні та контрдиверсійні механізми, спрямовані на своєчасне виявлення, попередження та нейтралізацію загроз, а також на забезпечення стійкого функціонування критично важливих сфер життєдіяльності держави в умовах воєнного протистояння [7, с. 59–65].

Реалі, які складаються на даний час в країні, обумовлюють необхідність створення ефективного протиракетного і протидронового захисту об'єктів критичної інфраструктури, розробки планів антидиверсійного та антитерористичного спрямування.

Як зазначає Стрельбицький М.П., заходи мають бути розроблені як на загальнодержавному рівні так і для кожного об'єкту окремо, складати чітку систему протидії, взаємозв'язку, здатну результативно протидіяти як самостійно так і в складі загальнодержавного механізму по захисту від загроз енергетичної безпеки, зокрема, та національної безпеки в цілому. Оскільки противник ставить за мету підрив функціонування усієї соціально-економічної системи України, застосовує засоби масового удару одночасно, охоплюючи кожен раз якомога більшу територію країни і масштаби враження [27].

Одним із пріоритетних напрямків контррозвідувального захисту вітчизняної критичної інфраструктури є протидія загрозам національній безпеці у кіберпросторі. В сучасних умовах подібні загрози набувають все більшої ваги, кратно зрісши після початку військової агресії рф проти України. Атаки у кіберпросторі стали невід'ємною складовою військової агресії рф, важливим елементом якої є акції кібервпливу. В цьому контексті важливою складовою функціонування національної системи кібербезпеки є забезпечення безпеки саме об'єктів критичної інфраструктури, посилення спроможностей складових сектору безпеки і оборони, державних органів адекватно та з випередженням реагувати на кіберзагрози.

Як зазначає Мануйлов Я.С., забезпечення кібербезпеки об'єктів критичної інфраструктури передбачає масштабування технологічної інфраструктури кіберзахисту, який має здійснюватися за рахунок поступового збільшення (відповідно до визначених вимог до таких суб'єктів) кількості елементів децентралізованої зони, їх підключення до суб'єктів централізованої зони та нарощування спроможностей інформаційно-технологічної взаємодії між ними.

При цьому головним завданням технологічної інфраструктури кіберзахисту має стати оперативний та ефективний захист кіберпростору в частині протидії кібератакам, кіберзлочинам, кібертероризму, кібершпигунству, в тому числі шляхом: збору, аналізу, оцінювання, узагальнення та поширення інформації про кіберінциденти; надання методичної допомоги іншим суб'єктам кіберзахисту; взаємного інформування суб'єктів кіберзахисту про нові реальні та потенційні загрози; створення умов для відповідального та довіреного обміну інформацією між суб'єктами кіберзахисту всіх секторів кіберзахисту [18].

Висновки. Поняття критичної інфраструктури є типовим для національних економік різних держав світу, проте аспекти захисту її об'єктів як окрема складова забезпечення високого рівня національної безпеки є відносно новими для української практики. Його формування відбувається із врахуванням європейського досвіду як основного в умовах реалізації євроінтеграційних прагнень України.

Загалом, на підставі узагальнення іноземного досвіду розбудови національних систем захисту критичної інфраструктури у поєднанні з практикою України щодо забезпечення безпеки таких об'єктів в умовах збройної агресії та дії правового режиму воєнного стану, можна виокремити низку ключових напрямів трансформації контррозвідувального захисту критичної інфраструктури з урахуванням актуальних ризиків і загроз сучасного безпекового середовища.

Насамперед, умови війни об'єктивно зумовлюють потребу в тісній інтеграції заходів фізичного захисту з кіберзахистом. Контррозвідувальна діяльність у цій сфері має охоплювати не лише традиційні заходи охорони та режиму безпеки, а й протидію кібернетичним загрозам, що набувають системного характеру. Поєднання кінетичних засобів ураження з актами кібервійни, які застосовує противник, потребує цілісного підходу до захисту об'єктів критичної інфраструктури як у фізичному, так і в інформаційному вимірах.

Водночас ефективність контррозвідувального захисту значною мірою залежить від урахування специфіки кожного конкретного об'єкта. Використання противником різноманітних засобів нападу та диференційованих стратегій впливу зумовлює необхідність розроблення індивідуалізованих моделей захисту. Такі моделі мають базуватися на оцінці уразливостей, критичності функцій об'єкта та ймовірних сценаріїв загроз, що дозволяє сформувати оптимальні стратегії і тактичні рішення для протидії диверсійній, розвідувальній та терористичній діяльності.

Окремого значення набуває орієнтація контррозвідувального захисту не лише на запобігання загрозам, а й на управління ризиками та забезпечення спроможності до швидкого відновлення функціонування критичної інфраструктури. Умови тривалих бойових дій вимагають завчасного планування заходів з мінімізації наслідків можливих уражень, а також створення механізмів оперативного відновлення об'єктів після атак. У цьому контексті контррозвідувальна діяльність має інтегруватися з системами кризового реагування та відновлення.

Важливою передумовою ефективного захисту є налагодження взаємодії та співпраці на різних рівнях управління. Контррозвідувальний захист критичної інфраструктури повинен реалізовуватися на загальнодержавному, галузевому та об'єктовому рівнях із чітким розмежуванням повноважень і водночас із забезпеченням координації між відповідними суб'єктами. Така багаторівнева модель дозволяє враховувати як загальні воєнно-політичні умови, так і специфічні ризики окремих секторів та конкретних об'єктів.

Нарешті, з огляду на постійну зміну тактики, засобів і способів ведення війни з боку противника, контррозвідувальний захист має відзначатися високим рівнем адаптивності. Це передбачає безперервний перегляд і вдосконалення застосовуваних підходів, впровадження сучасних технологічних рішень, а також системне оновлення методів аналізу загроз. Адаптивність у поєднанні з проактивним підходом дозволяє забезпечити стійкість системи захисту критичної інфраструктури в умовах невизначеності та динамічного розвитку воєнних ризиків.

Список використаних джерел:

1. Про контррозвідувальну діяльність : Закон України від 26.12.2002р. № 374-IV. *Відомості Верховної Ради України*. 2003. № 12.

2. Балакін Р.Л. Державне регулювання критичної інфраструктури в Україні в період воєнного стану. *Фінанси України*. 2022. № 7. С. 70–94.

3. Богдан Б.В. Актуальні питання нормативно-правового регулювання захисту критичної інфраструктури в умовах воєнного стану в Україні. *Проблеми сучасних трансформацій*. 2022. № 6. С. 27–31.

4. Затонацький Д.А. Критична інфраструктура в структурі економічної безпеки держави. *Фінанси України*. 2025. № 6. С. 83–100.

5. Каніщев Г.Ю., Тур І.Ю. Критична інфраструктура тимчасово окупованих територій України в українському законодавстві. *Соціально-правові студії*. 2024. С. 18–25.

6. Кизим М.О., Хаустова В.Є., Трушкіна Н.В. Сутність поняття «критична інфраструктура» з позицій національної безпеки України. *Бізнес Інформ*. 2022. № 12. С. 58–78.

7. Кузьменко Ю.В., Коропатов О.М. Адміністративно-правове забезпечення захисту об'єктів критичної інфраструктури України під час воєнного стану. *Юридичний бюлетень*. Вип. 27. 2022. С. 59–65.

8. Мельник Д.С. Побудова моделі загроз національній критичній інфраструктурі України як основа забезпечення її безпеки та стійкості. *Вісник Харків. націон. унів-ту внутр. справ*. 2024. № 1. С. 237–250.

9. Плахотнюк Р.В. Забезпечення стійкості критичної інфраструктури в Україні в умовах сучасних викликів. *Економічний простір*. 2024. № 195. С. 47–54.

10. Страхніцький Я.О. Кластерний підхід до забезпечення захисту критичної інфраструктури в умовах воєнного стану в Україні. *Інвестиції: практика та досвід*. 2023. № 23. С. 163–169.

11. Шпатакова О.Л., Іваненко Р.О, Погребицький М.О. Перспективи відновлення критичної інфраструктури на деокупованих територіях України. *Економіка та суспільство*. 2022. № 40.

12. Крутов В.В., Форноляк В.М. Система суб'єктів боротьби з тероризмом, їх адміністративно-правовий статус. *Інформаційна безпека людини, суспільства, держава.* 2019. Вип. 2. С. 56–64.

13. Леонов Б.Д. Проблеми правового забезпечення антидиверсійної захищеності об'єктів критичної інфраструктури в умовах воєнного стану. *Інформація і право*. 2022. № 3.

14. Гордієнко С.Г., Доронін І.М. Інформаційно-правові аспекти захисту критичної інфраструктури України. *Інформація і право*. 2024. № 3. С. 115–123.

15. Казьмірук С.Д., Леонов Б.Д., Омельян О.С. Забезпечення кібербезпеки об'єктів критичної інфраструктури на основі використання штучного інтелекту в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2024. № 6.

16. Качаровський А.П. Актуальні питання інформаційно-аналітичного забезпечення контррозвідувального захисту об'єктів критичної інфраструктури у сфері електроенергетики в сучасних умовах. *Науковий вісник*. 2023. № 85. С. 146–153.

17. Кучма О.М., Котух Є.В. Критична інфраструктура та кіберзагрози: досягнення стратегічних цілей державного аудиту щодо кіберзахисту критичної інфраструктури. *Наукові перспективи*. 2023. № 10.

18. Мануілов Я.С. Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. *Інформація і право*. 2023. № 1. С. 154–167.

19. Пядишев В.Г. Кібербезпека критичних інфраструктур: закордонний досвід та українські реалії. *Теоретичні та практичні аспекти забезпечення національної безпеки*. 2022. № 4. С. 229–234.

20. Скіцько О.І., Ширшов Р.А. Система управління інформаційною безпекою як інструмент підвищення захисту та ефективності об'єктів критичної інфраструктури. *Міжнародний науковий журнал інженерії*. 2023. № 2. С. 12–22.

21. Іванов Ю.А. Актуальні питання розбудови в Україні національної системи захисту критичної інфраструктури крізь призму реалій воєнного часу. *Збірник наукових праць*. 2023. № 86. С. 16–23.

22. Іванов Ю.А. Правове регулювання та організація оперативно-розшукової та контррозвідувальної діяльності. *Науковий вісник*. 2023. № 87. С. 88–105.

23. Іванов Ю.А. Особливості критичної інфраструктури як об'єкта контррозвідувального захисту. *Збірник наукових праць*. 2024. № 89. С. 96–102.

24. Меленті Є.О. Особливості взаємодії Служби безпеки України зі складовими сил безпеки і оборони у сфері захисту критичної інфраструктури. *Науковий вісник*. 2023. № 88. С. 93–103.

25. Осипчук І.І. Адміністративно-правові засади діяльності Служби безпеки України як суб'єкта забезпечення критичної інфраструктури : автореф. дис. ...канд. юрид. наук : 12.00.07. Київ. 2021. 20 с.

26. Слюсарчук І.В. Критична інфраструктура в умовах війни: питання доступу громадськості до публічної інформації. *Збірник наукових праць*. 2023. № 86. С. 81–88.

27. Стрельбицька Л.М., Стрельбицький М.П. Міжнародно-правове регулювання забезпечення енергетичної та ядерної безпеки України в умовах війни. *Інформація і право*. № 1. 2023.

28. Тарнавський Ю.Є., Коваленко С.М. Проблематика безпеки об'єктів критичної інфраструктури України через призму зарубіжних наукових досліджень. *Науковий вісник*. 2023. № 85. С. 103–110.

29. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження Кабінету Міністрів України від 06.12.2017 р. № 1009-р. *Офіційний вісник України*. 2018. № 7.

30. Про критичну інфраструктуру: Закон України від 16.11.2021р. № 1882-IX. *Голос України*. 2021. № 236.

31. Про внесення змін до постанови Кабінету Міністрів України від 09 жовтня 2020 р. : постанова Кабінету Міністрів України від 16.12.2022р. № 1384. *Офіційний вісник України*. 2022. № 101.