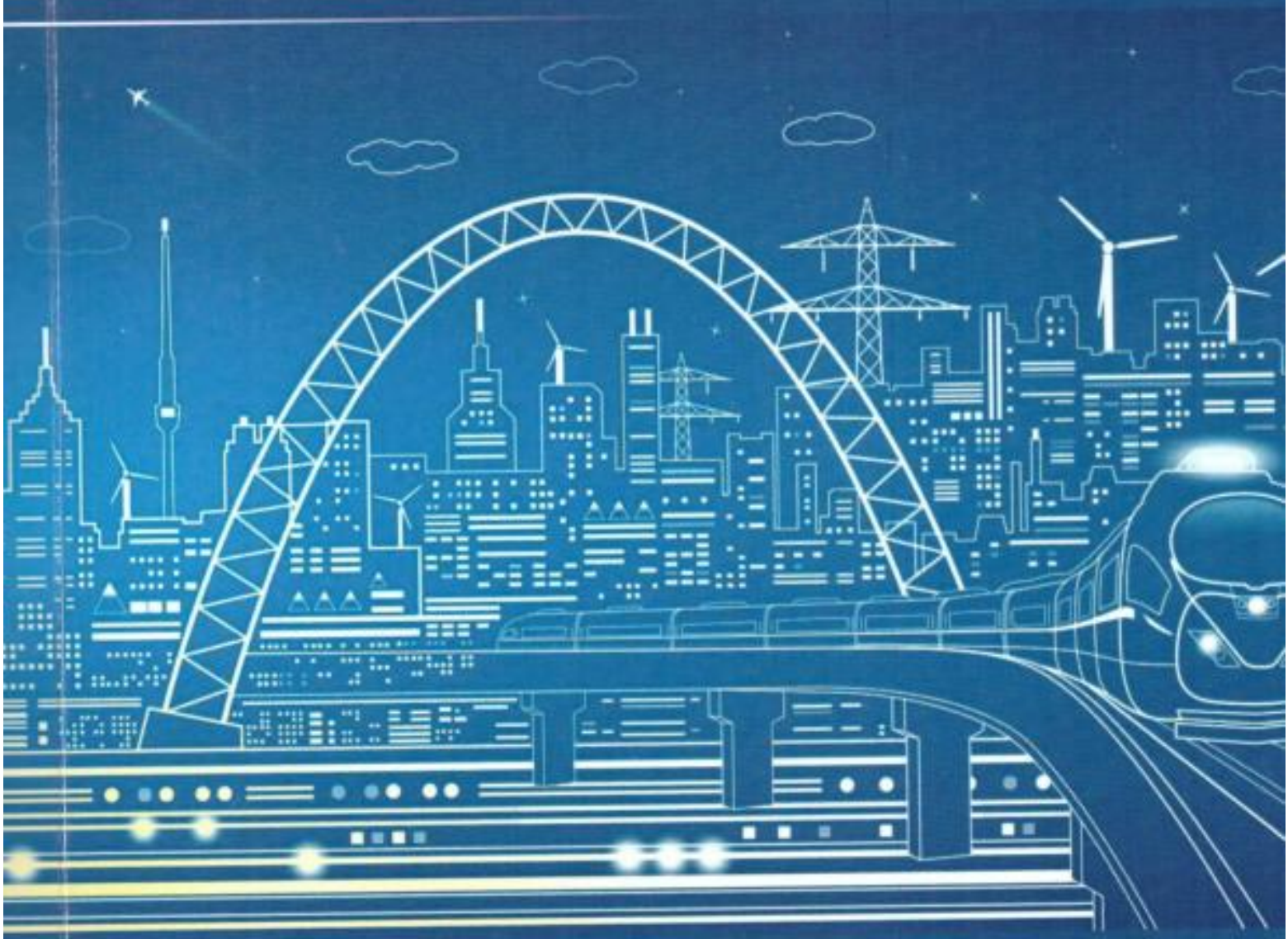
Т. В. Запорожець

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Навчальний посібник



Київ - 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

Т. В. ЗАПОРОЖЕЦЬ

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Навчальний посібник

Київ - 2024

УДК 351.86 (063)
З-33

Рецензенти:
доктор наук з державного управління, професор С.М.Домбровська
(Національний університет цивільного захисту України);
доктор наук з державного управління, доцент Н.О.Васюк
(Київський національний економічний університет імені Вадима Гетьмана);
доктор юридичних наук, професор, Н.М.Корчак
(Київський національний університет імені Тараса Шевченка)

Рекомендовано до друку Вченою Радою Навчально-наукового інституту публічного управління та державної служби (протокол № 6 від 6 листопада 2024 року)

Запорожець Т.В.
Державна політика у сфері захисту критичної інфраструктури: навчальний посібник. Київ: ДКС–Центр, 2024. 186 с.

ISBN 978-617-8080-12-9

Посібник висвітлює теоретичні основи та практичні підходи до захисту критично важливих об'єктів у сучасних умовах державотворення, розкриваючи концептуальні й правові аспекти, огляд міжнародних стандартів, методи моніторингу та кібербезпеки, що дозволить фахівцям вирішувати комплексні завдання у сфері захисту критичної інфраструктури як складової національної безпеки України.

Посібник орієнтований на студентів Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка, які навчаються за спеціальністю 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону». Він також може бути корисним фахівцям, на яких покладаються аналітичні, консультативно-дорадчі й організаційно-розпорядчі функції у сфері забезпечення захисту критичної інфраструктури України в межах своєї професійної компетенції

УДК 351.86 (063)

ISBN 978-617-8080-12-9

© Запорожець Т.В., 2024
© Київський національний університет імені Тараса Шевченка, 2024

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 5

ПЕРЕДМОВА 6

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 8

ГЛАВА 1. Захист критичної інфраструктури: теоретичні положення та класифікація *8*

1.1. Значення критичної інфраструктури для забезпечення державної стабільності 8

1.2. Поняття та класифікація критичної інфраструктури 19

1.3. Принципи та підходи до захисту критичної інфраструктури 28

ГЛАВА 2. Міжнародні стандарти та практики захисту критичної інфраструктури *38*

2.1. Огляд міжнародних стандартів: вплив на захист критичної інфраструктури 38

2.2. Особливості стандартів захисту у різних країнах 49

2.3. Взаємодія міжнародних організацій у сфері захисту критичної інфраструктури 59

ГЛАВА 3. Інституційно-правові основи державної політики у сфері захисту критичної інфраструктури *67*

3.1. Національне законодавство та регуляції 67

3.2. Роль та завдання органів державної влади у захисті критичної інфраструктури 76

3.3. Державно-приватне партнерство у галузі 91

Завдання для самоконтролю
Теми для самостійних робіт
Список рекомендованої літератури

РОЗДІЛ 2 ПРАКТИЧНІ ПІДХОДИ ТА ТЕХНОЛОГІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 111

ГЛАВА 4. Методи та технології захисту критичної інфраструктури *111*

4.1. Системи моніторингу та контролю 111

4.2. Технологічні рішення та інновації 117

4.3. Кібербезпека та захист інформації 122

ГЛАВА 5. Оцінка ефективності державних заходів захисту критичної інфраструктури *127*

5.1. Методи оцінки ризиків 127

5.2. Показники ефективності 133

5.3. Коригувальні заходи щодо вдосконалення 140

ГЛАВА 6. Кращі практики захисту критичної інфраструктури 146

6.1. Аналіз успішних кейсів з різних країн 146

6.2. Рекомендації для впровадження кращих практик 154

6.3. Перспективи розвитку державної політики у сфері захисту критичної інфраструктури 159

Завдання для самоконтролю
Теми для самостійних робіт
Список рекомендованої літератури

ГЛОСАРІЙ 170

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 176

ПЕРЕЛІК СКОРОЧЕНЬ

Скорочення та умовні позначення	*Повне словосполучення та поняття, що скорочуються*
ДПП	Державно-приватне партнерство
ДССЗЗІ	Державна служба спеціального зв’язку та захисту інформації України
ДСНС	Державна служба з надзвичайних ситуацій
ІКТ	Інформаційно-комунікативні технології
ISO	Система управління якістю
НАТО	Організація Північноатлантичного договору
ООН	Організація Обєднаних Націй
ОКІ	Об’єкти критичної інфраструктури
ЄС	Європейський Союз
КМУ	Кабінет Міністрів України
KPI	Ключові показники ефективності
МОЗ	Міністерство охорони здоров’я

ПЕРЕДМОВА

У світі, де загрози для функціонування держави та суспільства набувають все більш складного і непередбачуваного характеру, захист критичної інфраструктури виходить далеко за межі суто технічних рішень та постає як один із ключових пріоритетів держави для забезпечення стабільності, безпеки та розвитку.

Захист критичної інфраструктури є комплексним і багатогранним процесом, який вимагає не лише залучення передових технологій, але й розробки стратегічних підходів, ефективної державної політики та міжнародної співпраці. У цьому контексті виникає необхідність у поглибленому розумінні теоретичних основ і практичних аспектів державної політики в цій сфері, що і стало основною метою створення цього посібника.

Критична інфраструктура, до якої належать енергетичні системи, транспортні мережі, водопостачання, інформаційно-комунікаційні технології, фінансові установи, охорона здоров’я та багато інших життєво важливих секторів, забезпечує безперервне функціонування держави та суспільства. Її стійке і безперебійне функціонування має визначальне значення для економічної стабільності, національної безпеки, соціального благополуччя та життєзабезпечення громадян.

У першому розділі розглядаються теоретичні основи державної політики у сфері захисту критичної інфраструктури. У ньому детально розглядаються ключові аспекти, починаючи від визначення та класифікації критичної інфраструктури, значення її захисту для держави, до аналізу загроз та ризиків, які виникають у сучасному світі. Особлива увага приділяється міжнародним стандартам і практикам захисту, які можуть бути використані для підвищення національної стійкості, а також законодавчій базі, яка визначає роль державних органів та взаємодію з приватним сектором у сфері захисту критичної інфраструктури.

Другий розділ присвячений практичним підходам та технологіям, які можуть бути застосовані для забезпечення ефективного захисту критичної інфраструктури. У цьому розділі систематизовано сучасні методи та технології моніторингу, контролю, кібербезпеки та захисту інформації. Окрім того, розглядаються питання організації державного захисту, включаючи визначення ключових елементів критичної інфраструктури, розробку та впровадження національних планів захисту, а також механізми взаємодії між різними суб'єктами захисту. Не менш важливим аспектом є оцінка ефективності державних заходів, що включає аналіз ризиків, визначення показників ефективності та впровадження коригувальних заходів для постійного вдосконалення захисту критичної інфраструктури.

У завершальній частині посібника звернено увагу на кращі практики захисту критичної інфраструктури у різних країнах світу, які можуть слугувати зразком для впровадження у національних умовах. Ці практики базуються на реальних кейсах і надають цінні рекомендації для подальшого розвитку та вдосконалення державної політики у сфері захисту критичної інфраструктури.

Посібник розрахований на широкий спектр фахівців, які працюють у сфері державного управління, національної безпеки, а також дослідників і студентів, які прагнуть поглибити свої знання у цій сфері. Матеріали посібника можуть бути корисними для розробки стратегій та планів захисту критичної інфраструктури, для підвищення професійної компетентності та розвитку наукових досліджень.

Авторка висловлює щиру подяку своїм колегам, друзям та шановним рецензентам за зауваження та пропозиції, які надійшли від них під час редагування остаточного варіанта тексту навчального посібника.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ГЛАВА 1. Захист критичної інфраструктури: теоретичні положення та класифікація

1.1. Значення критичної інфраструктури для забезпечення державної стабільності

У сучасному світі критична інфраструктура відіграє ключову роль у забезпеченні стабільності та ефективності функціонування держави, оскільки вона забезпечує основу для стабільного функціонування економіки, безпеки та соціального життя країни. Критична інфраструктура розглядається як ключовий елемент національної безпеки. Закон «Про національну безпеку України» [1] підкреслює її важливість в контексті загальної стабільності держави, Закон «Про критичну інфраструктуру» [2] конкретизує заходи і стратегії для її захисту. Це відображає важливість критичної інфраструктури для забезпечення функціонування держави і її стабільності. Критична інфраструктура охоплює об’єкти, системи, мережі та послуги, від яких залежить життєдіяльність суспільства, і будь-яке порушення в їхній роботі може мати серйозні наслідки для держави.

Оскільки держава є ключовим елементом системи захисту критичної інфраструктури, її основна мета полягає в забезпеченні безперебійної роботи критичної інфраструктури, незалежно від типу власності об’єктів або мереж. Це є критично важливим для стабільного функціонування суспільства та підтримання його життєдіяльності. Враховуючи ці обставини, важливо підвищувати рівень усвідомлення і розуміння значення критичної інфраструктури у стратегічному управлінні державою та її інституціями. Це включає розробку ефективних політик, інтеграцію

новітніх технологій для моніторингу та захисту, а також активну співпрацю з приватним сектором і міжнародними партнерами для забезпечення комплексного підходу до захисту критичної інфраструктури.

Відтак, значення критичної інфраструктури обумовлюється наступними аспектами.

Економічна стабільність. Критична інфраструктура є основою економічної стабільності держави. Її функціонування безпосередньо впливає на економічну активність, оскільки енергетичні системи, транспортні мережі, телекомунікації та інші сектори критичної інфраструктури забезпечують діяльність промисловості, сільського господарства, фінансового сектору та інших економічних галузей [3].

Безперебійна робота цих систем є необхідною умовою для підтримки економічного зростання, розвитку бізнесу та залучення інвестицій. Наприклад, стабільне енергопостачання дозволяє промисловим підприємствам працювати на повну потужність, що сприяє виробництву товарів і послуг, забезпечуючи робочі місця та доходи для населення. Надійна транспортна інфраструктура забезпечує ефективну логістику, що знижує витрати на транспортування товарів, поліпшує доступ до ринків і підвищує конкурентоспроможність вітчизняної продукції.

Крім того, стійка інфраструктура сприяє економічній стабільності, мінімізуючи ризики, пов’язані з перериваннями в роботі ключових систем. Наприклад, надійність електромереж запобігає масовим відключенням електроенергії, що може мати катастрофічні наслідки для економіки, включаючи зупинку виробництва, порушення роботи фінансових ринків та дестабілізацію банківської системи [4].

Комунікаційні мережі є ще одним критично важливим елементом, оскільки вони забезпечують безперервний обмін інформацією, що є основою для сучасних економічних процесів. Безперебійний зв’язок дозволяє підприємствам, державним установам та громадянам ефективно

взаємодіяти, підтримуючи таким чином економічну активність і сприяючи інноваціям.

В умовах глобалізації та зростаючої інтеграції світової економіки наявність стійкої критичної інфраструктури також є ключовим фактором для залучення іноземних інвестицій [5]. Інвестори прагнуть вкладати кошти в країни, де інфраструктура забезпечує надійність і передбачуваність бізнес-операцій, мінімізуючи ризики, пов’язані з можливими збоями. Це не лише гарантує безпеку населення, але й є фундаментом для сталого економічного розвитку, підтримки конкурентоспроможності на міжнародному рівні та забезпечення добробуту суспільства.

Національна безпека. Цілком очевидно, що вразливість критичної інфраструктури становить серйозну загрозу для держави, оскільки її порушення здатні спричинити значні наслідки для функціонування суспільства, економіки та безпеки. Зв’язок між національною безпекою та захистом критичної інфраструктури є ключовим елементом розвитку суспільства та забезпечення його стабільного функціонування. Термін «критична інфраструктура», відтоді як виник у США в 1990-х роках, еволюціонував, охоплюючи аспекти безпеки [6]. Технологічний прогрес, поряд із значними перевагами, приніс й нові виклики, оскільки сучасні загрози, такі як кібератаки й асиметричні методи впливу, здатні порушити функціонування важливих об’єктів. Це, своєю чергою, спричиняє ланцюгову реакцію з катастрофічними наслідками для економіки, суспільства та державного управління.

Важливість захисту критичної інфраструктури полягає в тому, що її дестабілізація через технологічні чи фізичні загрози може мати масштабні кризи. Атаки призводять до збоїв у роботі енергетичних систем, транспортних мереж або банківської інфраструктури, що впливає не лише на окремі сектори, але й на всі ключові аспекти національної безпеки. Наприклад, використання новітніх методів кіберзброї дозволяє завдати

серйозного удару по економіці, пошкоджуючи інфраструктуру без прямого військового вторгнення. Вказане підкреслює необхідність комплексного підходу до забезпечення безпеки - від технологічних рішень до правового регулювання та міжнародного співробітництва [7].

З огляду на це, підвищення стійкості критичної інфраструктури до таких загроз є необхідною складовою державної політики. Ефективне реагування на виклики вимагає не лише наявності планів дій на випадок надзвичайних ситуацій, але й впровадження попереджувальних заходів для зниження ризиків. У сучасному науково-технологічному контексті, кібербезпека є ключовим елементом захисту критичних об’єктів. Недоліки в інформаційних системах здатні стати інструментом дестабілізації не лише окремих секторів економіки, але й загалом державного управління. У зв’язку з цим, впровадження новітніх технологій захисту, систем шифрування даних та механізмів раннього виявлення загроз є надзвичайно важливим [8].

Забезпечення стійкості критичної інфраструктури вимагає також координації зусиль між державними структурами, приватним сектором та міжнародними організаціями. Важливим науково-практичним аспектом є інтеграція знань про потенційні загрози та найкращі методи їх нейтралізації, а також розробка загальносистемних стратегій для мінімізації ризиків. Така співпраця дозволяє не лише ефективно реагувати на існуючі загрози, але й адаптувати державну політику під постійно змінювані умови сучасного світу.

Отже, надійний захист критичної інфраструктури є ключовим елементом у стратегіях національної безпеки, оскільки забезпечує стійкість держави перед різноманітними загрозами, що постійно еволюціонують, знижує ризик дестабілізації держави, сприяє забезпеченню її стійкості до зовнішніх та внутрішніх загроз і є надзвичайно важливим у стратегічному плануванні національної безпеки, стає першочерговим завданням для урядів

усіх країн.

Соціальна стабільність. Функціонування критичної інфраструктури безпосередньо впливає на соціальну стабільність в державі. Стабільна робота об’єктів і систем критичної інфраструктури забезпечує впевненість громадян у безпеці свого життя. Навпаки, відмова або порушення в роботі цих систем можуть спричинити паніку, соціальні заворушення, зниження рівня довіри громадян до державних інституцій та загальну дестабілізацію суспільства. Наприклад, тривалі перебої з електропостачанням, водопостачанням чи доступом до інтернету викликають соціальну напругу, призводять до масових протестів і загострення політичної ситуації в країні. Відповідно, забезпечення надійного функціонування критичної інфраструктури є необхідним для підтримання соціального спокою, довіри населення до держави та запобігання соціальним конфліктам.

У цьому контексті критична інфраструктура забезпечує безперервне надання основних послуг, від яких залежить повсякденне життя громадян. До таких послуг належать енергопостачання, водопостачання, зв’язок, транспорт, медичне обслуговування, а також функціонування систем громадської безпеки. Стабільна робота цих об’єктів є критично важливою для забезпечення життєдіяльності суспільства, оскільки вони підтримують базові потреби населення, включаючи доступ до електроенергії, чистої води, можливість безперешкодного пересування та надання медичної допомоги. Будь-які перебої у функціонуванні цих систем породжують кризи громадського здоров’я, соціальні незадоволення або масові міграційні процеси.

Забезпечення громадського здоров’я та безпеки. Система охорони здоров’я, водопостачання, санітарні служби та інші об’єкти критичної інфраструктури мають вирішальне значення для захисту громадського здоров’я та забезпечення безпеки населення. Медичні установи, наприклад, залежать від стабільного постачання електроенергії, води, а також від

функціонування транспортних мереж для перевезення пацієнтів та медичних ресурсів. Будь-які перебої в роботі цих систем ставлять під загрозу життя і здоров'я громадян, що особливо критично під час надзвичайних ситуацій, таких як епідемії, стихійні лиха чи терористичні акти. Захист об'єктів критичної інфраструктури, пов'язаних з охороною здоров'я, гарантує надання своєчасної медичної допомоги, забезпечення населення чистою водою та ефективне управління санітарними умовами, що є необхідним для збереження здоров'я нації [9].

Під час пандемії COVID-19 було особливо помітно, наскільки залежить система охорони здоров'я від безперебійної роботи транспортних мереж для доставки медикаментів, постачання енергії для роботи життєво необхідного медичного обладнання та забезпечення належного санітарного режиму. Система водопостачання і санітарії також відіграє критичну роль у запобіганні розповсюдженню інфекційних захворювань, підтримуючи гігієнічні стандарти, необхідні для здорового життя населення [10].

Крім того, в умовах російського повномасштабного військового вторгнення на територію України важливість критичної інфраструктури зросла багаторазово. В умовах війни об'єкти охорони здоров'я та комунальні системи стають першочерговими мішенями для ворога, адже їх знищення або виведення з ладу може призвести до хаосу, паніки та масових жертв серед мирного населення. Військові конфлікти створюють додаткові загрози для критичної інфраструктури: обстріли, диверсії, кібератаки спричиняють тривалі перебої у функціонуванні лікарень, водопостачальних систем, санітарних служб та суттєво ускладнюють роботу медиків, погіршуючи гуманітарну ситуацію [11].

У таких умовах захист критичної інфраструктури набуває стратегічного значення для держави, оскільки він є запорукою виживання та відновлення нації в умовах війни. Забезпечення безперебійного постачання енергії, води та медикаментів, а також стійкість транспортних мереж є

критично важливими для підтримання обороноздатності та забезпечення медичної допомоги пораненим і хворим. Інвестиції у зміцнення та захист критичної інфраструктури, особливо під час війни, повинні бути пріоритетом державної політики, адже від цього залежить не лише безпека громадян, але й сама можливість подальшого існування держави [12].

Повсюдна цифровізація усіх сфер та забезпечення кібербезпеки критичної інфраструктури. Зі зростанням кіберзагроз інфраструктура, що забезпечує стабільність розвитку держави, стає вразливою до атак, здатних спричинити значні збитки. Цифровізація у сферах промислового виробництва та фінансів покращує продуктивність, але водночас збільшує ризик кібернападів. Фінансовий сектор зазнає значних втрат через несанкціоновані транзакції та викрадення даних, що впливає на довіру інвесторів і ринок. В енергетичному секторі загрози пов’язані з підвищеною інтеграцією мереж, а геополітичні чинники здатні дестабілізувати постачання енергії, що безпосередньо впливає на економічну стійкість [13].

До прикладу, енергетичний сектор зазнає значних перетворень завдяки інтеграції відновлювальних джерел енергії, розвитку інтелектуальних електромереж та переходу до децентралізованих систем виробництва та споживання енергії. Ці зміни, хоча й забезпечують більшу енергетичну незалежність і знижують ризики, пов’язані з централізованими джерелами енергії, водночас створюють нові виклики. Вони можуть призвести до виникнення нових вразливостей, таких як збільшення кількості потенційних цілей для кібератак або технічних збоїв. Тому ефективне управління цими ризиками є критично важливим для забезпечення національної стабільності.

Стрімкий розвиток автономних транспортних засобів і прогрес у сфері штучного інтелекту радикально змінюють транспортний сектор. Ці інновації мають потенціал для покращення безпеки і ефективності транспортних систем, проте також вводять нові елементи ризику.

Наприклад, автономні транспортні засоби та нові технології управління дорожнім рухом можуть бути вразливими до кібератак, що може вплинути на загальний транспортний ландшафт і викликати серйозні перебої у переміщенні людей і товарів. Стабільність транспортних систем має безпосередній вплив на функціонування економіки та забезпечення громадської безпеки.

Інформаційно-комунікаційні технології (ІКТ) змінили спосіб обміну даними та спілкування в нашому щоденному житті. Розвиток розумних міст, які базуються на даних і інтегрованих міських послугах, демонструє, як ІКТ можуть поліпшити управління міськими процесами і зробити мегаполіси більш ефективними. Проте ці технології також вносять нові ризики. Залежність від великих обсягів даних і розширене використання кодування можуть стати мішенями для кібератак, що може порушити функціонування критичних міських інфраструктур.

З розвитком кіберзагроз у глобальному вимірі ключовим елементом захисту критичної інфраструктури стає міжнародна співпраця. Стандарти, створені в рамках міжнародних угод, таких як Будапештська конвенція про кіберзлочинність, допомагають країнам ефективно реагувати на загрози, що часто не мають державних кордонів. Для забезпечення стійкості інфраструктури потрібна координація зусиль між урядами, приватними компаніями та міжнародними організаціями, які працюють над створенням глобальної системи протидії кібернападам.

Крім того, цифровізація потребує створення адекватної законодавчої бази та впровадження регуляторних механізмів, що стимулюють захист критичних систем. Законодавчі вимоги повинні передбачати як технічні стандарти кіберзахисту, так і відповідальність за їх порушення.

Людський фактор залишається ключовим аспектом забезпечення кібербезпеки. Підготовка кадрів, здатних ефективно реагувати на сучасні загрози, стає пріоритетом державної політики. Освітні програми мають

включати не лише теоретичні основи, а й практичні навички в умовах симуляції реальних кіберзагроз. До того ж, кожна критична інфраструктура повинна мати резервні сценарії дій на випадок успішних кібератак. Розробка планів відновлення функцій, резервних мереж та інструментів швидкого реагування є необхідними складовими сучасної стратегії захисту.

Швидкий розвиток інновацій і технологій впливає також на управління ризиками, оскільки децентралізовані системи і автономні механізми замінюють централізовані мережі з автоматизованим управлінням. Ці зміни можуть підвищити стійкість завдяки гнучкості та надмірності, проте вони також створюють нові форми вразливостей. Зокрема, зростання кількості потенційних слабких місць у децентралізованих системах і підвищений ризик кібератак на ці системи потребують нових стратегій захисту та адаптації.

Для ефективного управління цими змінами необхідно впроваджувати нові політики і стратегії, які враховують як переваги, так і нові ризики, пов’язані з технологічними перетвореннями. Інтеграція інновацій у стратегії захисту критичної інфраструктури допоможе зберегти її функціональність і підтримати загальну стабільність держави. Окрім того, ефективне управління ризиками цифровізації критичної інфраструктури повинно базуватися на комплексному підході, що охоплює не лише технологічні, але й регуляторні, освітні та міжнародні аспекти [14].

При цьому варто зазначити, що зростаючі інвестиції в інфраструктуру створюють можливості для забезпечення стійкості. У найближчі десятиліття заплановано значні інвестиції в нові об’єкти інфраструктури, що створює унікальну можливість для інтеграції питань стійкості з самого початку проектування і реалізації інфраструктурних проектів. З огляду на це, забезпечення стійкості критичної інфраструктури повинно стати пріоритетом у процесі планування та реалізації нових проектів.

Згідно з останнім аналізом Організації економічного співробітництва і

розвитку (ОЕСР), для покриття потреб в інвестиціях в інфраструктуру до 2030 року необхідно близько 95 трильйонів доларів США. Багато країн з розвиненою економікою стикаються з проблемою застарілої інфраструктури, яка потребує оновлення. Інновації в цій сфері можуть значно підвищити продуктивність і ефективність інфраструктурних систем, проте для досягнення цього важливо, щоб інвестиції були направлені на стійкі і адаптивні рішення [15].

У 2017 році ОЕСР розробила Концепцію кращого управління інфраструктурою, спрямовану на удосконалення підходів до планування, реалізації та управління інфраструктурними проектами [16].

Ця концепція відповідає на потребу забезпечення стійкості та ефективності інфраструктурних інвестицій у світлі швидко змінюваного середовища і зростаючих викликів. Концепція підкреслює важливість забезпечення економічної ефективності інфраструктурних проектів. Це означає, що проекти повинні бути сплановані таким чином, щоб максимізувати користь при мінімізації витрат. ОЕСР рекомендує використання сучасних методів оцінки витрат і вигод, а також забезпечення прозорості у фінансуванні проектів. Концепція акцентує також увагу на необхідності врахування інтересів усіх зацікавлених сторін, включаючи місцеві громади та інвесторів, що пов’язується із участю громадськості у процесах прийняття рішень, а також забезпеченням рівного доступу до інфраструктурних послуг. Інклюзивність допомагає враховувати різні потреби та забезпечує соціальну справедливість.

Враховуючи швидкі технологічні зміни, ОЕСР рекомендує інтегрувати сучасні інновації у процес управління інфраструктурою, зокрема використання новітніх технологій для моніторингу та управління інфраструктурними системами, а також впровадження нових методів і рішень, що сприяють підвищенню ефективності та стійкості.

ОЕСР пропонує низку наступних практичних рекомендацій для

реалізації концепції ефективного управління інфраструктурою:

– оцінка життєвого циклу проектів з метою комплексного дослідження потенційних витрат і вигод протягом усього життєвого циклу інфраструктури, включаючи етапи проектування, будівництва, експлуатації та утилізації;

– впровадження новітніх технологій для покращення управління інфраструктурою, таких як автоматизовані системи моніторингу і аналітики даних;

– залучення громадськості через організацію консультаційних процесів з громадами з метою отримання зворотного зв’язку і врахування їхніх потреб у плануванні та реалізації інфраструктурних проектів;

– стратегічне планування та розробка документів, які включають прогнози можливих ризиків і сценарії адаптації до змінюваних умов;

– моніторинг та регулярне проведення оцінок ефективності і стійкості інфраструктурних проектів, а також коригування планів і стратегій відповідно до отриманих результатів.

Концепція ОЕСР також надає важливі рекомендації для забезпечення стійкості і ефективності інфраструктурних проектів, що є ключовим аспектом для підтримки загальної стабільності держави і підвищення якості життя населення.

Таким чином, активне і продумане впровадження інновацій у процесі інвестицій в інфраструктуру може забезпечити підвищення стійкості систем, допомагаючи зберігати їх функціональність і надійність, що, в свою чергу, підтримує загальну стабільність держави.

Отже, критична інфраструктура є основою стабільного функціонування держави, економіки та суспільства. Її захист та ефективне управління мають стратегічне значення для забезпечення національної безпеки, економічної стабільності, соціального благополуччя та захисту громадського здоров’я. Державна політика у сфері захисту критичної

інфраструктури повинна бути орієнтована на створення комплексної системи заходів, що включає правове регулювання, розвиток технологій захисту, міжнародне співробітництво та постійне вдосконалення підходів до управління ризиками і загрозами. Лише за таких умов надійний захист критичної інфраструктури та стійкість держави перед викликами сучасного світу можна вважати гарантованим.

1.2. Поняття та класифікація критичної інфраструктури

Зусилля урядів щодо захисту критичної інфраструктури навряд чи є чимось новим. У Сполучених Штатах перші спроби були кодифіковані ще в 1998 році в Директиві 63 щодо захисту критичної інфраструктури, у якій визначено, що «Критичні інфраструктури - це фізичні та кіберсистеми, необхідні для мінімального функціонування економіки та уряду. Вони включають, але не обмежуються ними, телекомунікації, енергетику, банківську справу та фінанси, транспорт, системи водопостачання та екстрені служби, як державні, так і приватні» [17].

Ця місія здається цілком зрозумілою, оскільки встановлюються завдання налагодити комплексні моделі державно-приватної співпраці з питань ефективного функціонування об’єктів критичної інфраструктури та забезпечення надання основних послуг уряду, економіці та громадськості.

Сполучені Штати Америки стали першою країною, яка не лише розробила, але й впровадила концепцію критичної інфраструктури (КІ) та її захисту. Вперше поняття «критична інфраструктура» було офіційно визначено у США в 1996 році, але після терактів 11 вересня 2001 року його зміст значно розширився та уточнився. Важливим кроком у цьому напрямі стало прийняття 23 жовтня 2001 року закону, відомого як USA PATRIOT Act, який закріпив визначення критичної інфраструктури та підкреслив її безпосередній зв’язок із національною внутрішньою безпекою [18].

Після прийняття цього закону в США було сформовано цілу низку

нормативно-правових актів, спрямованих на забезпечення належного рівня захисту критичної інфраструктури. Ці заходи включали реорганізацію державних структур, зміну системи розподілу відповідальності та повноважень між різними державними і приватними суб'єктами. Увага до захисту КІ не обмежувалася лише створенням нових правових норм, але й включала модернізацію управлінських підходів, покращення інформаційно-аналітичної підтримки для прийняття рішень, впровадження передових технологій та активне навчання персоналу і населення.

США продовжують утримувати лідерство у сфері захисту критичної інфраструктури завдяки постійному вдосконаленню своїх підходів. Важливу роль відіграє не тільки безпека та стійкість самої інфраструктури, але й забезпечення стабільності ланцюгів постачання критично важливих ресурсів, матеріалів, технологій та послуг. Цей комплексний підхід розширює поняття національної безпеки, включаючи в нього всі аспекти, які забезпечують стійкість країни перед загрозами будь-якого характеру.

Цей досвід став основою для інших країн, які також стали приділяти більше уваги захисту своєї критичної інфраструктури, розробляючи власні стратегії та законодавчі рамки. Таким чином, США не лише започаткували концепцію захисту КІ, але й продовжують вдосконалювати її, забезпечуючи свою національну безпеку на сучасному рівні.

Зважаючи на зростання загроз тероризму в розвинених країнах, у 1998 році почалися активні дискусії щодо вразливості національних інфраструктур. Аналіз охоплював не лише кібернетичні системи, але й інші важливі сектори суспільного життя. У Сполучених Штатах прийняття Президентської Директиви 63 (1998 рік) визначило критичну інфраструктуру як базові системи, що можуть мати фізичну або віртуальну форму, і чиє порушення або пошкодження може вплинути на функціональність економіки та безпеку держави. До таких систем були віднесені телекомунікації, енергетичні системи, банківські та фінансові

послуги, транспорт, водопостачання, а також рятувальні служби.

У Європі також почали звертати увагу на питання захисту критичної інфраструктури. У 1998 році в багатьох європейських країнах було розпочато національні ініціативи з цього питання, з особливим акцентом на ІКТ, які становили важливий елемент для забезпечення безпеки. У Великій Британії, зокрема, наприкінці 1999 року було визначено критичну національну інфраструктуру як системи, безперебійне функціонування яких є життєво важливим для держави, а їх пошкодження або знищення може спричинити значні економічні або соціальні наслідки, а також становити загрозу життю громадян [19]. Серед таких систем були енергетика, водопостачання, транспорт, телекомунікації, охорона здоров'я, громадські та рятувальні служби, банківська справа, юстиція, соціальні послуги, а також наукові та освітні заклади.

У XXI столітті поняття критичної інфраструктури постійно розширюється, охоплюючи нові сфери суспільного життя через стрімкий розвиток технологій та зростання нових загроз. Особливо актуальними стають питання кібербезпеки, оскільки цифровізація систем енергетики, фінансів, транспорту та комунікацій збільшує ризики кібератак, що можуть мати катастрофічні наслідки.

Після терористичних нападів 11 вересня 2001 року в США тема захисту критичної інфраструктури набула нового рівня важливості. Це стало поштовхом для розробки в лютому 2003 року Національної стратегії фізичного захисту критичної інфраструктури та ключових активів, в якій було надано більш широке визначення критичної інфраструктури. Вона включала як матеріальні, так і віртуальні системи та об'єкти, які є життєво важливими для забезпечення національної безпеки, економічної стабільності та здоров'я населення. Серед таких секторів були сільське господарство, продовольство, вода, охорона здоров'я, телекомунікації, енергетика, транспорт, банківська справа, хімічна промисловість та поштові

послуги. До ключових активів було віднесено національні культурні пам’ятки, атомні електростанції, дамби та місця великого скупчення людей [19].

Оскільки більшість сучасних загроз є транскордонними, у захисті критичної інфраструктури ключову роль відіграє міжнародне співробітництво. Створення міжнародних стандартів і механізмів обміну інформацією, таких як Будапештська конвенція про кіберзлочинність [20], дозволяє країнам ефективніше координувати свої зусилля для попередження та реагування на надзвичайні ситуації. Прийнята у 2001 році Радою Європи, вона забезпечує правову базу для міжнародної співпраці у протидії кіберзлочинам, зокрема злочинам, які становлять загрозу для критичної інфраструктури. Основні положення Конвенції та її значення для захисту критичної інфраструктури повзуються із:

– *криміналізацією діянь у кіберпросторі* (Конвенція встановлює єдиний набір кримінальних злочинів, які охоплюють неавторизований доступ до комп’ютерних систем; перехоплення даних; втручання у функціонування комп’ютерних систем, що є критичним для захисту енергетичних, фінансових та інформаційних мереж); такі положення є важливими для захисту об’єктів критичної інфраструктури від зловмисних кібератак, які можуть паралізувати діяльність ключових секторів економіки, транспорту чи зв’язку;

– *правове регулювання обміну інформацією* (Конвенція створює правові основи для міжнародної співпраці та обміну даними між країнами щодо розслідування кіберзлочинів, що дозволяє забезпечити оперативне реагування на атаки на критичну інфраструктуру, що мають транскордонний характер, та ефективно обмінюватися інформацією між правоохоронними органами різних країн;

– *процедурні заходи для збереження доказів* (Конвенція вимагає від країн-учасниць зберігати дані про трафік, які можуть використовуватися для

виявлення та запобігання кіберзлочинам, що також є важливим для захисту критичної інфраструктури; при цьому відстеження активності у кіберпросторі допомагає запобігти кібератакам на об’єкти, такі як електричні мережі чи системи водопостачання.

Додатковий Протокол 2021 року передбачає посилення міжнародного співробітництва, зокрема надання спрощеного доступу до електронних доказів у межах розслідувань, що стосуються кіберзлочинності [21]. Для захисту критичної інфраструктури цей протокол є критичним, оскільки кіберзлочини часто мають міжнародний характер і потребують негайного обміну доказами між країнами.

Конвенція про кіберзлочинність та її протоколи створюють правову основу для захисту критичної інфраструктури, яка зазнає нових кіберзагроз в умовах швидкого розвитку технологій. Міжнародна координація та обмін інформацією між державами, що передбачено Конвенцією, допомагають посилити кіберзахист ключових об’єктів інфраструктури, мінімізуючи ризики масштабних порушень у їхньому функціонуванні [20].

Інтеграція європейських економік та взаємозалежність між країнами-членами ЄС, а також спільні загрози призвели до ухвалення документа «Захист критичної інфраструктури у боротьбі з тероризмом». У ньому критична інфраструктура визначається як сукупність фізичних об’єктів, інформаційних технологій та мереж (транспортних, енергетичних тощо), порушення або знищення яких може мати серйозні наслідки для здоров’я, безпеки громадян, а також для нормального функціонування урядів держав-членів.

Документ є першим звітом Європейської Комісії щодо реалізації Стратегії безпеки ЄС на 2020-2025 роки. Основна мета цього документа полягає у забезпеченні прогресу в побудові безпечного середовища для громадян Європейського Союзу та підвищенні стійкості до сучасних загроз [22]. У зв’язку з останніми терористичними атаками в Європі,

документ акцентує на потребі посилених дій ЄС для забезпечення безпеки своїх громадян. Стратегія базується на попередніх досягненнях у межах Європейського порядку денного безпеки на 2015-2020 роки. Документом передбачається чотири стратегічні пріоритети:

– *забезпечення стійкості критичної інфраструктури*. Пандемія COVID-19 підкреслила необхідність захисту важливих секторів і систем від загроз, таких як терористичні атаки, кібератаки, гібридні загрози, зміни клімату, а також порушення ланцюгів постачання.

– *боротьба з новими загрозами*. Це включає захист від технологічних загроз (дрони, 5G, штучний інтелект), кібератак і маніпуляцій в інформаційному просторі.

– *захист від тероризму та організованої злочинності*. ЄС акцентує увагу на боротьбі з транснаціональними злочинними мережами.

– *формування європейської екосистеми безпеки*. Це передбачає посилення співпраці між державними структурами, приватними компаніями та громадянським суспільством.

– *посилення кібербезпеки*. У звіті підкреслюється важливість оновлення існуючого законодавства для підвищення стійкості цифрових інфраструктур, особливо у фінансовому секторі, енергетиці та мережевих системах.

Загалом, звіт акцентує увагу на необхідності тісної співпраці всіх рівнів управління для створення безпечного середовища у всіх секторах економіки, від енергетики до фінансових послуг, з метою захисту критичної інфраструктури та забезпечення стійкості до сучасних загроз. Цей документ став основою для подальшого посилення зусиль у сфері захисту критичної інфраструктури на рівні ЄС [22].

Отже, критична інфраструктура - це *комплекс секторів і елементів, що забезпечують життєво важливі функції для стабільного функціонування держави* і будь-яке порушення їх роботи, особливо

внаслідок терористичних актів або інших загроз, може призвести до серйозних наслідків у різних сферах. Ці складові є ключовими для національної безпеки, що включає: політичну стабільність держави, включно з безперебійним функціонуванням державного управління; обороноздатність країни; стабільність економіки; життя та здоров'я громадян, а також їхнє майно; функціонування транспортних, інформаційних і комунікаційних систем; підтримання житлових умов.

Таке визначення підкреслює важливість критичної інфраструктури не лише в стабільних умовах суспільного розвитку, але й під час кризових ситуацій, що можуть бути викликані як зовнішніми, так і внутрішніми факторами - природними, техногенними або соціальними.

При визначенні елемента інфраструктури як критичного використовуються такі критерії:

– територіальний масштаб наслідків (можуть бути транскордонні, національні, регіональні або місцеві наслідки);

– рівень наслідків (гуманітарні, матеріальні, економічні, політичні чи екологічні збитки);

– тривалість наслідків (час від настання негативних наслідків (негайно, протягом 24 годин) і їхня тривалість (до 24 годин, 3 діб тощо).

Таким чином, критична інфраструктура є складною системою, де взаємопов'язаність між секторами робить її надзвичайно вразливою до різного роду загроз. Тому захист таких об'єктів є пріоритетним завданням держави, зокрема шляхом запровадження нових політик, які враховують сучасні виклики та ризики.

Критична інфраструктура складається з об'єктів, систем і мереж, які є життєво важливими для нормального функціонування суспільства, економіки, а також для забезпечення національної безпеки та громадського порядку. Ці об'єкти мають бути захищеними від різноманітних загроз, включаючи тероризм, природні катастрофи, техногенні аварії та

кібернапади, оскільки їхня нездатність функціонувати може мати серйозні наслідки для суспільства та держави. Вони включають, але не обмежуються наступними секторами, наведеними у таблиці 1.

Таблиця 1

Сектори та об’єкти критичної інфраструктури

Сектори	**Об’єкти**
Енергетика та енергопостачання	- електростанції (атомні, теплові, гідроелектростанції, вітрові тощо) - електричні мережі та системи розподілу електроенергії - системи постачання нафтопродуктів, газу та інших енергетичних ресурсів
Транспортна інфраструктура	- автомобільні дороги, залізниці - аеропорти та морські порти - метрополітени та громадський транспорт - логістичні центри та транспортні вузли
Водопостачання та водовідведення	- водосховища, дамби - системи водопостачання та каналізаційні мережі - очисні споруди
Охорона здоров’я	- лікарні, медичні центри - системи екстреної медичної допомоги - постачання ліків та медичних матеріалів
Інформаційні та телекомунікаційні системи	- інтернет-мережі та дата-центри - мобільні та стаціонарні телекомунікаційні мережі - системи кібербезпеки
Фінансовий сектор	- банківські установи та платіжні системи - системи управління фінансовими потоками - біржі, страхові та пенсійні інституції
Продовольчий сектор	- сільське господарство - харчова промисловість - продовольчі запаси та торгівля продуктами
Урядові та адміністративні установи	- установи центрального та місцевого управління - органи правопорядку та національної безпеки - об’єкти, що забезпечують функціонування органів державної влади
Хімічна та біологічна промисловість	- заводи з виробництва хімічних речовин - лабораторії та підприємства з небезпечними матеріалами
Засоби масової інформації	- телевізійні та радіокомпанії - новинні агентства - інформаційні портали та медіаплатформи

Розглянемо поняття «захист критичної інфраструктури». Поняття «захист критичної інфраструктури» можна розглядати як багатогранне

завдання, яке включає в себе заходи для попередження, захисту та зниження впливу загроз на ключові елементи державної інфраструктури. Захист у цьому контексті означає забезпечення безпеки об’єктів, які є критично важливими для функціонування держави та суспільства. Йдеться не лише про захист фізичних об’єктів, але й про організацію системного управління ризиками. Захист критичної інфраструктури є процесом, що включає:

– виявлення та захист ключових секторів інфраструктури держави, таких як енергетика, транспорт, комунальні послуги, фінансові та інформаційні системи. ці сектори є критичними для забезпечення безпеки, стабільності та функціональності держави та суспільства;

– забезпечення раннього попередження про можливі загрози через системи моніторингу та кризового управління, що допомагає запобігати або мінімізувати вплив потенційних загроз на критичну інфраструктуру.

Основними елементами критичної інфраструктури є сектори, які забезпечують стабільне функціонування державного управління, економіки, безпеки та надання життєво важливих послуг. Це включає: забезпечення функціонування державних інститутів та органів влади; забезпечення належного функціонування економічних систем та публічних послуг; підтримання громадського порядку та соціальної стабільності.

Загрози для критичної інфраструктури можуть бути як зовнішніми (природні катастрофи, терористичні акти), так і внутрішніми (технічні збої, інсайдерські атаки). Розуміння та оцінка цих загроз дозволяють організувати належний рівень захисту та впровадити системи моніторингу для попередження можливих катастроф.

Процес захисту критичної інфраструктури передбачає проведення ретельного аналізу, який включає:

1. Виявлення об’єктів критичної інфраструктури на різних рівнях: національному, регіональному та місцевому.
2. Оцінку можливих ризиків для цих об’єктів.

3. Аналіз вразливості окремих секторів.
4. Прийняття профілактичних заходів для забезпечення їх захисту.

Ключовою частиною цього процесу є оцінка ризиків, яка допомагає передбачити ймовірність негативних подій і їх можливі наслідки для інфраструктури. Ризик визначається як взаємозв'язок між імовірністю негативної події та її наслідками, що залежить від вразливості об'єкта та рівня загроз [23, с. 25].

Таким чином, захист критичної інфраструктури є комплексним завданням, що вимагає постійного моніторингу, аналізу та взаємодії між державними органами та приватним сектором. Це забезпечує належний рівень безпеки та стійкості держави перед загрозами, які постійно змінюються.

1.3. Принципи та підходи до захисту критичної інфраструктури

Захист критичної інфраструктури є ключовим елементом національної безпеки, оскільки ця інфраструктура забезпечує стабільне функціонування держави, економіки та суспільства. Сучасні загрози, як-от: тероризм, кібератаки, природні катастрофи та техногенні інциденти, вимагають ефективного управління безпекою критичних об'єктів. Це завдання стає ще складнішим у зв'язку з взаємозалежністю різних секторів інфраструктури, таких як енергетика, транспорт, зв'язок та фінанси.

Ефективний захист критичних об'єктів базується на декількох основних підходах та послуговується відповідними принципами функціонування. Кожен підхід спрямований на максимальне зменшення ризиків і мінімізацію наслідків у випадку кризових ситуацій.

Забезпечення захисту критичної інфраструктури потребує основоположного підходу, який враховує складність та взаємозалежність різних її секторів. Для ефективної охорони цих об'єктів необхідно

розробити стратегії, які об’єднують державний та приватний сектори, забезпечують належне управління ризиками та здатні адаптуватися до нових загроз. Важливою передумовою є те, що жоден окремий сектор не може бути повністю захищений ізольовано, оскільки він впливає на інші компоненти інфраструктури.

Саме тут ключову роль відіграє системний підхід, який дозволяє бачити критичну інфраструктуру як єдиний комплекс взаємопов’язаних елементів. Цей підхід сприяє узгодженню дій різних секторів та забезпечує координацію між усіма учасниками процесу - від державних органів до приватних підприємств.

Системний підхід до захисту критичної інфраструктури базується на кількох важливих принципах, які забезпечують його ефективність і комплексність. Ці принципи лежать в основі управління захистом критичних об’єктів.

Комплексність і координація між різними секторами та рівнями. Основою системного підходу є принцип комплексності, який передбачає необхідність інтеграції всіх секторів критичної інфраструктури в єдину систему захисту. Це означає, що всі компоненти інфраструктури, незалежно від їхньої специфіки, мають бути взаємопов’язаними та координованими для забезпечення загальної безпеки.

Взаємодія між державними і приватними структурами. Оскільки значна частина критичної інфраструктури перебуває під контролем приватних підприємств, ефективний захист можливий лише через тісну взаємодію державних і приватних структур. Державні органи повинні забезпечувати координацію та обмін інформацією з приватним сектором, щоб запобігти загрозам і швидко реагувати на кризи.

До завдань органів державної влади в межах цього підходу належить розробка національних стратегій захисту критичної інфраструктури, яка враховує всі сектори, від енергетики до транспорту та інформаційних

систем. Стратегія повинна охоплювати всі рівні – від загальнонаціонального до регіонального та місцевого. При цьому органи влади повинні створити механізми взаємодії між державними та приватними структурами, що включає розробку планів реагування на надзвичайні ситуації, обмін інформацією про загрози та ризики, а також спільне навчання для підвищення готовності до кризових ситуацій.

При побудові ефективної системи захисту критичної інфраструктури важливим є не лише системний, але й **ризик-орієнтований підхід**. Цей підхід акцентує увагу на визначенні і управлінні ризиками, які можуть вплинути на функціонування критичних об’єктів. В умовах зростаючих загроз, таких як тероризм, кібератаки та природні катастрофи, ризик-орієнтований підхід стає все більш актуальним і необхідним для забезпечення стабільності та безпеки.

Ризик-орієнтований підхід полягає в систематичній оцінці ризиків, пов’язаних із критичною інфраструктурою, та визначенні їхньої ймовірності і потенційного впливу. Він дозволяє фокусувати зусилля на найбільш критичних об’єктах, забезпечуючи максимальну ефективність використання ресурсів для їх захисту. Важливими елементами цього підходу є виявлення вразливостей, аналіз загроз та розробка заходів, спрямованих на зниження ризиків.

Ризик-орієнтований підхід передбачає реалізацію через принцип оцінки ризиків і вразливостей та фокус на найбільш критичні об’єкти.

Принцип оцінки ризиків передбачає ідентифікацію, аналіз та оцінку ризиків для критичних об’єктів інфраструктури. Оцінка ризиків включає визначення ймовірності виникнення негативних подій, а також їх можливого впливу на об’єкти. Зокрема, важливо оцінити вразливість об’єктів до зовнішніх і внутрішніх загроз, щоб зрозуміти, які з них можуть призвести до серйозних наслідків.

Фокус на найбільш критичні об’єкти зосереджується на пріоритезації

ресурсів і зусиль для захисту тих об’єктів, які є найбільш важливими для функціонування держави та суспільства. Визначення критичності об’єктів дозволяє максимально ефективно використовувати наявні ресурси, сприяючи захисту тих секторів, чия функціональність має найбільший вплив на безпеку та стабільність держави.

Таким чином, ризик-орієнтований підхід є необхідним компонентом у системі захисту критичної інфраструктури. Його принципи: оцінка ризиків та фокус на критичних об’єктах дозволяють забезпечити більш ефективний захист, знижуючи вразливість об’єктів та мінімізуючи можливі негативні наслідки. У сучасних умовах, коли загрози стають все більш складними і різноманітними, цей підхід стає ключовим у формуванні стратегії захисту критичної інфраструктури.

У рамках ризик-орієнтованого підходу до захисту критичної інфраструктури органи влади виконують кілька ключових завдань, критично важливих для забезпечення безпеки та стабільності в різних секторах. По-перше, проведення аналізу ризиків, вразливостей і потенційних загроз для кожного сектора критичної інфраструктури є основою для ефективного управління ризиками. Цей аналіз дозволяє державним органам ідентифікувати ключові вразливості, виявляючи слабкі місця у кожному секторі, які потребують термінового уваги та ресурсів для захисту. Крім того, важливо оцінити ймовірність загроз, таких як терористичні акти, кібератаки, природні катастрофи чи техногенні аварії. Це дозволяє зрозуміти характер загрози та її вплив на конкретний сектор, а також формувати рекомендації на основі отриманих даних для зниження ризиків і підвищення готовності до реагування на загрози.

По-друге, органи влади мають розробляти інструменти і методики для оцінки ризиків та створювати системи їхнього моніторингу. Це передбачає створення чітких методик оцінки ризиків, які дозволяють проводити регулярні та систематичні аналізи. Використання статистичних моделей,

програмного забезпечення для моніторингу загроз та вразливостей, а також методів збору і аналізу даних є важливими елементами цього процесу. Важливо також впроваджувати ефективні системи моніторингу, що дозволяють в реальному часі відстежувати стан критичної інфраструктури, виявляти потенційні загрози та вразливості, що забезпечує швидке реагування на зміни в середовищі безпеки.

Нарешті, оцінка ризиків і моніторинг повинні бути динамічними процесами, тому органи влади повинні забезпечувати постійне вдосконалення методик і інструментів на основі нових даних та технологічних досягнень. Цей підхід дозволяє забезпечити належний рівень захисту критичної інфраструктури та адаптуватися до постійно змінюваного середовища загроз.

Аналізуючи принципи та підходи до захисту критичної інфраструктури, варто важливо розглянути **інтегрований підхід**, який акцентує увагу на взаємозв’язку та взаємодії між різними секторами. Сучасні загрози для критичної інфраструктури, такі як кібератаки, тероризм або природні катастрофи, часто вимагають комплексного реагування, яке виходить за межі одного сектора. Інтегрований підхід дозволяє з’єднати зусилля різних секторів, таких як енергетика, транспорт, охорона здоров’я та інформаційні технології, що забезпечує більш ефективний захист і підвищує стійкість інфраструктури.

Основними принципами інтегрованого підходу є взаємозв’язок і взаємодія секторів, а також спільна координація між державними органами і приватним сектором.

Взаємозв’язок і взаємодія між різними секторами дозволяють краще розуміти, як зміни або кризи в одному секторі можуть вплинути на інші. Наприклад, перебої в енергетичній інфраструктурі можуть мати каскадні наслідки для транспорту і комунальних послуг, тому важливо, щоб усі сектори працювали спільно для розробки узгоджених стратегій захисту.

Спільна координація між державними органами і приватним сектором забезпечує обмін інформацією, ресурсами і технологіями, що робить систему захисту більш стійкою і адаптивною до нових загроз.

Завдання органів влади в рамках інтегрованого підходу включають забезпечення взаємодії між секторами для захисту критичної інфраструктури на національному рівні. Це передбачає створення платформ для обміну інформацією та кращими практиками, організацію спільних навчань і тренінгів для фахівців різних секторів. Важливо також, щоб державні органи координували свої дії з приватним сектором, проводячи спільні заходи з реагування на надзвичайні ситуації, що дозволяє швидше та ефективніше реагувати на потенційні загрози. Таким чином, інтегрований підхід до захисту критичної інфраструктури є необхідним для забезпечення надійності і стійкості всієї системи в умовах сучасних викликів.

Незважаючи на досягнуті успіхи в забезпеченні координації між різними секторами, необхідність адаптації до нових загроз залишалася нагальною. Сучасний світ характеризується швидким розвитком технологій та постійними змінами у загрозах, що вимагає від державних органів не лише інтеграції, а й здатності швидко реагувати на зміни. Саме тому виникає потреба в **адаптивному підході**, який зосереджується на гнучкості рішень і постійному вдосконаленні систем захисту.

Адаптивний підхід ґрунтується на *принципі гнучкості* у прийнятті рішень. Цей принцип передбачає, що органи влади повинні бути готовими оперативно змінювати свої стратегії та методи захисту в умовах нових викликів і загроз. Другим принципом є *постійне вдосконалення та оновлення систем захисту*. Це передбачає регулярний аналіз інцидентів, що сталися, та коригування стратегій захисту на основі отриманих даних; прогнозування майбутніх ризиків, адаптуючи свої системи захисту відповідно до нових умов. Основним завданням органів влади в межах адаптивного підходу є підтримка здатності державних структур швидко

адаптуватися до нових загроз, що, в свою чергу, вимагає модернізації захисних систем на основі новітніх технологій. У результаті адаптивний підхід доповнює інтегрований, створюючи більш динамічну та ефективну систему захисту критичної інфраструктури, здатну реагувати на швидко змінювані умови зовнішнього середовища.

В таких умовах, коли загрози стають все більш складними і різноманітними, важливо не лише реагувати на них, а й активно виявляти та нейтралізувати їх, що обумовлює потребу обгрунтувати **превентивний підхід** до захисту критичної інфраструктури, який зосереджується на запобіганні загрозам до того, як вони стануть реальністю. Превентивний підхід передбачає виявлення потенційних загроз, їх оцінку та впровадження систем раннього попередження. Це дозволяє не лише знизити ймовірність виникнення кризових ситуацій, але й підвищити загальний рівень готовності державних структур до можливих викликів. Таким чином, у рамках превентивного підходу органи влади можуть використовувати знання, отримані під час аналізу інцидентів в адаптивному підході, для створення ефективних механізмів запобігання, що, у свою чергу, підвищує стійкість критичної інфраструктури до загроз.

Превентивний підхід до захисту критичної інфраструктури акцентує увагу на проактивних заходах, які дозволяють запобігти виникненню загроз і забезпечити стійкість критично важливих систем. Основними принципами цього підходу є раннє попередження та профілактика, а також підготовка до потенційних кризових ситуацій.

Принцип раннього попередження та профілактики полягає у створенні та впровадженні систем раннього оповіщення про загрози, які можуть вплинути на критичну інфраструктуру. Системи раннього попередження повинні забезпечувати своєчасну інформацію про потенційні загрози, що дозволяє органам влади та відповідальним службам оперативно реагувати на можливі ризики через застосування технологій моніторингу,

аналізу даних і прогнозування, які допомагають виявити загрози ще до їх реалізації.

Підготовка до потенційних кризових ситуацій. Цей принцип акцентує увагу на підготовці персоналу та проведенні тренувань для оперативного реагування на кризові ситуації. Регулярні навчання, симуляції та тренінги допомагають підвищити рівень готовності співробітників до дій у випадку надзвичайних ситуацій. Важливо, щоб органи влади та відповідальні служби мали чітко узгоджені плани реагування, які враховують різні сценарії загроз.

В рамках превентивного підходу органи влади виконують кілька ключових завдань. По-перше, вони повинні розробити та впровадити системи раннього попередження про загрози, що включає інтеграцію сучасних технологій для моніторингу та аналізу ризиків. Це дозволяє виявляти потенційні загрози на ранніх стадіях і вжити необхідних заходів для їх нейтралізації. По-друге, органи влади мають забезпечити підготовку персоналу через регулярні навчання та тренінги. Це включає розробку сценаріїв кризових ситуацій і проведення симуляцій, що допомагають співробітникам набути практичного досвіду в умовах, наближених до реальних.

Відомо, що ефективність будь-якої стратегії забезпечення безпеки значною мірою залежить від належної правової основи. **Правовий підхід** виступає необхідним елементом у формуванні чітких нормативно-правових рамок, які регламентують зобов’язання державних органів, приватного сектора та громадських організацій у сфері захисту критичної інфраструктури.

В умовах постійно змінюваних загроз правовий підхід забезпечує створення стандартів безпеки та правових норм, які визначають обов’язки всіх учасників процесу. Наявність чіткої правової основи забезпечує узгодження дій різних секторів, унормування повноважень та

відповідальності суб’єктів управління у сфері, встановлення механізмів контролю за дотриманням стандартів безпеки тощо. Цей підхід також сприяє формуванню правового середовища, в якому можливе ефективне реагування на загрози та реалізація превентивних заходів. Без належної законодавчої бази запобігання загрозам та забезпечення стійкості інфраструктури можуть бути значно ускладнені. Правовий підхід до захисту критичної інфраструктури передбачає створення і впровадження чітких законодавчих рамок, які регулюють безпеку в цій сфері. Основними принципами цього підходу є регулювання захисту на законодавчому рівні та встановлення стандартів безпеки та відповідальності.

Принцип регулювання захисту на законодавчому рівні передбачає розробку законодавчих актів, що регламентують захист критичної інфраструктури. Законодавство має охоплювати всі аспекти безпеки, включаючи права та обов’язки органів державної влади, приватних компаній, а також механізми контролю за виконанням норм. Чіткі законодавчі акти формують правову основу для захисту інфраструктури, що забезпечує обґрунтованість і справедливість у регулюванні відносин між усіма учасниками процесу.

Принцип встановлення стандартів безпеки та відповідальності акцентує увагу на необхідності встановлення стандартів безпеки та відповідальності для всіх суб’єктів, залучених до управління критичною інфраструктурою. Встановлення відповідальності державних і приватних структур є важливим аспектом, оскільки воно стимулює їх дотримання норм безпеки та заохочує до активного управління ризиками. Законодавство повинно визначати конкретні вимоги до безпеки, а також передбачати механізми контролю за їх виконанням. Основні підходи, принципи та завдання органів влади у сфері захисту критичної інфраструктури наведено у таблиці 2.

Таблиця 2

Основні підходи, принципи та завдання органів влади у сфері захисту критичної інфраструктури

Підходи	**Принципи**	**Завдання органів влади**
Системний підхід	Комплексність і координація між різними секторами та рівнями	Розробка національних стратегій захисту критичної інфраструктури
	Взаємодія між державними і приватними структурами	Координація дій між різними державними установами та приватними підприємствами
Ризик-орієнтований підхід	Оцінка ризиків і вразливостей	Проведення аналізу ризиків, вразливостей і потенційних загроз для кожного сектора критичної інфраструктури
	Фокус на найбільш критичні об’єкти	Розробка інструментів і методик для оцінки ризиків та створення системи їхнього моніторингу
Інтегрований підхід	Взаємозв’язок і взаємодія секторів (енергетика, транспорт тощо)	Забезпечення взаємодії між секторами для захисту критичної інфраструктури на національному рівні
	Спільна координація між державними органами і приватним сектором	Організація спільних навчань та заходів для підвищення координації між секторами
Адаптивний підхід	Гнучкість у прийнятті рішень	Підтримка здатності державних органів швидко адаптуватися до нових загроз, модернізація захисних систем
	Постійне вдосконалення та оновлення систем захисту	Аналіз інцидентів і постійне коригування стратегій захисту інфраструктури
Превентивний підхід	Раннє попередження та профілактика	Створення та впровадження систем раннього оповіщення про загрози
	Підготовка до потенційних кризових ситуацій	Підготовка персоналу і проведення тренувань для оперативного реагування на кризові ситуації
Правовий підхід	Регулювання захисту на законодавчому рівні	Розробка законодавчих актів, що регламентують захист критичної інфраструктури
	Встановлення стандартів безпеки та відповідальності	Контроль за виконанням нормативних вимог щодо безпеки та відповідальності державних і приватних структур

Джерело: складено автором

Цілком очевидно, що для забезпечення національної безпеки та стабільності необхідна комплексна і систематизована стратегія. Захист критичної інфраструктури охоплює не лише виявлення та реагування на загрози, а й інтеграцію зусиль з усіх секторів, адже ефективність цього процесу залежить від взаємодії державних і приватних структур, а також адаптації до постійно змінюваних умов.

Кожен підхід: системний, ризик-орієнтований, інтегрований, адаптивний та превентивний, відіграє свою унікальну роль у формуванні надійної системи захисту. Правовий підхід, у свою чергу, забезпечує цю систему чіткою нормативно-правовою основою, що регулює обов’язки учасників і стандарти безпеки. Важливо, щоб усі ці елементи взаємодіяли між собою, створюючи динамічну і ефективну систему захисту критичної інфраструктури, яка здатна протистояти сучасним викликам.

Отже, для досягнення належного рівня захисту критичної інфраструктури необхідно впроваджувати інтеграційні механізми, що поєднують усі зазначені підходи та принципи. Це дозволить забезпечити стійкість і безпеку інфраструктури, що, в свою чергу, позитивно вплине на загальну стабільність держави і суспільства.

ГЛАВА 2. Міжнародні стандарти та практики захисту критичної інфраструктури

2.1. Огляд міжнародних стандартів: вплив на захист критичної інфраструктури

Захист критичної інфраструктури є глобальним викликом, що вимагає злагоджених дій на міжнародному рівні. У світі, де загрози безпеці постійно еволюціонують, від міжнародних терористичних актів до кібератак, необхідність у чітких стандартах і практиках захисту стає більш

актуальною, ніж будь-коли. Міжнародні стандарти відіграють ключову роль у формуванні спільного підходу до захисту критично важливих об’єктів, адже вони визначають основні принципи, рекомендації та процедури, яких повинні дотримуватись держави, аби забезпечити належний рівень безпеки.

ISO 22301: Системи управління безперервністю бізнесу – це міжнародний стандарт, який визначає вимоги до створення та підтримки ефективної системи управління безперервністю бізнесу (BCMS - Business Continuity Management System). Цей стандарт є незамінним інструментом для організацій, які прагнуть забезпечити безперервність своїх операцій навіть за умов виникнення непередбачених ситуацій, таких як природні катаклізми, кібератаки або інші кризові події. Він є важливим елементом у контексті захисту критичної інфраструктури, оскільки забезпечує структурований підхід до управління ризиками та забезпечення стійкості організацій.

Стандарт передбачає систематичну ідентифікацію ризиків, що можуть вплинути на безперервність бізнес-процесів, і розробку стратегій для їх мінімізації. Цей аспект є критично важливим для захисту критичної інфраструктури, оскільки ризики можуть мати широкий спектр: від природних катастроф до техногенних аварій і кібератак. ISO 22301 визначає чіткі вимоги до документації процесів управління безперервністю, що дозволяє організаціям формувати політики, процедури та плани дій. Це створює основи для підготовки та навчання персоналу, а також забезпечує ясність у розподілі відповідальності. Стандарт включає рекомендації щодо впровадження системи управління, а також механізми моніторингу та оцінки ефективності. Це дозволяє організаціям постійно вдосконалювати свої процеси, реагуючи на зміни в зовнішньому середовищі та нові загрози.

ISO 22301 визначає етапи, пов’язані з плануванням відновлення після інцидентів, що є критично важливим для зменшення наслідків для організації. Це включає створення планів дій, які повинні бути випробувані

та оновлені регулярно. Стандарт може бути інтегрований з іншими системами управління, такими як ISO 9001 (управління якістю) або ISO 27001 (управління інформаційною безпекою), що дозволяє організаціям створити єдину систему управління, що відповідає всім їхнім потребам.

ISO 22301 є важливим стандартом для забезпечення безперервності критичної інфраструктури, оскільки він надає організаціям необхідні інструменти для систематичного управління ризиками та забезпечення стійкості до загроз. Впровадження цього стандарту дозволяє не лише зменшити ймовірність виникнення інцидентів, але й підвищити готовність до швидкого реагування та відновлення, що є критично важливим у випадках, коли інфраструктурні системи стикаються з серйозними викликами.

ISO 27001: Управління інформаційною безпекою - це міжнародний стандарт, що встановлює вимоги до системи управління інформаційною безпекою (ISMS - Information Security Management System) [24]. Він спрямований на допомогу організаціям у забезпеченні конфіденційності, цілісності та доступності інформації шляхом систематичного управління ризиками, пов’язаними з інформаційною безпекою.

ISO 27001 передбачає створення, впровадження, підтримку та постійне вдосконалення системи управління інформаційною безпекою. Стандарт містить чіткі вимоги до політик, процедур, документів, ролей та відповідальності, що забезпечують належний рівень захисту інформації. Один з ключових аспектів стандарту — це проведення оцінки ризиків, яка включає ідентифікацію, аналіз і оцінку ризиків для інформаційних активів. Це дозволяє організаціям зрозуміти, які загрози можуть вплинути на їхні інформаційні системи, і вжити відповідних заходів для їх усунення або зменшення.

ISO 27001 містить перелік контрольних заходів, які організації можуть впровадити для захисту інформаційних активів. Ці заходи

охоплюють різні аспекти, такі як фізична безпека, управління доступом, управління інцидентами, навчання персоналу та багато інших. Стандарт можна інтегрувати з іншими системами управління, такими як ISO 9001 (система управління якістю) або ISO 22301 (системи управління безперервністю бізнесу), що дозволяє організаціям створювати комплексні системи управління. Організації можуть пройти аудит і отримати сертифікацію ISO 27001, що підтверджує їх відповідність стандарту та є важливим фактором для підвищення довіри партнерів.

Отже, ISO 27001 є критично важливим стандартом для забезпечення інформаційної безпеки в контексті захисту критичної інфраструктури. У сучасному цифровому світі, де кібератаки та витоки даних стають все більш розповсюдженими, цей стандарт допомагає організаціям захистити свої інформаційні системи і дані, що, в свою чергу, сприяє загальному захисту критично важливих об’єктів [25].

ISO 9001: Система управління якістю - це міжнародний стандарт, що визначає вимоги до системи управління якістю в організаціях (QMS - Quality management systems) та є одним з найбільш відомих і використовуваних стандартів у всьому світі. Стандарт підкреслює важливість управління процесами та їх взаємозв’язками. Це дозволяє організаціям оптимізувати свої діяльності, підвищуючи ефективність і результативність.

ISO 9001 включає в себе елементи ризик-орієнтованого підходу, що дозволяє організаціям ідентифікувати потенційні ризики та можливості, які можуть вплинути на якість продукції та послуг. Це передбачає регулярний аналіз та вдосконалення процесів. Стандарт акцентує увагу на залученні всіх співробітників у процес управління якістю, що підвищує обізнаність про значення якості на всіх рівнях організації та сприяє розвитку корпоративної культури, орієнтованої на якість.

ISO 9001 містить політики, процедури, інструкції та записи, які

допомагають контролювати та аналізувати процеси. Стандарт включає механізми внутрішнього аудиту, які дозволяють організаціям оцінювати відповідність своїх процесів вимогам стандарту та виявляти можливості для покращення. Це допомагає забезпечити постійне вдосконалення системи управління якістю. Хоча він створений для широкого кола організацій, його застосування для об’єктів критичної інфраструктури особливо актуальне з кількох причин.

По-перше, об’єкти критичної інфраструктури забезпечують життєво важливі послуги для суспільства, і будь-які перебої в їхній роботі можуть мати серйозні наслідки. Стандарт ISO 9001 допомагає встановити та підтримувати процеси, які мінімізують ризики таких перебоїв.

По-друге, об’єкти критичної інфраструктури часто працюють у високих ризикових умовах, тому важливо забезпечити постійний контроль якості, що підвищує надійність систем і процесів. Також, з огляду на постійні зміни у зовнішньому середовищі, ISO 9001 сприяє розробці гнучких і адаптивних систем управління, що дозволяє організаціям ефективно реагувати на нові виклики.

Крім того, низка країн мають законодавчі вимоги до організацій, що забезпечують функціонування критичної інфраструктури. У цьому контексті ISO 9001 може стати інструментом для доведення відповідності цим вимогам. Хоча стандарт не є спеціалізованим у сфері кібербезпеки, він закладає основи для впровадження заходів з захисту від кібератак, оскільки вимагає систематичного аналізу ризиків і розробки планів реагування на інциденти.

Конкретні переваги впровадження ISO 9001 для об’єктів критичної інфраструктури включають збільшення надійності завдяки ідентифікації та усуненню потенційних слабких місць, поліпшення координації через чітке визначення ролей і відповідальності, а також зменшення ризиків через систематичний аналіз загроз. Крім того, стандарт сприяє покращенню

комунікації між усіма учасниками процесу, що підвищує загальну ефективність роботи.

Впровадження ISO 9001 також підвищує довіру громадськості, адже сертифікат свідчить про те, що організація докладає всіх зусиль для забезпечення безпеки та надійності своїх послуг. У результаті, ISO 9001 є універсальним інструментом, що може бути ефективно застосований для управління якістю в будь-якій організації, включаючи об’єкти критичної інфраструктури. Він допомагає підвищити рівень безпеки, надійності та ефективності роботи таких об’єктів, що є критично важливим для суспільства. Отже, ISO 9001 є важливим інструментом для управління якістю в організаціях, що забезпечують критичну інфраструктуру. Його вимоги допомагають створити ефективну систему управління, що забезпечує постійне вдосконалення, залучення персоналу та адаптацію до нових викликів [26].

Таким чином, сучасні міжнародні стандарти, такі як ISO 22301, ISO 27001 та ISO 9001, демонструють важливі тенденції в захисті критичної інфраструктури: необхідність глобального підходу до безпеки, впровадження ризик-орієнтованого управління, інтеграцію стандартів управління, підвищення стійкості та адаптивності систем, а також залучення всіх учасників процесу. Ці особливості підкреслюють важливість міжнародних стандартів у формуванні ефективних практик захисту критичної інфраструктури, що є критично важливим для забезпечення безпеки і стійкості сучасних суспільств.

Важливо також звернути увагу на ініціативи та рекомендації від міжнародних інституцій. До прикладу, Організація Об’єднаних Націй, НАТО, Європейський Союз та Асоціація країн Південно-Східної Азії (ASEAN), відіграють важливу роль у формуванні політик та практик, що сприяють підвищенню безпеки критичної інфраструктури. Ці організації надають цінні рекомендації щодо забезпечення стійкості та безпеки

критично важливих об’єктів у світлі нових загроз і викликів. Вони пропонують методи, засновані на кращому досвіді, обміні інформацією та співпраці між країнами, що допомагає знизити ризики і покращити реакцію на можливі інциденти. Таким чином, розгляд рекомендацій від цих міжнародних організацій є невід’ємною частиною комплексного підходу до забезпечення безпеки критичної інфраструктури, що доповнює стандарти управління.

Організація Об’єднаних Націй (ООН) відіграє провідну роль у формуванні міжнародної політики щодо безпеки критичної інфраструктури. Завдяки своїм численним агентствам та програмам, ООН розробляє рекомендації, стандарти та ініціативи, спрямовані на підвищення стійкості та захищеності життєво важливих об’єктів.

Ключовими напрямами діяльності ООН у сфері безпеки критичної інфраструктури є:

Інтегрований підхід до управління ризиками. ООН закликає до комплексного підходу до управління ризиками, що враховує взаємозв’язки між різними секторами критичної інфраструктури. Цей підхід відображено в таких документах, як Глобальна оцінка ризиків (Global Risk Assessment), що регулярно оновлюється Програмою розвитку ООН (UNDP) [27].

Міжнародне співробітництво. ООН сприяє міжнародному співробітництву в галузі безпеки критичної інфраструктури. Важливу роль відіграють такі платформи, як Резолюція Ради Безпеки ООН 1373 (щодо боротьби з тероризмом), яка передбачає співпрацю між державами в обміні розвідувальною інформацією та боротьбі з фінансуванням тероризму [28].

Розробка стандартів. ООН, через такі спеціалізовані агентства, як Міжнародна організація цивільної авіації (ICAO) та Міжнародне агентство з атомної енергії (МАГАТЕ), розробляє міжнародні стандарти безпеки для різних секторів критичної інфраструктури, зокрема, Міжнародна організація цивільної авіації розробляє міжнародні стандарти безпеки цивільної авіації,

які є основою для забезпечення безпеки аеропортів та повітряного транспорту; Міжнародне агентство з атомної енергії розробляє міжнародні стандарти безпеки ядерних установок та матеріалів. Ці стандарти забезпечують основу для національних регулятивних рамок [29; 30].

Підвищення обізнаності. ООН проводить різноманітні заходи з підвищення обізнаності про важливість безпеки критичної інфраструктури. Програма розвитку ООН (UNDP) та інші агентства ООН організовують тренінги, семінари та конференції для державних службовців, представників приватного сектору та громадськості [31].

Адаптація до нових викликів. ООН відстежує нові загрози, такі як кібератаки та зміни клімату, і розробляє рекомендації щодо адаптації систем безпеки критичної інфраструктури. Ця робота відображена в численних доповідях та дослідженнях, що публікуються різними агентствами ООН, що відіграє важливу роль у координації зусиль міжнародного співтовариства щодо забезпечення безпеки критичної інфраструктури. Завдяки своїм численним ініціативам та документам, ООН сприяє підвищенню стійкості та захищеності життєво важливих об’єктів, що є ключовим фактором для забезпечення сталого розвитку та добробуту населення [32].

НАТО відіграє ключову роль у забезпеченні безпеки критичної інфраструктури держав-членів. Згідно зі Стратегічною концепцією НАТО 2022 року [], Альянс розглядає захист критичної інфраструктури як невід’ємну частину колективної оборони. Документ має важливе значення в контексті захисту критичної інфраструктури, оскільки підкреслює роль Альянсу в забезпеченні стійкості держав-членів та їхньої здатності реагувати на сучасні загрози.

У світлі російської воєнної агресії проти України, стратегія НАТО акцентує увагу на важливості посилення оборонних можливостей і зміцнення ключових систем, таких як енергетика, транспорт, зв’язок та інформаційні мережі. Одним з основних напрямів діяльності НАТО є

колективна оборона, що забезпечується через стримування і захист критичних об’єктів інфраструктури, важливих для національної безпеки. Оскільки кіберзагрози та гібридні атаки стають все більш розповсюдженими, НАТО прагне посилити свою кібербезпеку і розробляє ефективні механізми для захисту інфраструктур від атак, що можуть паралізувати ключові системи держав-членів.

Крім того, концепція передбачає підвищення стійкості інфраструктури до різноманітних загроз, включаючи природні катастрофи та техногенні аварії, через системи раннього попередження та координацію зусиль між державними та приватними структурами. З огляду на стратегічну важливість енергетичних, транспортних і комунікаційних мереж, НАТО підтримує країни-члени в їхніх зусиллях з модернізації та посилення стійкості цих систем.

Важливою частиною Стратегічної концепції НАТО 2022 є взаємодія між цивільними та військовими структурами, що дозволяє забезпечити інтегровану оборону критичної інфраструктури, яка включає не лише фізичний захист, а й кібернетичну та інформаційну безпеку. НАТО також акцентує увагу на співпраці з міжнародними організаціями (ЄС, ООН) з питань забезпечення безпеки критичної інфраструктури, що допомагає розширювати спектр методів і ресурсів для протидії сучасним загрозам [33].

Отже, Стратегічна концепція НАТО 2022 року чітко окреслює ключову роль захисту критичної інфраструктури у забезпеченні стабільності та безпеки держав-членів, адаптуючи підходи до змін у світовій безпековій ситуації та технологічному розвитку.

Міжнародні стандарти постійно еволюціонують у відповідь на технологічні зміни та виникнення нових загроз, особливо в контексті захисту критичної інфраструктури. Зазначене дозволяє окреслити основні тенденції та зміни, що впливають на ці стандарти.

1. Розвиток кібербезпеки. Зі зростанням цифровізації та поширенням

інтернету речей (IoT), нові кіберзагрози стають головною проблемою. Міжнародні стандарти, такі як ISO 27001 (Управління інформаційною безпекою) та ISO 22301 (Управління безперервністю бізнесу), активно розширюються для того, щоб охопити нові вимоги до кібербезпеки. Стандарти тепер включають рекомендації щодо захисту хмарних технологій, великих даних та штучного інтелекту.

2. Інтеграція кліматичних ризиків. Внаслідок зростання частоти та масштабу природних катастроф, стандарти почали включати вимоги до стійкості критичної інфраструктури до кліматичних ризиків. Наприклад, ISO 14090 (Адаптація до змін клімату) [34] визначає підходи до управління кліматичними ризиками, які можуть вплинути на інфраструктурні об’єкти.

3. Інтеграція штучного інтелекту (AI). Штучний інтелект почав грати значну роль в аналізі даних, прогнозуванні загроз і реагуванні на інциденти. Нові стандарти включають рекомендації щодо впровадження AI для моніторингу інфраструктури в режимі реального часу, як у стандартах кібербезпеки та управління ризиками.

4. Підвищення уваги до приватного сектору. Оскільки значна частина критичної інфраструктури перебуває в приватній власності, нові міжнародні стандарти роблять акцент на державно-приватному партнерстві. Це включає нові вимоги до обміну інформацією між державними структурами та приватними компаніями, як це передбачено у стандарті NIST Cybersecurity Framework (США) [35].

5. Гібридні загрози. У відповідь на зростання гібридних загроз, які поєднують фізичні атаки з кібернетичними, стандарти розширюють свої вимоги для забезпечення безпеки від багатофункціональних атак. Наприклад, ENISA (Агентство ЄС з кібербезпеки) випустила нові рекомендації для захисту критичної інфраструктури, що передбачають одночасний захист фізичних і цифрових систем.

6. Зростаюча роль стійкості. Стійкість (resilience) стає важливим

концептом у стандартах. Міжнародні стандарти, такі як ISO 22316 (Управління організаційною стійкістю) [37], розвиваються, щоб зосередитися не лише на запобіганні ризикам, але й на здатності організацій швидко відновлюватися після інцидентів.

Ці тенденції відображають зміну парадигм у сфері захисту критичної інфраструктури, де акцент робиться на превентивних і проактивних заходах, а також на системній інтеграції сучасних технологій для підвищення стійкості. Замість реагування на кризи після їх виникнення, нові стандарти орієнтовані на запобігання загрозам через моніторинг, раннє попередження та постійну адаптацію до змін. Це підхід, де безперервність функціонування є ключовим фактором, а інтеграція систем управління ризиками і кібербезпеки в реальному часі дозволяє запобігати загрозам ще на етапі їхнього формування.

Інші важливі аспекти включають:

– кооперацію між державним і приватним секторами для підвищення рівня безпеки в різних сферах критичної інфраструктури, включаючи енергетику, транспорт, фінанси та охорону здоров’я;

– глобальну інтеграцію стандартів і рекомендацій, що забезпечують спільний підхід до захисту критичної інфраструктури через міжнародну співпрацю та обмін інформацією та об’єднання зусиль таких організацій, як Європейський Союз, НАТО та ООН;

– адаптивність і гнучкість у прийнятті рішень, які враховують стрімкі мінливі умови зовнішнього середовища, включаючи нові загрози, як-то зміна клімату або нові форми гібридних атак.

У цій новій парадигмі велике значення приділяється підготовці кадрів і постійному вдосконаленню систем моніторингу й управління, що дозволяє не тільки реагувати на загрози, але й активно їх передбачати та знижувати ризики.

2.2. Особливості стандартів захисту у різних країнах

У США захист критичної інфраструктури регулюється низкою федеральних і державних законів. Основним документом є Закон про захист критичної інфраструктури 2001 року [38], який визначає ключові сектора, такі як енергетика, транспорт, зв'язок, фінанси та охорона здоров'я. Крім того, існують специфічні закони, які регулюють питання кібербезпеки, наприклад, Закон про кібербезпеку 2015 року. Стандарти, такі як NIST [35] (Національний інститут стандартів і технологій), розробляють рекомендації та методики для захисту критичної інфраструктури, включаючи NIST Cybersecurity Framework. Ці стандарти забезпечують основи для управління ризиками, захисту інформаційних систем та інтеграції технологій.

У США існує багаторівнева система управління, де федеральні, державні та місцеві органи влади співпрацюють для забезпечення безпеки критичної інфраструктури. Наприклад, Департамент внутрішньої безпеки (DHS) координує дії між різними секторами. Держава виділяє кошти на програми безпеки через різні програми фінансування, такі як Homeland Security Grant Program [39]. Це дозволяє державам та місцевим громадам реалізовувати заходи з покращення безпеки інфраструктури.

У США існує розвинена співпраця між державними органами та приватними підприємствами, оскільки значна частина критичної інфраструктури перебуває в приватному секторі. Спільні ініціативи, такі як Public-Private Partnerships (PPP), забезпечують обмін інформацією та ресурсами. Відповідно до стандартів NIST, організації зобов'язані проводити систематичну оцінку ризиків, що дозволяє ідентифікувати вразливості та загрози. Це є важливим етапом у формуванні стратегій захисту.

США активно впроваджують новітні технології для покращення захисту критичної інфраструктури. Використання штучного інтелекту, великих даних та технологій моніторингу стало стандартом у багатьох

секторах. Організації зобов’язані проводити регулярні навчання та тренінги для своїх співробітників. DHS та інші агенції пропонують програми підвищення кваліфікації, щоб підготувати кадри до реагування на надзвичайні ситуації. США активно співпрацюють з міжнародними організаціями, такими як НАТО та ООН, в питаннях безпеки критичної інфраструктури. Це включає обмін інформацією, спільні тренінги та участь у міжнародних ініціативах для підвищення безпеки.

Таким чином, Сполучені Штати Америки мають добре розвинену систему стандартів та рекомендацій щодо захисту критичної інфраструктури, що враховує особливості національної безпеки, технологічні інновації та співпрацю між державним і приватним секторами.

Німеччина має чітку правову основу для захисту критичної інфраструктури, яка охоплює законодавчі акти на федеральному, земельному та місцевому рівнях. Основним документом є Закон про безпеку критичної інфраструктури (Gesetz über die Sicherheit der kritischen Infrastrukturen), що визначає основи для захисту об’єктів критичної інфраструктури, включаючи енергетику, транспорт і інформаційні системи [40].

Німеччина впроваджує міжнародні стандарти, такі як ISO 22301 і ISO 27001, для управління безперервністю бізнесу та інформаційною безпекою [24; 25]. Крім того, NIS-Direktive (Директива про мережеву та інформаційну безпеку) регулює заходи з кібербезпеки для критичної інфраструктури. Захист критичної інфраструктури в Німеччині організовано через федеральні міністерства [41], такі як Міністерство внутрішніх справ (BMI) і Міністерство економіки та енергетики (BMWi). Ці органи координують зусилля з безпеки між різними секторами та на всіх рівнях.

Держава виділяє ресурси для фінансування проектів, пов’язаних із захистом критичної інфраструктури, включаючи інвестиції в технології безпеки та модернізацію існуючих систем. Фінансування також

здійснюється через програми національної безпеки. У Німеччині активно розвивається співпраця між державними органами та приватними підприємствами. Наприклад, програма «Партнерство безпеки» (Sicherheitspartnerschaft) заохочує обмін інформацією та спільну діяльність у сфері безпеки [42].

Німецькі організації зобов'язані проводити регулярну оцінку ризиків, що є важливим елементом у формуванні стратегій захисту критичної інфраструктури. Вони використовують стандартні методології, такі як IT-Grundschutz [43], для аналізу вразливостей. Німеччина активно впроваджує нові технології для захисту критичної інфраструктури, зокрема в сферах кібербезпеки та моніторингу. Технології, такі як штучний інтелект та великі дані, використовуються для прогнозування загроз і управління інцидентами.

Організації в Німеччині зобов'язані проводити навчання та підготовку персоналу з питань безпеки. Наприклад, ініціативи щодо навчання у сфері кібербезпеки сприяють підвищенню кваліфікації кадрів у приватному та державному секторах.

Німеччина активно співпрацює з міжнародними організаціями, такими як ЄС, НАТО та ООН, для обміну інформацією та кращими практиками в сфері безпеки критичної інфраструктури. Це співробітництво допомагає покращити реакцію на нові загрози та забезпечити загальну безпеку в регіоні. Таким чином, Німеччина має розвинену систему стандартів і рекомендацій щодо захисту критичної інфраструктури, що враховує національні потреби, міжнародні вимоги та технологічні інновації.

Особливості стандартів захисту критичної інфраструктури у Великобританії можна охарактеризувати через кілька ключових аспектів, включаючи національні закони, міжнародні стандарти та механізми управління ризиками. В основі британської системи лежить ефективне правове регулювання діяльності суб'єктів державного управління та приватного сектору, що працюють у тісній координації.

Одним з ключових елементів захисту критичної інфраструктури у Великобританії є National Infrastructure Protection Plan. Ця програма визначає важливі сектори інфраструктури та розробляє стратегії для забезпечення їх безпеки. Серед основних секторів критичної інфраструктури в країні – енергетика, транспорт, водопостачання, інформаційно-комунікаційні технології та фінансові послуги. Ще один важливий документ – The Civil Contingencies Act 2004, який визначає законодавчі рамки для забезпечення національної безпеки та реагування на надзвичайні ситуації [44]. Цей закон вимагає від державних органів та операторів критичної інфраструктури проводити регулярні оцінки ризиків, а також розробляти плани для зниження їх впливу.

Великобританія використовує підхід risk-based approach для захисту критичної інфраструктури. Це означає, що організації зобов'язані ідентифікувати загрози та оцінювати ризики на основі їхньої вразливості. Основним інструментом тут є UK National Risk Register, який допомагає ідентифікувати ключові ризики для критичної інфраструктури, включаючи природні катастрофи, терористичні атаки та кіберзагрози.

Кіберзахист є одним із пріоритетів британської стратегії. National Cyber Security Strategy (NCSS), що розробляється за підтримки National Cyber Security Centre (NCSC), фокусується на протидії кіберзагрозам для критичних об'єктів інфраструктури [45]. У рамках цієї стратегії Великобританія впроваджує заходи з управління ризиками для цифрових систем та проводить постійний моніторинг інформаційних систем критичної інфраструктури.

Організації, що працюють у критичних секторах Великобританії, використовують міжнародні стандарти, такі як ISO 22301 (управління безперервністю бізнесу) і ISO 27001 (інформаційна безпека) [24; 25]. Окрім того, британські компанії також можуть керуватися стандартами NIST Cybersecurity Framework, розробленими у США, для посилення

кіберзахисту.

У Великобританії критична інфраструктура переважно належить приватним компаніям, тому співпраця між державними органами і бізнесом є ключовим компонентом захисту. Public-Private Partnership (PPP) у цій сфері включає обмін інформацією про загрози, а також спільне проведення навчань і тестувань для підвищення стійкості інфраструктури. Ефективність впроваджених заходів контролюється через регулярні аудити та симуляції надзвичайних ситуацій. Важливим аспектом є KPI для моніторингу ефективності, а також оцінка результатів симуляцій для покращення готовності до кризових ситуацій. Великобританія також активно використовує міжнародні оцінки та рейтинги, щоб зіставити свої стандарти із глобальними практиками.

Великобританія активно співпрацює з іншими державами та організаціями, як-от ЄС і НАТО, з метою забезпечення спільної стратегії у сфері безпеки критичної інфраструктури. Це включає обмін передовим досвідом, спільні навчання та розробку нових підходів до захисту від гібридних загроз.

З урахуванням зростання загроз, пов’язаних із змінами клімату, Великобританія активно інтегрує кліматичні ризики до своєї стратегії захисту інфраструктури. Нові програми адаптації спрямовані на підвищення стійкості інфраструктурних об’єктів до природних катастроф, таких як повені, посухи або шторми.

Великобританія робить значні інвестиції у кібербезпеку та модернізацію критичної інфраструктури. Ці інвестиції спрямовані на розширення можливостей захисту та впровадження нових технологій для мінімізації ризиків.

Отже, стандарти захисту критичної інфраструктури у Великобританії вирізняються чіткою організаційною структурою, інтеграцією міжнародних стандартів, акцентом на кібербезпеці та ефективним державно-приватним

партнерством. Механізми оцінки ефективності, такі як регулярні аудити та тестування, забезпечують високу ступінь готовності до нових загроз і кризових ситуацій.

Європейський Союз (ЄС) активно працює над забезпеченням безпеки критичної інфраструктури через розробку законодавчих ініціатив, стратегій і співпрацю між державами-членами [46]. Основні рекомендації ЄС щодо захисту критичної інфраструктури включають декілька ключових напрямів.

Європейська програма захисту критичної інфраструктури (EPCIP). EPCIP є основною програмою ЄС, спрямованою на захист критичних об'єктів і систем [47]. Вона включає заходи для ідентифікації та оцінки критичної інфраструктури, аналіз загроз та вразливостей, а також розробку заходів з їхньої охорони. В рамках EPCIP [48] передбачається створення національних програм з визначення критичних об'єктів у кожній державі-члені та встановлення відповідних протоколів реагування.

Директива про захист критичних інфраструктур (ECI Directive) спрямована на зміцнення стійкості важливих об'єктів до загроз, зокрема тероризму та природних катастроф [49]. Директива зобов'язує держави-члени ЄС:

– визначати національні критичні інфраструктури та захищати їх;

– розробляти національні плани дій для запобігання ризикам, а також системи раннього попередження про потенційні загрози;

– забезпечувати належний обмін інформацією між державами-членами та організаціями, що відповідають за критичну інфраструктуру.

Нова Директива NIS2 (2020). У 2020 році ЄС представив оновлену версію Директиви NIS2, яка спрямована на покращення кібербезпеки критичних інфраструктур. NIS2 зосереджується на підвищенні стійкості та кіберзахисту ключових секторів, таких як енергетика, транспорт, охорона здоров'я та фінанси [50]. Директива запроваджує нові вимоги для кібербезпеки та зміцнює співпрацю між державами-членами у сфері

кіберзахисту, зокрема через створення мережі кіберінцидентів.

Спільна європейська програма кіберзахисту (EU Cybersecurity Act). Ініціатива націлена на підвищення стійкості до кіберзагроз через введення сертифікації кібербезпеки для критичних об'єктів інфраструктури [51]. Цей механізм дозволяє гарантувати, що всі важливі об'єкти, включаючи цифрові системи, відповідають високим стандартам захисту від кіберзагроз.

Інтеграція кліматичних ризиків у захист інфраструктури передбачає, що ЄС визнає, що зміни клімату можуть створювати нові ризики для критичної інфраструктури. Тому він рекомендує державам-членам інтегрувати кліматичні ризики у стратегії захисту інфраструктури, щоб підвищити їх стійкість до природних катастроф, таких як повені, урагани та екстремальні погодні умови. ЄС надає значне фінансування через програми, такі як Horizon Europe [52], для інноваційних рішень у сфері захисту критичної інфраструктури та розробки новітніх технологій для моніторингу, управління ризиками та адаптації до нових викликів у сфері безпеки.

ЄС закликає до активної співпраці між державними органами та приватним сектором для забезпечення ефективного захисту інфраструктури. Це передбачає обмін даними про загрози, розробку спільних протоколів безпеки та проведення спільних навчань для реагування на кризи. Європейський Союз підкреслює важливість комплексного підходу до захисту критичної інфраструктури, що включає фізичну безпеку, кібербезпеку та стійкість до кліматичних ризиків. ЄС постійно оновлює свої стратегії та нормативні акти для адаптації до нових загроз, наголошуючи на важливості міжнародної співпраці, інновацій та інтеграції різних секторів економіки.

Що стосується оцінки ефективності стандартів захисту критичної інфраструктури, вона залежить від механізмів моніторингу, аналізу й адаптації, що використовуються країнами для контролю і вдосконалення впроваджених заходів. У вищерозглянутих країнах механізми оцінки

ефективності стандартів захисту мають схожі характеристики, хоча і відрізняються залежно від національних особливостей.

У США ефективність стандартів захисту критичної інфраструктури оцінюється через Національний інститут стандартів і технологій (NIST), що розробляє методики оцінки ризиків та кібербезпеки. Інтеграція стандартів NIST Cybersecurity Framework [36] допомагає організаціям аналізувати рівень захисту критичних об’єктів. Федеральні та державні органи влади співпрацюють у рамках Програми захисту критичної інфраструктури та фінансують проекти через програми, як-от Homeland Security Grant Program [39]. Регулярні аудити, тести на проникнення, симуляції кризових ситуацій та звіти про оцінку ризиків дозволяють перевіряти ефективність впроваджених заходів.

У Німеччині оцінка ефективності проводиться через федеральні органи, такі як Міністерство внутрішніх справ та Федеральне управління інформаційної безпеки, яке застосовує стандарти, як-от IT-Grundschutz для аналізу вразливостей [43]. NIS-Direktive регулює кібербезпеку для критичної інфраструктури, забезпечуючи обов’язкову звітність і регулярні перевірки для підприємств. Німецька система передбачає використання ключових показників ефективності (KPI) для вимірювання безпеки критичних систем і оцінки успіху впровадження стандартів.

У Великобританії механізми оцінки ефективності впровадження стандартів включають National Cyber Security Strategy (NCSS) та National Cyber Security Centre (NCSC) [45], які проводять регулярні аудити та оцінку кіберризиків для критичних об’єктів. Public-Private Partnerships (PPP) дозволяють уряду й приватному сектору координувати дії та забезпечувати належний рівень захисту через спільні тренінги та навчання. Також використовується UK National Risk Register, що допомагає визначати ефективність захисту від кіберзагроз та інших ризиків.

Усі країни використовують схожі механізми оцінки ефективності, які

включають:

– регулярні аудити для перевірки відповідності стандартам і рекомендаціям;

– тестування на проникнення для оцінки кібербезпеки;

– ключові показники ефективності (KPI), які вимірюють рівень захисту інфраструктури;

– звітування про інциденти та аналіз кризових ситуацій для вдосконалення стратегій безпеки;

– симуляції кризових ситуацій для перевірки готовності систем і співробітників до надзвичайних ситуацій.

Країни оцінюють успіх впровадження стратегій захисту через відповідність міжнародним стандартам, таким як ISO 22301 (управління безперервністю бізнесу), ISO 27001 (управління інформаційною безпекою) [24; 25] та інших. Міжнародне співробітництво з організаціями, такими як НАТО та ООН, дозволяє країнам аналізувати свої стратегії, отримуючи зворотний зв’язок та беручи участь у міжнародних рейтингах і оцінках.

Таким чином, оцінка ефективності впровадження стандартів захисту критичної інфраструктури базується на моніторингу, аудиту, тестуванні, співпраці між державою і бізнесом, а також на інтеграції міжнародних стандартів у національні системи.

Країни, такі як США, Великобританія, Німеччина та інші держави ЄС, стикаються з низкою викликів при адаптації міжнародних стандартів захисту критичної інфраструктури до своїх умов. Основні з них можна класифікувати за політичними, економічними, технологічними та культурними факторами. Розглянемо їх детальніше.

Суверенітет та національні інтереси. Кожна держава прагне зберегти свій контроль над критично важливими секторами, особливо якщо йдеться про питання національної безпеки. Наприклад, США та Великобританія можуть бути обережні щодо впровадження стандартів,

розроблених іншими країнами або міжнародними організаціями, через побоювання втрати контролю над власними процесами захисту. Це може ускладнити адаптацію таких стандартів, як ISO 27001 або NIST.

Різні підходи до регулювання. У ЄС країни-учасники часто стикаються з труднощами узгодження національного законодавства з європейськими директивами, такими як Директива NIS2, яка вимагає покращення кібербезпеки критичних інфраструктур. Різні політичні системи та адміністративні структури можуть утруднювати єдину та швидку адаптацію міжнародних стандартів.

Висока вартість впровадження. Впровадження міжнародних стандартів, таких як ISO 22301 для управління безперервністю бізнесу або ISO 9001 для управління якістю, вимагає значних фінансових ресурсів. Це особливо актуально для країн із менш розвиненою економікою, а також для малого та середнього бізнесу, який не завжди має доступ до таких ресурсів. У той час як великі компанії можуть дозволити собі ці витрати, менші організації часто стикаються з труднощами при інтеграції дорогих технологічних рішень.

Економічна нерівність між регіонами. Наприклад, у країнах ЄС існують значні економічні відмінності між державами-членами, що створює дисбаланс у рівні захисту критичної інфраструктури. Багатші країни, як-от Німеччина або Франція, мають більше ресурсів для адаптації міжнародних стандартів, ніж країни з менш розвиненими економіками.

Різний рівень технологічної підготовки. Інтеграція новітніх технологій, таких як штучний інтелект, великі дані або технології моніторингу, вимагає від країн високого рівня технологічного розвитку. Наприклад, США активно використовують нові технології для моніторингу критичної інфраструктури, тоді як інші країни можуть відставати через брак технологічної бази або фахівців.

Інтеграція кібербезпеки. У Великобританії та інших європейських

країнах одним із найбільших викликів є захист критичних інформаційних систем від кіберзагроз. Потреба в постійному оновленні інфраструктури для захисту від нових кіберзагроз створює значний тиск на країни, де кібербезпека не була достатньо розвинутою раніше.

Різні управлінські культури. Країни мають різні підходи до управління та організації процесів захисту критичної інфраструктури. У США, наприклад, існує тісна взаємодія між приватним і державним секторами, тоді як у деяких європейських країнах держава грає більш домінуючу роль. Така різниця в управлінській культурі може ускладнити адаптацію міжнародних стандартів.

Освітні бар'єри. У деяких країнах нестача спеціалізованих кадрів і експертів може стати серйозним бар'єром для впровадження міжнародних стандартів, таких як ISO 27001 або NIST Cybersecurity Framework. Ці стандарти вимагають висококваліфікованого персоналу для їх ефективної реалізації, а не всі країни мають доступ до такої кількості експертів.

Таким чином, адаптація міжнародних стандартів захисту критичної інфраструктури стикається з комплексом викликів, які залежать від національних особливостей, економічних можливостей, рівня технологічного розвитку та політичних пріоритетів кожної країни.

2.3. Взаємодія міжнародних організацій у сфері захисту критичної інфраструктури

Міжнародні зусилля у сфері кібербезпеки можна відстежити з кінця XX-го століття, коли розвиток цифрових технологій та Інтернету почав суттєво змінювати характер загроз для держав, бізнесу та суспільства в цілому. Ключові етапи цього процесу включають такі періоди.

У 1990-х роках кібербезпека почала поступово ставати однією з важливих сфер міжнародного співробітництва. Держави почали розуміти

необхідність координації зусиль для захисту від нових цифрових загроз, які не обмежуються кордонами. Саме у цей період з'явилися перші концепції захисту інформаційних систем, що підштовхнуло розвиток національних і міжнародних політик кібербезпеки.

Одним із найважливіших етапів в історії міжнародних зусиль у сфері кібербезпеки стало підписання Будапештської конвенції про кіберзлочинність у 2001 році. Ця конвенція, розроблена Радою Європи, стала першою міжнародною угодою, яка націлена на гармонізацію законодавства різних країн у боротьбі з кіберзлочинністю. Будапештська конвенція стала основним документом у міжнародному праві, що регулює кіберзлочинність, і заклала основи для подальшого розвитку правового регулювання в цій сфері, визначила правові інструменти для співпраці між країнами щодо злочинів, що скоюються в кіберпросторі, таких як хакерство, кібершпигунство та фінансові махінації.

Протягом періоду 2004-2010 років міжнародні організації, зокрема Організація Об'єднаних Націй (ООН) та Організація з безпеки і співробітництва в Європі (ОБСЄ), почали активно розробляти механізми для співпраці у сфері кібербезпеки. ООН створила Групу урядових експертів (GGE), яка фокусувалася на питаннях кібербезпеки та правових основах для врегулювання кіберінцидентів. ОБСЄ також розробила рекомендації для країн-учасниць щодо безпеки інформаційних систем.

У 2013 році Організація економічного співробітництва та розвитку (ОЕСР) представила оновлені рекомендації щодо кібербезпеки, акцентуючи увагу на необхідності інтеграції принципів кібербезпеки у національні та міжнародні стратегії. ОЕСР виділяє такі ключові елементи кібербезпеки, як захист критичної інфраструктури, співпраця між державами та приватним сектором і забезпечення захисту прав користувачів в Інтернеті. Рекомендації ОЕСР слугують основою для розробки національних стратегій кібербезпеки та забезпечують правову рамку для міжнародної співпраці у цій сфері [53].

Європейський Союз у 2016 році ухвалив Директиву NIS (Directive on security of network and information systems), що стало першим значним кроком у ЄС для впорядкування кібербезпеки на рівні держав-членів [55]. Ця директива спрямована на забезпечення стійкості цифрових і мережевих систем, що критично важливо для захисту критичної інфраструктури. Директива NIS стала першим правовим актом ЄС, який встановлює обов'язкові вимоги щодо кібербезпеки для держав-членів, що підвищує загальний рівень безпеки в Європі.

У світлі глобальних кібератак, таких як WannaCry (2017) та NotPetya (2017), міжнародна спільнота впродовж останніх десяти років стала приділяти особливу увагу кібербезпеці критичної інфраструктури. ООН, НАТО, ЄС та інші міжнародні організації значно активізували свої зусилля щодо підвищення стійкості критичних об'єктів до кібератак, розробляючи нові політики і стандарти для співпраці та взаємодії. Історичний огляд міжнародних зусиль у сфері кібербезпеки, включаючи ключові події та ініціативи показано у таблиці 3.

Вказані міжнародні документи та угоди свідчать про поступову еволюцію підходів до кібербезпеки та зростаючу важливість міжнародного співробітництва. Встановлення правових рамок, механізмів співпраці та обміну інформацією є ключовими аспектами для підвищення ефективності захисту критичної інфраструктури від кіберзагроз, оскільки ці документи формують основу для подальшого розвитку міжнародних зусиль у цій важливій сфері, сприяючи створенню більш безпечного кіберпростору.

Таким чином, історія міжнародних зусиль у сфері кібербезпеки демонструє поступову еволюцію від локальних ініціатив до глобальних, включаючи створення правових інструментів та механізмів координації для боротьби з кіберзагрозами та захисту критичної інфраструктури.

Таблиця 3

Основні етапи розвитку міжнародних зусиль у сфері кібербезпеки та їх еволюція у відповідь на зростаючі загрози у сфері захисту об'єктів критичної інфраструктури

Рік	**Подія/Ініціатива**	**Характреистика**
1990-ті	Перші ініціативи з кібербезпеки	Початок усвідомлення необхідності міжнародної координації для захисту від цифрових загроз. Розробка перших концепцій захисту інформаційних систем.
2001	Підписання Будапештської конвенції	Перша міжнародна угода для боротьби з кіберзлочинністю, розроблена Радою Європи, що забезпечила правові інструменти для співпраці між країнами щодо кіберзлочинів (хакерство, кібершпигунство, фінансові махінації).
2004-2010	Ініціативи ООН та ОБСЄ	Створення Групи урядових експертів (GGE) ООН для питань кібербезпеки. ОБСЄ розробила рекомендації для країн-учасниць щодо безпеки інформаційних систем.
2013	Прийняття Рамкової програми ОЕСР	Оновлені рекомендації щодо кібербезпеки, акцент на інтеграції кібербезпеки в національні та міжнародні стратегії. Визначення ключових елементів кібербезпеки: захист критичної інфраструктури, співпраця між державами та приватним сектором, захист прав користувачів в Інтернеті.
2016	Ухвалення Директиви NIS в ЄС	Перше значне регулювання кібербезпеки на рівні держав-членів ЄС. Спрямовано на забезпечення стійкості цифрових і мережевих систем, критично важливих для захисту критичної інфраструктури.
2017	Глобальні кібератаки WannaCry та NotPetya	Підвищення уваги міжнародної спільноти до кібербезпеки критичної інфраструктури у відповідь на великі кібератаки, що активізувало зусилля ООН, НАТО, ЄС щодо підвищення стійкості критичних об'єктів.
Останнє десятиліття	Акцент на кібербезпеку критичної інфраструктури	Розробка нових політик і стандартів для співпраці та взаємодії між міжнародними організаціями, підвищення стійкості до кібератак.

Джерело: складено автором за [47-54]

Міжнародне співробітництво у сфері захисту критичної інфраструктури є надзвичайно важливим завданням у сучасному глобалізованому світі, але воно стикається з численними проблемами та викликами, які ускладнюють ефективну взаємодію між міжнародними

організаціями, такими як ООН, ЄС, НАТО та інші.

По-перше, відсутність чіткої координації є однією з основних перешкод. Різні міжнародні організації можуть мати власні ініціативи та програми, що призводить до дублювання зусиль і фрагментації підходів до захисту критичної інфраструктури. Брак узгодженої глобальної стратегії або дорожньої карти може ускладнити ефективну координацію між цими організаціями, що часто призводить до затримок у реагуванні на загрози.

По-друге, правові бар'єри значно ускладнюють співпрацю. Країни мають різні правові системи та норми, що може заважати впровадженню спільних стандартів і механізмів захисту критичної інфраструктури. Відмінності у законодавстві можуть затримувати процес укладання міжнародних угод і створення спільних нормативних актів, ускладнюючи правове співробітництво.

Крім того, політичні інтереси та конфлікти також виступають серйозним викликом. Держави можуть мати протилежні політичні або економічні інтереси, що ускладнює їхню готовність до співпраці у питаннях захисту критичної інфраструктури. Геополітичні чинники, такі як напруженість між державами, можуть ще більше негативно впливати на цю готовність.

Технічні виклики також становлять значну проблему. Швидкість технологічних змін у кіберзагрозах може перевищувати темпи адаптації міжнародних організацій, що ускладнює реалізацію ефективних заходів. Складність інтеграції різних технологій та систем між країнами може призвести до вразливостей у захисті критичної інфраструктури.

Проблеми довіри та обміну інформацією є ще одним важливим аспектом. Країни можуть бути обережними в обміні даними про потенційні загрози або вразливості через ризик витоку інформації, що ускладнює оперативне реагування на інциденти. Постійні кібератаки можуть підірвати довіру між державами та міжнародними організаціями, що заважає активній

співпраці.

Фінансова нестабільність також суттєво обмежує можливості співробітництва. Багато країн не можуть виділити достатні ресурси для участі в міжнародних ініціативах, що впливає на їхню здатність до активного співробітництва. Високі витрати на модернізацію та захист критичної інфраструктури можуть стати серйозною перешкодою.

Останнім, але не менш важливим, є дефіцит кваліфікованих кадрів. Брак спеціалістів у сфері кібербезпеки в країнах може ускладнити їхню участь у міжнародних проектах. Необхідно підвищити рівень освіти і підготовки кадрів у сфері захисту критичної інфраструктури, щоб країни могли ефективно реагувати на нові виклики.

Відтак, проблеми та виклики міжнародного співробітництва у сфері захисту критичної інфраструктури потребують комплексного підходу до їх вирішення. Створення механізмів координації, розробка спільних стандартів, посилення довіри та обміну інформацією, а також підвищення фінансування і підготовки кадрів здатні суттєво покращити взаємодію міжнародних організацій у цій важливій сфері.

Перспективи розвитку міжнародного співробітництва в галузі кібербезпеки критичної інфраструктури стають дедалі актуальнішими у світлі зростаючих загроз у кіберпросторі. З огляду на складність і динамічність сучасних загроз, країни та міжнародні організації повинні активізувати свої зусилля для створення більш ефективних механізмів співпраці.

Важливим напрямком розвитку є інтеграція кібербезпеки в загальні стратегії національної та міжнародної безпеки. Низка держав визнають, що кібербезпека є невід’ємною частиною національної безпеки та забезпечують розробку відповідних політик, формують спільні стандарти і практики, що сприяє більшій координації зусиль між країнами.

Інтеграція кібербезпеки в загальні стратегії національної та

міжнародної безпеки є важливим кроком у забезпеченні захисту критичної інфраструктури. Кібербезпека стає невід'ємною частиною національних стратегій, що створює основу для більш структурованого підходу до формування політики. Водночас такий підхід підкреслює необхідність активної участі не лише держав, але й приватного сектора, оскільки більшість критичних інфраструктур, таких як енергетика, транспорт і зв'язок, перебувають в приватній власності або експлуатуються приватними компаніями.

Зміцнення партнерства між державним і приватним секторами стає природним продовженням інтеграції кібербезпеки в загальні стратегії. Враховуючи, що держави визнають важливість кібербезпеки як елемента національної безпеки, вони мають намір співпрацювати з приватними підприємствами для створення ефективних механізмів захисту. Приватні компанії, які відповідають за управління критичною інфраструктурою, володіють технологіями та експертизою, необхідними для виявлення та реагування на загрози в кіберпросторі.

Таким чином, активне залучення приватного сектора до розробки стратегій кібербезпеки не лише покращує рівень захисту, але й забезпечує більш комплексний підхід до оцінки ризиків. Успішна співпраця між державою і бізнесом дозволяє об'єднати ресурси, інформацію та технології, що, в свою чергу, підвищує загальну ефективність реагування на кіберзагрози. Це партнерство стає критично важливим для створення системи безпеки, що відповідає сучасним викликам, адже лише спільними зусиллями можна досягти значних результатів у захисті критичної інфраструктури від кіберзагроз.

Зміцнення партнерства між державним і приватним секторами в сфері кібербезпеки створює потужну основу для більшої ефективності захисту критичної інфраструктури. Однак, щоб досягти максимального результату, необхідно забезпечити належний обмін інформацією та тісну співпрацю не

лише на національному рівні, а й між міжнародними організаціями.

Розширення обміну інформацією та співпраці між міжнародними організаціями стає критично важливим компонентом у цьому процесі. Об’єднання зусиль держав на глобальному рівні дозволяє створити єдину інформаційну екосистему, яка забезпечує своєчасне реагування на кібератаки. Наприклад, організації, такі як ООН, НАТО та ЄС, можуть координувати дії, обмінюватися даними про нові загрози та вразливості, а також розробляти спільні політики для протидії кіберзлочинності.

Таке співробітництво дозволяє не лише оперативно реагувати на конкретні інциденти, а й підвищувати загальний рівень кіберстійкості на міжнародному рівні. Створення спільних платформ для обміну інформацією, таких як центри моніторингу загроз, сприяють аналізу нових методів атаки та розробці відповідних стратегій захисту. Таким чином, підвищений рівень взаємодії між міжнародними організаціями є ключовим елементом у формуванні ефективної глобальної системи кібербезпеки, яка дозволяє країнам більш швидко і злагоджено реагувати на виклики сучасного кіберпростору.

Ще одним важливим аспектом є розвиток спільних навчальних програм та тренінгів для фахівців у сфері захисту критичної інфраструктури. Освіта і підготовка кадрів стануть основою для забезпечення кваліфікованих кадрів, здатних ефективно реагувати на нові виклики. Міжнародні організації можуть ініціювати програми обміну досвідом, що дозволить фахівцям з різних країн отримувати знання про кращі практики та новітні технології.

Не менш важливим напрямом є формування правових рамок для міжнародного співробітництва в галузі. Розробка угод, що регулюють питання кіберзлочинності, а також створення механізмів для вирішення спорів можуть сприяти більшій стабільності та передбачуваності у взаєминах між країнами. Це, у свою чергу, підвищує довіру між державами

та стимулює їх до більш активного співробітництва в умовах кіберзагроз критичній інфраструктурі.

На завершення, перспективи розвитку міжнародного співробітництва з питань безпеки критичної інфраструктури залежать від здатності країн і міжнародних організацій до адаптації та інтеграції нових підходів. Системний підхід до вирішення проблем, активне залучення усіх зацікавлених сторін та розробка ефективних механізмів співпраці можуть суттєво підвищити рівень безпеки критичної інфраструктури в умовах зростаючих кіберзагроз. Саме правові рамки, в свою чергу, забезпечать платформу для співпраці, де країни можуть обмінюватися досвідом, ресурсами та інформацією та ефективно адаптуватися до нових викликів у кіберпросторі. Таким чином, інтеграція правових механізмів у систему міжнародного співробітництва є ключовою для забезпечення комплексного захисту критичної інфраструктури на глобальному рівні.

ГЛАВА 3. Інституційно-правові основи державної політики у сфері захисту критичної інфраструктури

3.1. Національне законодавство та регуляції

Захист критичної інфраструктури є ключовим елементом забезпечення національної безпеки та стійкості держави. Критична інфраструктура охоплює різноманітні сфери, такі як енергетика, транспорт, зв’язок, охорона здоров’я, вода та продовольство, які є необхідними для функціонування суспільства та економіки. Порушення в роботі цих систем може призвести до серйозних наслідків, включаючи економічні втрати, загрозу життю людей та загострення соціальної напруженості.

В Україні законодавство у цій сфері значно зміцнилося останніми роками через ухвалення низки нормативно-правових актів, зокрема Закону

України «Про критичну інфраструктуру» від 16.11.2021 №1882-IX [2]. Цей закон визначає правові та організаційні засади функціонування національної системи захисту критичної інфраструктури та є складовою національної безпеки. Він включає основні принципи, такі як ідентифікація критичної інфраструктури, управління ризиками, забезпечення стійкості та оперативне реагування на надзвичайні ситуації тощо. Закон визначає, які об'єкти та системи вважаються критично важливими для функціонування держави. Це охоплює, зокрема, енергетичний сектор, транспорту, охорони здоров'я, водопостачання та інформаційні технології.

Встановлено також правовий статус операторів критичної інфраструктури та їх обов'язки щодо забезпечення безпеки. Також закон визначає повноваження державних органів, відповідальних за захист критичної інфраструктури, що включає Міністерство інфраструктури, Міністерство енергетики та інші відповідні органи. Закон передбачає формування системи управління ризиками, що включає ідентифікацію, оцінку та моніторинг ризиків, а також розробку планів реагування на надзвичайні ситуації. Оператори критичної інфраструктури зобов'язані розробляти і впроваджувати власні плани захисту, що відповідають державним стандартам.

Крім того, акцентовано увагу на необхідності тісної співпраці між державними органами та приватними операторами критичної інфраструктури. Це передбачає обмін інформацією про загрози, а також спільну роботу над проектами, спрямованими на підвищення стійкості інфраструктури. Важливим аспектом закону є передбачення навчання та підвищення кваліфікації спеціалістів, які працюють у сфері захисту критичної інфраструктури. Це включає не лише теоретичні знання, але й практичні навички, необхідні для швидкого реагування на інциденти. Однак, необхідно зазначити, що реалізація закону стикається з певними викликами. Це включає недостатнє фінансування заходів з безпеки,

необхідність адаптації підприємств до нових вимог, а також складнощі у співпраці між державними структурами та приватним сектором. Проте, незважаючи на ці виклики, закон «Про критичну інфраструктуру» є важливим кроком у зміцненні національної безпеки та підвищенні стійкості держави до зовнішніх і внутрішніх загроз.

Закон України «Про критичну інфраструктуру» від 16.11.2021 №1882-IX, незважаючи на те, що був ухвалений у мирний час, отримав особливу актуальність під час воєнного стану, оголошеного в Україні з 24 лютого 2022 року у зв'язку з агресією з боку Російської Федерації. У цьому контексті, законом №2684-IX від 18.10.2022 року було внесено зміни до раніше прийнятого законодавства, що істотно посилило роль держави в управлінні захистом критичної інфраструктури.

Основні зміни, внесені законом №2684-IX передбачають:

– передачу повноважень; Закон №2684-IX передає повноваження щодо управління системою захисту критичної інфраструктури до Державної служби спеціального зв'язку та захисту інформації України. Це рішення стало відповіддю на зростаючі загрози для критичної інфраструктури, які виникли в умовах війни. Державна служба, яка традиційно відповідала за забезпечення безпеки інформаційних систем, отримала розширені повноваження для охоплення всіх аспектів захисту критичної інфраструктури;

– створення спеціалізованого департаменту; у рамках цих змін був створений Департамент захисту критичної інфраструктури, який відповідає за реалізацію заходів щодо захисту об'єктів критичної інфраструктури; цей департамент функціонує як центральний орган, що координує зусилля різних державних і приватних структур, а також міжнародних партнерів у забезпеченні безпеки критичних об'єктів;

– адаптацію до умов воєнного стану; в умовах воєнного стану, новий законодавчий акт передбачає більш гнучкі механізми реагування на загрози,

що з’являються; це включає оперативне оновлення протоколів безпеки, вдосконалення механізмів взаємодії між державними органами та підприємствами, що керують критичною інфраструктурою, а також забезпечення пріоритетного фінансування для критично важливих об’єктів;

– посилення контролю та моніторингу; закон надає Державній службі спеціального зв’язку повноваження для здійснення моніторингу стану безпеки критичної інфраструктури, проведення регулярних оцінок ризиків, перевірки готовності до надзвичайних ситуацій і розробку сценаріїв реагування на кібератаки або інші загрози;

– співпрацю з міжнародними організаціями; у рамках реалізації закону передбачається активна співпраця з міжнародними партнерами, що включає обмін інформацією, досвідом та кращими практиками у сфері захисту критичної інфраструктури; вказане є важливим для підвищення рівня стійкості об’єктів до зовнішніх загроз, оскільки більшість сучасних загроз має транснаціональний характер.

Ці законодавчі зміни свідчать про проактивний підхід України до захисту критичної інфраструктури в умовах війни. Вони створюють основу для ефективного управління загрозами, з якими стикається країна, і підвищують загальний рівень безпеки в державі.

Упровадження системи захисту критичної інфраструктури дозволяє Україні не лише реагувати на існуючі загрози, але й розробляти довгострокові стратегії для зміцнення стійкості, адаптації до нових викликів і забезпечення безперервності функціонування критично важливих об’єктів.

Законодавство в сфері захисту критичної інфраструктури України продовжує еволюціонувати відповідно до сучасних викликів. Забезпечення належного захисту критичної інфраструктури є важливим аспектом не лише національної безпеки, але й економічного розвитку держави. Система, що формується, має потенціал стати важливим елементом у боротьбі з новими загрозами та викликами, які можуть виникнути в умовах глобальних змін і

нестабільності.

Основні завдання уповноважених органів у сфері захисту критичної інфраструктури включають функціональне управління системою на загальнодержавному рівні, створення та ведення реєстру об’єктів критичної інфраструктури (ОКІ), а також організацію оцінки їх захищеності. Уряд щорічно проводить оцінку ризиків і загроз національного рівня, що дозволяє координувати державну політику в цій галузі.

Уповноважені органи, такі як Державна служба спеціального зв’язку та захисту інформації України, відповідають за координацію дій усіх суб’єктів, що беруть участь у забезпеченні захисту критичної інфраструктури. Це включає стратегічне планування, розробку загальних стратегій і політик, які визначають основні напрямки діяльності у сфері захисту критичної інфраструктури, а також постійний моніторинг стану критичних об’єктів, виявлення вразливостей і контроль за виконанням заходів безпеки.

Важливим аспектом є ведення реєстру об’єктів критичної інфраструктури, що служить основою для планування та підтримує співпрацю з іншими державними реєстрами та базами даних. Крім того, уповноважені органи проводять регулярні оцінки захищеності об’єктів критичної інфраструктури, визначаючи потенційні загрози та вразливості, що можуть вплинути на їх функціонування. Ці оцінки є основою для розробки рекомендацій щодо підвищення рівня захищеності об’єктів, включаючи вдосконалення технологічних, адміністративних та фізичних засобів безпеки.

Щорічна оцінка ризиків і загроз національного рівня, яку проводить уряд, дозволяє координувати державну політику, формувати національну програму безпеки, базуючись на актуальних даних і тенденціях у сфері загроз, а також встановлювати пріоритетні напрямки у захисті критичної інфраструктури, які потребують термінового втручання або підвищених

заходів безпеки.

Секторальні органи, що відповідають за захист критичної інфраструктури в окремих секторах економіки, відіграють важливу роль у реалізації цієї політики. Вони відповідають за категоризацію об’єктів критичної інфраструктури, формування секторальних переліків, а також погодження паспортів безпеки, які містять інформацію про специфіку об’єкта, рівень загроз та відповідні заходи захисту.

Отже, основні завдання уповноважених органів у сфері захисту критичної інфраструктури є комплексними і взаємопов’язаними. Вони не лише сприяють підвищенню рівня безпеки критичних об’єктів, але й забезпечують інтеграцію зусиль національного рівня, що є особливо актуальним в умовах постійно зростаючих загроз. Цей системний підхід до захисту критичної інфраструктури дозволяє Україні створювати ефективні механізми для протидії ризикам, зберігаючи стійкість та безпеку держави в цілому.

В Україні на сьогодні діють різні нормативно-правові акти, які визначають порядок ідентифікації, категоризації та паспортизації об’єктів критичної інфраструктури (ОКІ). Одними з ключових документів у цій сфері є Постанова Кабінету Міністрів України №1109 від 09.10.2020 [55] та Постанова №415 від 28.04.2023 [56]. Ці постанови встановлюють детальні процедури, які забезпечують системний підхід до управління та захисту критичної інфраструктури.

Постанова №1109 від 09.10.2020 стала першим кроком до формалізації механізмів ідентифікації та категоризації ОКІ в Україні. Вона визначає, що усі об’єкти критичної інфраструктури повинні проходити процес ідентифікації на основі їх важливості для національної безпеки, економіки та суспільства. Постанова також встановлює критерії для класифікації об’єктів за їх значенням і вразливістю.

Основні положення Постанови №1109 включають:

– процедуру ідентифікації - встановлюються механізми для виявлення об’єктів, які підлягають категоризації, на основі їх важливості для функціонування держави;

– класифікацію об’єктів - запроваджуються категорії для різних типів ОКІ, що дозволяє встановити пріоритети у їх захисті;

– формування паспорта безпеки - постанова зобов’язує власників об’єктів розробити паспорти безпеки, які містять інформацію про характеристики об’єкта, рівень загроз і необхідні заходи захисту.

З прийняттям Постанови №415 у 2023 році, нормативно-правова база в сфері захисту критичної інфраструктури була значно розширена [56]. Ця постанова деталізує процедуру ведення Реєстру об’єктів критичної інфраструктури, що є центральним елементом системи захисту.

Ключові аспекти Постанови №415 включають:

– ведення Реєстру ОКІ - встановлюються вимоги до ведення Реєстру об’єктів критичної інфраструктури, що дозволяє систематизувати інформацію про всі критичні об’єкти та їх характеристики;

– моніторинг та аналіз - з метою забезпечення стійкості та безпеки об’єктів, передбачається регулярний моніторинг їх стану, оцінку ризиків і загроз, а також впровадження відповідних заходів реагування;

– координація заходів захисту - регламентується механізми координації дій між різними державними органами, що відповідають за захист критичної інфраструктури, зокрема у випадках виникнення загроз або надзвичайних ситуацій.

Обидві постанови є важливими складовими унормування функціонування системи управління критичною інфраструктурою в Україні, оскільки вони сприяють формуванню чіткої та ефективної структури захисту, що забезпечує національну безпеку. Системний підхід до ідентифікації та паспортизації ОКІ, закладений у цих нормативних актах, дозволяє Україні бути більш готовою до реагування на сучасні виклики в

умовах постійно зростаючих кіберзагроз та інших ризиків. Зазначені постанови слугують основою для подальшого розвитку механізмів захисту критичної інфраструктури, які повинні адаптуватися до динамічного середовища загроз і потребувати постійного вдосконалення на всіх рівнях управління.

Моніторинг рівня безпеки є важливою складовою системи захисту критичної інфраструктури, оскільки він дозволяє регулярно оцінювати стан захищеності об’єктів, які включені до реєстру. Безперервний моніторинг є критично важливим для забезпечення своєчасного виявлення вразливостей та загроз, що може суттєво вплинути на національну безпеку.

Ці процеси регламентовані Постановами Кабінету Міністрів України від 22.07.2022 №821 Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури [57] та Про затвердження Регламенту обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури від 14.10.2022 №1174 [58], які визначають механізми обміну інформацією між суб’єктами системи захисту, а також заходи реагування у кризових ситуаціях.

Постанова №821 від 22.07.2022 встановлює порядок проведення моніторингу та оцінки рівня безпеки об’єктів критичної інфраструктури. Основні положення цієї постанови включають:

– регулярність оцінки - постанова передбачає, що моніторинг стану захищеності ОКІ має проводитися на регулярній основі, що дозволяє оперативно реагувати на зміни в зовнішньому середовищі та адаптувати заходи безпеки;

– методологію оцінки для оцінки ризиків і загроз, що допомагає визначити, які саме аспекти безпеки потребують посилення чи вдосконалення;

– обмін інформацією - постанова акцентує увагу на необхідності обміну інформацією між різними суб’єктами системи захисту, що

забезпечує більш ефективну координацію дій і підвищує рівень готовності до реагування на можливі загрози.

Постанова №1174 від 14.10.2022 розширює механізми реагування у кризових ситуаціях і визначає порядок дій у разі виникнення загроз для критичної інфраструктури. Її основні положення включають:

– план реагування - постанова зобов’язує створення планів реагування на надзвичайні ситуації для кожного об’єкта критичної інфраструктури. Це дозволяє швидко і чітко реагувати на різноманітні загрози, включаючи кібернетичні атаки, природні катастрофи та техногенні аварії;

– впровадження систем раннього попередження, які допомагають своєчасно виявляти загрози та оперативно реагувати на них;

– координація дій - у документі також регламентується координація дій між різними державними органами та приватними суб’єктами, що забезпечує комплексний підхід до захисту критичної інфраструктури.

Впровадження зазначених постанов значно підвищує ефективність моніторингу рівня безпеки об’єктів критичної інфраструктури. Систематичний підхід до оцінки їх захищеності дозволяє не лише виявляти потенційні загрози, але й оперативно реагувати на них, що є особливо важливим в умовах зростаючих ризиків у сучасному світі.

Крім того, наявність чітких механізмів обміну інформацією між різними суб’єктами забезпечує прозорість процесів і дає змогу всім учасникам системи захисту діяти у скоординованій манері. Це, в свою чергу, підвищує загальний рівень безпеки критичної інфраструктури та зміцнює національну безпеку України в цілому.

Таким чином, моніторинг рівня безпеки та своєчасне реагування на виявлені загрози є ключовими елементами в забезпеченні надійності та стійкості критичної інфраструктури країни. Вони дозволяють адаптувати систему захисту до динамічних умов, що зумовлюються як внутрішніми,

так і зовнішніми факторами.

Отже, законодавча база захисту критичної інфраструктури в Україні демонструє проактивний підхід до забезпечення національної безпеки в умовах сучасних викликів. Необхідність інтеграції дій усіх суб'єктів, а також постійна адаптація до нових загроз, свідчать про динамічний розвиток у цій сфері. З урахуванням цих тенденцій, можна стверджувати, що законодавство в Україні прагне не лише реагувати на існуючі загрози, але й забезпечувати довгострокову стійкість критичної інфраструктури, що є основою для стабільного розвитку держави.

3.2. Роль та завдання органів державної влади у захисті критичної інфраструктури

Відомо, що критична інфраструктура є основою стабільного функціонування суспільства та економіки. Будь-які порушення в її роботі можуть призвести до серйозних наслідків, які можуть загрожувати національній безпеці, суспільному порядку та життю громадян. У сучасних умовах глобалізації та динамічного технологічного розвитку захист критичної інфраструктури є одним із пріоритетних завдань державної політики. Ефективний захист критичної інфраструктури можливий лише за умови злагодженої роботи різних державних органів, які мають специфічні повноваження та обов'язки в цій сфері. Від їхніх дій залежить не лише своєчасне реагування на загрози, але й запобігання можливим кризовим ситуаціям. У рамках державної системи управління захистом КІ важливу роль відіграють центральні органи влади, уповноважені органи у сфері захисту критичної інфраструктури, місцеві органи влади, які відповідають за реалізацію політики у відповідних секторах, здійснюють моніторинг та аналіз ризиків, а також розробляють заходи для підвищення стійкості критичної інфраструктури до зовнішніх і внутрішніх загроз.

Кабінет Міністрів України (КМУ) [59] виконує ключову роль у загальному управлінні та координації дій усіх органів влади, які беруть участь у забезпеченні захисту критичної інфраструктури. Як вищий орган виконавчої влади, КМУ формує державну політику в цій сфері, що є особливо важливим у контексті забезпечення національної безпеки та стійкості суспільства.

По-перше, КМУ визначає стратегічні напрямки і загальні принципи політики у сфері захисту критичної інфраструктури, що регулюється ключовими законодавчими актами, такими як Закон України «Про національну безпеку України» (2018) [1] і Закон України «Про критичну інфраструктуру України» (2017) [2]. Ці закони встановлюють основні засади, цілі та завдання державної політики у сфері захисту критичної інфраструктури, а також механізми її реалізації.

По-друге, КМУ має повноваження розробляти та затверджувати державні програми і плани дій, спрямовані на захист критичної інфраструктури. Серед них можна виділити Національну програму з питань захисту критичної інфраструктури, яка містить заходи для зміцнення безпеки об’єктів критичної інфраструктури, що підлягають захисту. Також важливими є плани реагування на надзвичайні ситуації, які передбачають алгоритми дій державних органів та місцевих адміністрацій у разі виникнення загроз або надзвичайних ситуацій, пов’язаних із функціонуванням критичної інфраструктури, а також стратегія кіберзахисту, що спрямована на захист інформаційних систем критичної інфраструктури від кіберзагроз.

КМУ відповідає за забезпечення взаємодії між різними міністерствами та відомствами, що беруть участь у захисті критичної інфраструктури, формуючи єдину систему управління. Це включає Міністерство енергетики України, яке відповідає за безпеку енергетичної інфраструктури, Міністерство інфраструктури України, що здійснює

контроль за транспортною інфраструктурою та логістичними мережами, і Міністерство охорони здоров'я України, яке забезпечує функціонування медичної інфраструктури та реагування на кризові ситуації у сфері охорони здоров'я. Крім того, КМУ здійснює систематичний моніторинг стану об'єктів критичної інфраструктури, а також проводить оцінку ризиків і загроз, які можуть вплинути на їх функціонування. Ця діяльність дозволяє своєчасно виявляти потенційні проблеми та вживати необхідних заходів для їх усунення.

Таким чином, Кабінет Міністрів України виступає ключовим органом у системі державного управління, що відповідає за формування та реалізацію політики захисту критичної інфраструктури, забезпечуючи належний рівень безпеки та стійкості суспільства.

Міністерство енергетики України [60] відіграє основну роль у забезпеченні безпеки енергетичної інфраструктури, що є однією з ключових складових критичної інфраструктури країни. В умовах глобальних викликів, зокрема зміни клімату, зростання попиту на енергію та загроз з боку зовнішніх і внутрішніх чинників, безпека енергетичного сектора стає пріоритетом державної політики.

Міністерство енергетики розробляє та затверджує нормативно-правові акти, які регулюють діяльність у сфері енергетики. Одним із основних законодавчих актів у цій сфері є Закон України «Про електроенергетику», який визначає основні принципи функціонування ринку електричної енергії, механізми забезпечення безпеки постачання електроенергії, а також регулює діяльність суб'єктів ринку електричної енергії. Закон передбачає обов'язкову сертифікацію енергетичних компаній, що діють у цій сфері, а також встановлює вимоги до їх діяльності з метою забезпечення надійності постачань та підтримки стабільності енергетичної системи.

Міністерство здійснює аналіз ризиків у енергетичному секторі відповідно до норм Закону України «Про енергетичну ефективність» [61].

Цей закон передбачає впровадження заходів щодо підвищення енергоефективності, що сприяє зменшенню споживання енергії та оптимізації витрат у різних галузях економіки. Міністерство проводить оцінку ризиків, пов’язаних із виробництвом, транспортуванням та споживанням енергетичних ресурсів, що дозволяє своєчасно виявляти загрози та вживати відповідних заходів для їх мінімізації.

У рамках своїх функцій Міністерство також забезпечує моніторинг стану енергетичної інфраструктури, організовує проведення перевірок та аудиту підприємств, що працюють у енергетичній сфері, та здійснює контроль за їх відповідністю встановленим нормам і стандартам. Це передбачає як регулярний аналіз технічного стану енергетичних об’єктів, так і оцінку їх готовності до надзвичайних ситуацій.

Крім того, Міністерство енергетики співпрацює з іншими державними органами, такими як Державна служба спеціального зв’язку та захисту інформації України, Державна інспекція енергетичного нагляду, а також з міжнародними партнерами для обміну досвідом у сфері енергетичної безпеки. Це співробітництво включає розробку спільних програм та ініціатив, спрямованих на зміцнення енергетичної безпеки держави, включаючи кіберзахист енергетичних об’єктів та адаптацію до нових технологій.

Загалом, Міністерство енергетики України виступає головним державним органом, відповідальним за формування та реалізацію політики у сфері енергетичної безпеки, виконуючи ключові функції, які забезпечують стабільність та стійкість енергетичної інфраструктури країни в умовах постійних викликів і загроз.

Міністерство розвитку громад та територій України [62] є центральним органом виконавчої влади, відповідальним за формування та реалізацію державної політики в галузі транспорту та інфраструктури. Воно відіграє ключову роль в управлінні критично важливою інфраструктурою

країни, забезпечуючи стабільну роботу транспортних систем і логістичних шляхів.

Основні завданнями цього органу є:

Формування державної політики у сфері транспорту. Одним із головних завдань Міністерствf розвитку громад та територій України є розробка та впровадження державної політики у сфері транспортної інфраструктури. Відповідно до Закону України «Про транспорт» (ст. 8), міністерство забезпечує розробку і вдосконалення законодавчих норм і регуляторних механізмів у всіх видах транспорту (залізничний, автомобільний, авіаційний, водний тощо).

Безпека транспортної інфраструктури. Міністерство відповідальне за забезпечення безпеки транспортних шляхів і засобів пересування. Для цього воно впроваджує національні та міжнародні стандарти безпеки, зокрема через інтеграцію рекомендацій Європейського Союзу, ООН та інших міжнародних організацій. До його компетенції входить контроль за дотриманням стандартів безпеки на дорогах, аеропортах, морських і річкових портах, а також на залізничних шляхах.

Контроль і управління транспортною інфраструктурою. Міністерство забезпечує ефективне функціонування транспортної інфраструктури країни, включаючи дороги, мости, тунелі, аеропорти, порти та залізниці. Одним із важливих аспектів є модернізація транспортних шляхів і покращення їхньої стійкості до зовнішніх загроз. Це передбачає реалізацію програм будівництва та реконструкції інфраструктурних об’єктів.

Координація з іншими міністерствами і відомствами передбачає тісну співпрацю з іншими органами виконавчої влади, такими як Міністерство внутрішніх справ (МВС), Міністерство оборони (МОУ), Державна служба надзвичайних ситуацій (ДСНС). Ця взаємодія є особливо важливою для забезпечення національної безпеки та реагування на надзвичайні ситуації, що можуть виникнути в транспортній інфраструктурі.

Інвестиційна політика та міжнародна співпраця. Важливою частиною діяльності міністерства є залучення інвестицій у транспортну інфраструктуру та розвиток міжнародної співпраці, активна співпраця з міжнародними фінансовими організаціями, такими як Світовий банк і Європейський банк реконструкції та розвитку, для реалізації масштабних інфраструктурних проектів, спрямованих на покращення транспортної мережі країни.

Розробка стратегій щодо модернізації транспортних систем. Міністерство відповідає за довгострокове планування розвитку транспортної системи України. Це включає розробку стратегічних програм модернізації транспортних засобів та шляхів, спрямованих на зменшення викидів, підвищення енергоефективності та поліпшення екологічних стандартів.

Розвиток логістики та транспортних коридорів. Міністерство бере активну участь у розвитку міжнародних транспортних коридорів, зокрема в межах таких ініціатив, як Транскаспійський транспортний коридор і ініціатива «Один пояс, один шлях» (Belt and Road Initiative). Це сприяє інтеграції транспортної системи України в глобальні ланцюги постачання.

Забезпечення стійкості інфраструктури до надзвичайних ситуацій. Орган реалізує заходи для покращення стійкості інфраструктурних об’єктів до природних катастроф, техногенних аварій, терористичних актів та інших надзвичайних ситуацій. Це включає реалізацію комплексних програм підготовки транспортної інфраструктури до реагування на кризи та покращення кібербезпеки транспортних систем.

Отже, міністерство розвитку громад та територій України є важливим гравцем у формуванні та реалізації державної політики у сфері транспортної інфраструктури. Його діяльність охоплює широкий спектр питань – від розробки та впровадження законодавчих актів до забезпечення безпеки транспортних систем і шляхів. Завдяки міжнародній співпраці, залученню

інвестицій та модернізації інфраструктури, міністерство сприяє інтеграції України в міжнародні транспортні системи, що має велике значення для економічного зростання та національної безпеки країни.

Міністерство охорони здоров'я України (МОЗ) [63] є центральним органом виконавчої влади, який відповідає за формування та реалізацію державної політики в галузі охорони здоров'я. Однією з основних його функцій є гарантування медичної безпеки, особливо у випадках надзвичайних ситуацій, епідемій, пандемій та інших загроз для здоров'я населення. МОЗ також координує діяльність у сфері охорони здоров'я на національному та регіональному рівнях, забезпечуючи ефективне реагування на потенційні медичні кризи.

Основні функції та обов'язки цього органу такі.

Реалізація заходів у надзвичайних ситуаціях у сфері охорони здоров'я. МОЗ розробляє та впроваджує заходи для запобігання і протидії епідеміям, пандеміям та іншим надзвичайним ситуаціям у сфері охорони здоров'я. Відповідно до Закону України "Про захист населення від інфекційних хвороб", МОЗ є головним органом, відповідальним за проведення санітарних та протиепідемічних заходів, а також забезпечення карантинних обмежень у разі виникнення епідеміологічних загроз.

Організація реагування на медичні надзвичайні ситуації. МОЗ забезпечує підготовку та координацію реагування на медичні надзвичайні ситуації шляхом реалізації нормативних документів і постанов Кабінету Міністрів України, що регулюють порядок дій у випадку надзвичайних ситуацій, а також підготовку медичних закладів до реагування на кризові ситуації. МОЗ організовує навчання та підвищення кваліфікації медичних працівників для роботи в умовах надзвичайних ситуацій, включаючи інфекційні спалахи та масові травматичні події.

Координація міжвідомчих зусиль і взаємодія з іншими державними органами. Для ефективного забезпечення медичної безпеки МОЗ

співпрацює з іншими державними структурами, такими як Міністерство внутрішніх справ (МВС), Державна служба надзвичайних ситуацій (ДСНС) та Міністерство оборони України. Така координація дозволяє розподілити ресурси, підвищити готовність системи охорони здоров'я та забезпечити швидку реакцію на надзвичайні ситуації.

Забезпечення санітарного та епідеміологічного нагляду. МОЗ, у співпраці з Державною службою з питань безпеки харчових продуктів та захисту споживачів [64], відповідає за моніторинг і контроль інфекційних хвороб. Це включає запобігання спалахам небезпечних інфекцій, проведення регулярного санітарного нагляду, впровадження профілактичних заходів та забезпечення доступу до вакцин та медичних препаратів. МОЗ також контролює реалізацію програм з імунізації та боротьби з інфекційними хворобами.

Інформування громадськості та підвищення обізнаності. Міністерство регулярно інформує населення про поточні загрози для здоров'я, надає рекомендації щодо захисту від інфекційних хвороб та розповсюджує інформацію про заходи профілактики. Це включає організацію інформаційних кампаній, поширення рекомендацій для громадян у випадку спалахів захворювань і підтримку роботи гарячих ліній для інформування населення.

Міжнародна співпраця у сфері охорони здоров'я. МОЗ активно співпрацює з міжнародними організаціями, такими як Всесвітня організація охорони здоров'я (ВООЗ), Європейський центр з профілактики та контролю захворювань (ECDC), ООН, а також урядами інших країн. Така співпраця дозволяє Україні залучати міжнародний досвід, інновації та ресурси для підвищення ефективності медичних заходів. Зокрема, МОЗ бере участь у програмах обміну даними, що дозволяє швидко отримувати інформацію про нові загрози та підтримувати оперативне реагування на глобальні епідемії.

Забезпечення матеріально-технічної бази та інфраструктури для

медичних заходів. МОЗ відповідає за надання необхідних матеріалів, медичного обладнання, препаратів та технічних засобів для ефективного реагування на медичні кризи. Це включає забезпечення лікарень, мобільних медичних пунктів та лабораторій необхідними ресурсами, а також планування закупівель і розподіл медичних засобів на випадок надзвичайних ситуацій.

Отже, Міністерство охорони здоров'я України виконує одну з найважливіших функцій у системі національної безпеки, забезпечуючи готовність медичних установ та кадрового персоналу до реагування на надзвичайні ситуації, що можуть загрожувати здоров'ю населення. Завдяки законодавчим актам, міжвідомчій співпраці та міжнародному партнерству МОЗ здатне оперативно реагувати на медичні загрози, а також забезпечувати ефективну профілактику й інформування громадян щодо нових викликів.

Державна служба України з надзвичайних ситуацій (ДСНС) відіграє центральну роль у забезпеченні цивільного захисту та реагування на надзвичайні ситуації в Україні. ДСНС здійснює оперативне реагування на різного роду надзвичайні ситуації, а також виконує превентивні заходи для зниження їхнього впливу на населення і території. Діяльність Служби поширюється на всі етапи управління надзвичайними ситуаціями, від попередження ризиків до ліквідації їхніх наслідків, що охоплює як природні, так і техногенні катастрофи [65].

Цей комплексний підхід є особливо важливим для забезпечення національної безпеки та стабільності держави.

До основних функції ДСНС належить:

Оперативне реагування на надзвичайні ситуації. ДСНС несе відповідальність за швидку координацію дій у разі виникнення надзвичайних ситуацій, включаючи природні катастрофи, техногенні аварії, екологічні катастрофи, терористичні акти та інші загрози. Відповідно до

Кодексу цивільного захисту України, Служба використовує комплексний підхід для забезпечення якнайшвидшої локалізації та ліквідації наслідків інцидентів. Це включає:

– координацію дій між різними відомствами та рятувальними службами;

– мобілізацію необхідних ресурсів та технічних засобів для реагування;

– забезпечення тимчасового розселення і допомоги постраждалим, а також організацію евакуаційних заходів.

Навчання та підготовка населення. Однією з пріоритетних функцій ДСНС є підвищення обізнаності населення щодо дій в умовах надзвичайних ситуацій. Це включає проведення навчань, семінарів та тренінгів для громадян різного віку. Зокрема: навчальні програми для громадськості – курси та інформаційні кампанії з безпеки, які допомагають громадянам дізнатися про основні ризики, методи уникнення небезпеки, правила поведінки в разі стихійного лиха або техногенної катастрофи; програми для учнів і студентів – спеціалізовані навчальні матеріали та програми, що охоплюють основи безпеки життєдіяльності, що є частиною освітніх курсів у навчальних закладах.

Попередження та управління ризиками. У межах своїх повноважень ДСНС проводить системний аналіз і оцінку потенційних ризиків. З метою запобігання виникненню надзвичайних ситуацій, Служба реалізує комплекс профілактичних заходів:

– моніторинг та прогнозування загроз – збір і аналіз даних щодо можливих природних катастроф або техногенних аварій, таких як повені, землетруси, пожежі та інші загрози;

– аналіз інфраструктури та потенційних ризиків – перевірка надійності інфраструктурних об’єктів і підприємств із високим ризиком, а також проведення оцінки готовності цих об’єктів до надзвичайних ситуацій.

Інформаційне забезпечення та система оповіщення. ДСНС відповідає за своєчасне інформування населення та органів влади про надзвичайні ситуації. Служба забезпечує функціонування загальнонаціональної системи оповіщення, яка включає централізовану систему оповіщення – використання звукових сигналів, теле- та радіотрансляцій для інформування громадян у разі загрози; систему мобільного інформування – інтеграція з мобільними операторами для надсилання текстових повідомлень на мобільні телефони громадян у разі надзвичайних ситуацій.

Забезпечення ресурсів та матеріально-технічної бази. ДСНС також відповідає за створення, розвиток і утримання технічної бази, що дозволяє оперативно реагувати на надзвичайні ситуації. Це передбачає мобілізацію техніки, спеціалізованого обладнання і транспорту; забезпечення особового складу необхідними засобами захисту, аварійного та пожежного обладнання; розробку і підтримку запасів матеріальних ресурсів для оперативного реагування у разі масштабних інцидентів.

Отже, діяльність ДСНС є критично важливою для забезпечення національної безпеки та збереження життя громадян України. Завдяки комплексному підходу до управління надзвичайними ситуаціями, системному навчанню населення та тісній взаємодії з міжнародними партнерами, Служба створює базу для ефективного попередження, локалізації та ліквідації наслідків катастроф.

Державна служба спеціального зв’язку та захисту інформації України (ДССЗЗІ) [66] відіграє ключову роль у забезпеченні інформаційної безпеки держави, що є основою для захисту критичної інфраструктури. У умовах зростаючих кіберзагроз та загроз інформаційній безпеці, ДССЗЗІ відповідальна за формування та реалізацію державної політики у цій сфері.

Завдання та функції ДССЗЗІ у сфері захисту критичної інфраструктури наступні.

Координація захисту інформаційних систем критичної

інфраструктури. ДССЗЗІ координує зусилля з захисту інформаційних систем критичної інфраструктури через створений Департамент захисту критичної інфраструктури. Цей департамент забезпечує виконання державних програм, спрямованих на підвищення стійкості інформаційних систем до загроз. Основною метою департаменту є реалізація заходів, передбачених Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» [67], який визначає правові, організаційні та технологічні засади захисту інформації в таких системах.

Забезпечення інформаційної безпеки та захисту даних. ДССЗЗІ виконує заходи щодо забезпечення інформаційної безпеки, що включає в себе аналіз загроз, розробку та реалізацію заходів захисту даних. Це охоплює як технологічні, так і організаційні рішення для забезпечення безпеки інформаційних систем. В рамках цієї функції служба проводить навчання та підготовку фахівців у сфері інформаційної безпеки, що є важливим елементом для створення безпечного інформаційного середовища.

Моніторинг та реагування на загрози. ДССЗЗІ здійснює постійний моніторинг стану інформаційної безпеки в Україні, виявляє нові загрози та вживає заходів для їх нейтралізації. Це включає в себе оперативне реагування на кіберінциденти та співпрацю з іншими державними органами, міжнародними організаціями та приватним сектором. У разі виявлення загроз інформаційній безпеці, служба має право ініціювати проведення розслідувань та впроваджувати спеціальні заходи для захисту критичних інформаційних ресурсів.

Співпраця з міжнародними організаціями. ДССЗЗІ активно співпрацює з міжнародними організаціями та партнерськими країнами у сфері обміну інформацією та найкращими практиками у захисті критичної інфраструктури. Це важливо для отримання доступу до нових технологій та методик захисту, а також для підвищення загального рівня безпеки в країні.

Таким чином, Державна служба спеціального зв'язку та захисту інформації України є невід'ємною частиною системи захисту критичної інфраструктури в Україні. Успішна реалізація вищевказаних функцій сприяє підвищенню стійкості критичної інфраструктури та забезпечує безпеку інформаційного середовища в державі.

Служба безпеки України [68] та Національна поліція України [69] виконують критично важливі функції у забезпеченні захисту критичної інфраструктури. Їхня роль у запобіганні тероризму, охороні об'єктів та координації дій з іншими органами влади забезпечує комплексний підхід до національної безпеки. Ефективна взаємодія між цими органами є запорукою успішного реагування на загрози та підтримки стабільності в країні.

Місцеві органи влади є важливими учасниками у системі управління критичною інфраструктурою. Їхня діяльність зосереджена на реалізації державної політики на місцевому рівні та забезпечення безпеки та функціонування критично важливих об'єктів у межах їх юрисдикції. Від ефективності роботи місцевих органів влади значною мірою залежить успішність виконання завдань національної безпеки, включаючи захист критичної інфраструктури. Функції органів державної влади у сфері захисту критичної інфраструктури наведені у таблиці 4.

Підсумовуючи, зазначимо, що ефективність системи захисту критичної інфраструктури залежить від низки ключових факторів, що забезпечують комплексний та адаптивний підхід до захисту об'єктів, які є основою національної безпеки. Першим важливим фактором є чіткий розподіл відповідальності між органами державної влади. Кожен з них має чітко визначені функції, що забезпечує скоординованість дій у надзвичайних ситуаціях та дозволяє уникати дублювання зусиль. Так, відповідні міністерства та служби, інші профільні відомства розробляють та реалізують стратегії захисту критичної інфраструктури, забезпечуючи оперативність та ефективність в управлінні кризами.

Таблиця 4

Функції органів державної влади у сфері захисту критичної інфраструктури

Орган державної влади	Сфера діяльності	Основні функції
Кабінет Міністрів України	Загальне управління	- координація діяльності всіх органів влади у сфері захисту критичної інфраструктури - формування та реалізація через уповноважені органи державної політики у сфері захисту критичної інфраструктури
Міністерство енергетики України	Енергетичний сектор	- регулювання енергетичних відносин - захист енергетичної інфраструктури - розробка стандартів безпеки в енергетичному секторі
Міністерство інфраструктури України	Транспорт та інфраструктура	- управління транспортною інфраструктурою - забезпечення безпеки транспортних засобів і шляхів - розробка нормативних актів для транспортних об’єктів
Міністерство охорони здоров’я України	Охорона здоров’я	- забезпечення медичної безпеки - підготовка до надзвичайних ситуацій у сфері охорони здоров’я - контроль за санітарно-епідеміологічним станом
Державна служба України з надзвичайних ситуацій (ДСНС)	Цивільний захист	- реагування на надзвичайні ситуації - проведення рятувальних операцій - оцінка загроз і ризиків для критичної інфраструктури
Служба безпеки України (СБУ)	Національна безпека	- захист національних інтересів - запобігання тероризму та екстремізму - викриття загроз для критичної інфраструктури
Національна поліція України	Правопорядок	- забезпечення правопорядку на об’єктах критичної інфраструктури - запобігання правопорушенням - реагування на кримінальні загрози
Державна служба спеціального зв’язку та захисту інформації	Інформаційна безпека	- забезпечення стабільності зв’язку - контроль за інформаційною безпекою
Департамент захисту критичної інфраструктури	Координація зусиль між різними стейкхолдерами, що забезпечує інтегрований підхід до захисту критичної інфраструктури.	координація зусиль державних і приватних структур та міжнародних партнерів у забезпеченні безпеки критичних об’єктів - реалізація заходів щодо захисту об’єктів критичної інфраструктури - захист інформаційних систем критичної інфраструктури
Місцеві органи влади	Місцеве управління	- реалізація політики на місцевому рівні - співпраця з центральними органами

Джерело: складено автором

Другий фактор – це наявність сучасних технологій для моніторингу та управління ризиками. Технологічний розвиток значно підвищує здатність систем критичної інфраструктури виявляти потенційні загрози ще на етапі їх виникнення. Впровадження новітніх засобів моніторингу, таких як штучний інтелект, великі дані, системи раннього оповіщення та автоматизовані платформи, забезпечує можливість швидко виявляти потенційні загрози та реагувати на них. Ці інновації дозволяють забезпечити точний аналіз ситуації та прогнозування можливих ризиків, що значно підвищує загальну стійкість системи.

Наступним важливим фактором є регулярне навчання та підготовка фахівців, які безпосередньо працюють у сфері захисту критичної інфраструктури. Постійна підготовка дозволяє працівникам набувати новітніх методів реагування на надзвичайні ситуації та підтримувати високий рівень професійних навичок. Організація тренінгів, навчальних семінарів і симуляцій надзвичайних ситуацій допомагає розвивати координацію дій, покращувати комунікацію та відпрацьовувати навички швидкого реагування в умовах реальних криз.

Четвертим ключовим фактором є тісна співпраця з приватним сектором та міжнародними організаціями. Значна частина критичної інфраструктури перебуває у приватній власності, тому налагодження державно-приватного партнерства є необхідною умовою для забезпечення її безпеки. Держава та приватні компанії співпрацюють у сфері обміну інформацією про загрози, розробці спільних стандартів безпеки, а також у проведенні навчань. Міжнародна співпраця з організаціями, як-от НАТО, ООН та ЄС, забезпечує доступ до передового досвіду, сучасних технологій і методів управління ризиками, що сприяє підвищенню рівня захищеності інфраструктури від глобальних загроз.

Постійна адаптація до нових загроз та викликів є фінальним аспектом, який забезпечує актуальність системи захисту критичної інфраструктури. У

сучасному світі загрози постійно еволюціонують – це стосується кіберзагроз, терористичних атак, кліматичних змін тощо. Система має бути динамічною та здатною швидко адаптуватися до нових умов, що вимагає регулярного перегляду стратегій та процедур, впровадження нових технологій та інструментів.

Ці фактори в комплексі створюють надійну систему захисту критичної інфраструктури та стабільне функціонування ключових державних об’єктів та безпеку суспільства в умовах новітніх викликів і загроз.

3.3. Державно-приватне партнерство у галузі

Державно-приватне партнерство (ДПП) набуло критичного значення у сфері захисту критичної інфраструктури, оскільки ефективна безпека залежить від спільних зусиль держави та приватного сектору. Сучасна інфраструктура включає численні об’єкти та системи, більшість яких перебуває у приватній власності або управляється приватними операторами, що обумовлює потребу у взаємодії між державою та бізнесом для забезпечення надійного захисту від фізичних, кібернетичних та інших загроз.

Основними елементами такої співпраці є обмін інформацією про ризики, розробка загальних стандартів безпеки, а також спільні зусилля у реагуванні на надзвичайні ситуації. За допомогою державно-приватного партнерства вдається ефективніше управляти ризиками, а також підвищувати стійкість критичної інфраструктури до сучасних викликів, як-от тероризм, кіберзагрози чи природні катастрофи. Окрім цього, органи державної влади отримують можливість сприяти підготовці приватних структур до кризових ситуацій, надаючи доступ до ресурсів, експертизи та новітніх технологій.

Приватний сектор несе відповідальність за низку аспектів захисту критичної інфраструктури, зокрема за забезпечення фізичної безпеки об’єктів, впровадження заходів кібербезпеки, управління ризиками та зменшення їхньої потенційної шкоди. Зокрема, у сфері кібербезпеки приватні компанії інвестують у сучасні технології захисту даних, застосовують механізми моніторингу для виявлення загроз у режимі реального часу, впроваджують системи раннього попередження та відновлення після кіберінцидентів. Такі компанії також відповідають за фізичну безпеку своїх об’єктів, що включає впровадження заходів, які запобігають проникненню сторонніх осіб, забезпечують охорону та контролюють доступ до об’єктів критичної інфраструктури.

Важливою частиною залучення приватного сектору є управління ризиками, що охоплює оцінку та аналіз потенційних загроз, які можуть завдати шкоди критично важливим об’єктам. Приватні компанії розробляють плани дій на випадок надзвичайних ситуацій, а також активно співпрацюють з державними органами для своєчасного обміну інформацією про загрози, що дозволяє координувати заходи реагування та підвищувати стійкість інфраструктури до кризових подій.

Узгоджена співпраця між державою і приватним сектором сприяє створенню національних стандартів безпеки, які є обов’язковими до виконання і гарантують захищеність об’єктів критичної інфраструктури. Державні установи, зі свого боку, надають компаніям методичну та матеріально-технічну підтримку, організовують навчання та тренінги для персоналу, а також проводять перевірки дотримання вимог безпеки, забезпечуючи мінімізацію ризиків та стійкість у випадку виникнення кризових ситуацій.

ДПП у сфері захисту критичної інфраструктури регулюється низкою законодавчих актів та постанов, що визначають механізми співпраці між державою та приватним сектором для забезпечення національної безпеки.

Основною метою цих правових інструментів є забезпечення координації між державними органами та приватними компаніями, особливо у тих сферах, де інфраструктура перебуває у приватній власності.

Закон України «Про державно-приватне партнерство» [70] регулює правові, економічні та організаційні аспекти ДПП у різних галузях, включаючи критичну інфраструктуру. Він визначає основи та принципи взаємодії між державними та приватними партнерами, такі як рівноправність сторін, прозорість процесу прийняття рішень, а також забезпечення надійного захисту від можливих ризиків.

Кодекс цивільного захисту України встановлює порядок реалізації заходів із забезпечення безпеки об’єктів критичної інфраструктури, а також передбачає співпрацю між державними органами і приватним сектором у контексті надзвичайних ситуацій. Згідно з цим кодексом, приватні підприємства, що володіють об’єктами критичної інфраструктури, повинні дотримуватися встановлених норм безпеки, виконувати планові перевірки та брати участь у навчаннях, організованих державними органами.

Закон України «Про основні засади забезпечення кібербезпеки України» [71] визначає принципи забезпечення кібербезпеки в Україні і передбачає обов’язки державних та приватних структур щодо захисту інформаційних систем, що належать до критичної інфраструктури. Закон зобов’язує суб’єктів господарювання у критичній інфраструктурі забезпечувати захист інформаційних систем та обмінюватися інформацією про кіберзагрози з державними органами, зокрема з Державною службою спеціального зв’язку та захисту інформації.

Постанова Кабінету Міністрів України №943 «Деякі питання об’єктів критичної інформаційної інфраструктури» [72] регулює питання визначення та захисту об’єктів критичної інформаційної інфраструктури (КІІ) в Україні. Документ встановлює:

– процедуру ідентифікації об’єктів КІІ – визначає критерії для

віднесення певних інформаційних ресурсів та об’єктів до категорії критичних, що мають значення для національної безпеки, економіки, охорони здоров’я тощо;

– обов’язки суб’єктів КІІ – накладає обов’язки на організації, що володіють або використовують такі об’єкти, забезпечувати їхню безпеку, виконувати вимоги з кіберзахисту та своєчасно оновлювати дані про об’єкти у відповідних реєстрах;

– захист та відповідальність за кібербезпеку – встановлює вимоги до суб’єктів КІІ щодо захисту своїх об’єктів від кіберзагроз, а також зобов’язує їх взаємодіяти з державними органами, зокрема Держспецзв’язку, у сфері обміну інформацією про кіберінциденти;

– механізми моніторингу та контролю – створює умови для державного нагляду і контролю за виконанням суб’єктами КІІ обов’язкових вимог із кібербезпеки, а також передбачає періодичні перевірки і моніторинг стану захисту таких об’єктів.

Ця постанова є важливим компонентом української системи кібербезпеки і спрямована на підвищення стійкості критичної інформаційної інфраструктури перед загрозами та кіберінцидентами.

В Україні приватні компанії, особливо ті, що керують об’єктами критичної інфраструктури, зобов’язані дотримуватися низки регуляторних вимог для забезпечення безпеки своїх активів. Це включає комплексну підготовку, стратегічне планування і співпрацю з органами державної влади шляхом:

– обов’язкової участі у заходах із забезпечення безпеки (приватні компанії повинні брати участь у регулярних навчаннях, тренінгах та симуляційних тренуваннях, спрямованих на підвищення готовності до кризових ситуацій та забезпечення належного рівня безпеки на об’єктах критичної інфраструктури. Зокрема, Кодекс цивільного захисту України та Постанови Кабінету Міністрів України передбачають обов’язкові навчання

для персоналу таких підприємств, що дозволяє їм бути готовими до різних сценаріїв надзвичайних ситуацій; проводяться спільні заходи з ДСНС, СБУ, Нацполіцією та іншими органами, що сприяє кращій координації під час реальних загроз);

– розробки та виконання планів безпеки (приватні компанії зобов'язані розробляти плани безпеки для своїх об'єктів, які мають відповідати національним стандартам та пройти затвердження державними органами. Наприклад, ці плани мають включати заходи щодо фізичної безпеки, кібербезпеки, а також оперативного реагування на інциденти; вони повинні оновлюватися та перевірятися на відповідність з урахуванням поточних загроз);

– інформаційного партнерства (приватний сектор зобов'язаний активно співпрацювати з державними органами через обмін інформацією про можливі загрози, вразливості та інциденти на об'єктах критичної інфраструктури; відповідно до положень Постанови Кабінету Міністрів № 943 та Закону України «Про захист інформації в інформаційно-комунікаційних системах», підприємства повинні підтримувати канали зв'язку з державними органами, такими як Держспецзв'язок, і оперативно інформувати про виявлені ризики, щоб забезпечити своєчасне реагування на потенційні загрози, а також сприяти підвищенню загального рівня безпеки критичної інфраструктури.

Таким чином, регуляторні вимоги до приватного сектору забезпечують високий рівень підготовленості, стійкості та взаємодії, що необхідні для ефективного функціонування критичної інфраструктури та її захисту в Україні.

Україна активно співпрацює з Європейським Союзом щодо імплементації стандартів безпеки критичної інфраструктури. Наприклад, директиви ЄС, такі як NIS2 та програма EPCIP, встановлюють високі вимоги до кіберзахисту та управління ризиками, що підвищує ефективність

ДПП.

Директива NIS2 (Директива про мережеву та інформаційну безпеку) є важливою ініціативою Європейського Союзу, яка була прийнята для підвищення рівня кібербезпеки в усіх країнах-членах ЄС. Вона є оновленою версією попередньої директиви NIS і спрямована на адаптацію до нових викликів, пов’язаних із зростанням кіберзагроз.

NIS2 розширює коло організацій, які підпадають під дію директиви, включаючи більше секторів критичної інфраструктури, таких як енергетика, транспорт, охорона здоров’я, цифрові послуги та інші. Документ вимагає від держав-членів забезпечення суворих стандартів кібербезпеки для критичної інфраструктури, що включає впровадження заходів для управління ризиками, обміну інформацією та реагування на інциденти. Організації зобов’язані проводити регулярні оцінки ризиків і вживати заходів для їх зменшення, підвищення обізнаності щодо кіберзагроз і навчання персоналу.

Директива передбачає також створення механізмів для координації зусиль на рівні ЄС, включаючи співпрацю з такими установами, як ENISA (Європейське агентство з кібербезпеки), що має сприяти підтримці кібербезпеки у всіх країнах. NIS2 вводить жорсткі механізми покарання для організацій, які не дотримуються вимог директиви. Це включає штрафи за порушення, що стимулює компанії до впровадження належних заходів безпеки. ЄС вимагає від своїх держав-членів дотримання NIS2, що зобов’язує компанії впроваджувати стандарти кіберзахисту, створення систем раннього попередження, обмін даними про загрози та узгодження спільних протоколів реагування.

Європейська програма захисту критичної інфраструктури (European Programme for Critical Infrastructure Protection, EPCIP) [73] є ініціативою Європейського Союзу, спрямованою на зміцнення захисту критичних інфраструктур у країнах-членах ЄС. EPCIP була започаткована у 2006 році

як комплексна програма для забезпечення стабільності та безпеки основних секторів, таких як енергетика, транспорт, зв'язок, фінансові послуги та інші. Програма зосереджується на кількох основних напрямах, що забезпечують послідовний підхід до захисту критичної інфраструктури на рівні ЄС.

Основними компонентами EPCIP є:

– ідентифікація критичної інфраструктури (EPCIP запроваджує систематичний підхід до визначення та класифікації об'єктів, що вважаються критично важливими для національної та загальноєвропейської безпеки; важливим елементом програми є концепція Європейської критичної інфраструктури (European Critical Infrastructure, ECI), яка визначає ключові об'єкти, від яких залежить нормальне функціонування суспільства);

– національні програми захисту критичної інфраструктури (EPCIP зобов'язує країни-члени ЄС розробляти національні програми захисту критичної інфраструктури, які враховують особливості національних потреб і відображають європейські принципи захисту та передбачають заходи з ідентифікації, оцінки ризиків та забезпечення захисту об'єктів, які мають вирішальне значення для безпеки країни);

– механізми обміну інформацією та співпраця (EPCIP створює платформи для обміну інформацією, як на національному, так і на європейському рівні та передбачає регулярні зустрічі, семінари та симуляції для підвищення обізнаності про ризики та посилення співпраці між країнами ЄС, а також між державним і приватним секторами);

– фінансування та технічна підтримка (Програма EPCIP надає фінансову та технічну підтримку країнам-членам для реалізації заходів із захисту критичної інфраструктури: гранти на дослідження і розробку технологій, підвищення кваліфікації фахівців, а також розробку нових підходів до оцінки ризиків і управління кризовими ситуаціями);

– оцінка ризиків та управління кризами (EPCIP акцентує увагу на

постійному моніторингу та оцінці ризиків, пов’язаних із функціонуванням критичної інфраструктури; програма заохочує країни-члени створювати плани дій на випадок надзвичайних ситуацій та впроваджувати сучасні методи управління ризиками, зокрема через підхід до управління безперервністю бізнесу та запобігання терористичним загрозам.

У Сполучених Штатах, як і в Україні, співпраця державного і приватного сектору в захисті критичної інфраструктури підтримується на законодавчому рівні. Закон США про кібербезпеку 2015 року [74] є важливим етапом у формуванні національної політики кібербезпеки, оскільки він передбачає такі основні аспекти. Закон надає компаніям юридичну можливість ділитися інформацією про кіберінциденти та загрози з урядом і один з одним. Це сприяє кращому розумінню поточних загроз і ефективнішій взаємодії для захисту важливих об’єктів від атак. Закон забезпечує захист конфіденційності та недоторканності особистої інформації, яку компанії надають державі, зберігаючи її конфіденційність відповідно до визначених стандартів і вимог. Департамент внутрішньої безпеки США (Department of Homeland Security, DHS) отримав розширені повноваження для координації міждержавного обміну інформацією та для сприяння захисту критичної інфраструктури. DHS є центральним органом, що обробляє інформацію про кіберзагрози, отриману від приватних компаній, та допомагає у розробці механізмів реагування на кіберзагрози.

Роль DHS у регулюванні ДПП полягає у тому, що він виконує наглядову функцію в рамках державно-приватного партнерства у сфері кібербезпеки. Зокрема, департамент забезпечує: координацію між державними і приватними організаціями для оперативного реагування на кіберзагрози; надання технічної підтримки та рекомендацій для суб’єктів критичної інфраструктури; розробку політик і методологій для оцінки та зменшення ризиків, спираючись на стандарти NIST.

Національний інститут стандартів і технологій (National Institute of

Standards and Technology, NIST) - це федеральне агентство США, яке входить до складу Міністерства торгівлі США. Заснований у 1901 році, NIST займається розробкою та впровадженням стандартів, що сприяють інноваціям і підвищенню продуктивності в різних галузях економіки. Одним із ключових напрямів його роботи є підтримка і вдосконалення стандартів, зокрема в галузі кібербезпеки, метрології, матеріалознавства та технологій. Основними функціями NIST є наступні.

Розробка стандартів і рекомендацій. NIST створює стандарти, такі як NIST Cybersecurity Framework, що застосовується для управління ризиками кібербезпеки, особливо в секторі критичної інфраструктури. Цей рамковий документ використовується державними та приватними організаціями для підвищення рівня захищеності інформаційних систем.

Технологічні дослідження та інновації. NIST займається дослідженнями в галузі метрології, обчислень, квантових технологій та інших наукомістких сфер, сприяючи розвитку національних і міжнародних технологічних стандартів.

Розробка систем захисту критичної інфраструктури - NIST активно співпрацює з іншими агентствами, такими як DHS, з метою розробки рекомендацій для захисту кіберінфраструктури США від сучасних загроз.

NIST також відіграє ключову роль у створенні стандартів, які покращують безпеку і стійкість критичних інфраструктур до нових загроз, таких як кібератаки, та забезпечують підґрунтя для надійної та безпечної інфраструктури в різних галузях економіки.

Таким чином, Закон США про кібербезпеку та Національний інститут стандартів і технологій є ключовими елементами регулювання в галузі кібербезпеки та захисту критичної інфраструктури в Сполучених Штатах. Вони встановлюють стандарти та керівні принципи для приватних і державних організацій, сприяючи управлінню ризиками і зміцненню співпраці між державою та приватним сектором через державно-приватне

партнерство. Департамент внутрішньої безпеки (DHS) виконує загальний нагляд за виконанням цих рекомендацій, координуючи роботу організацій і забезпечуючи підтримку для суб'єктів критичної інфраструктури.

Механізми співпраці та обміну інформацією між державними установами та приватними компаніями є ключовими для своєчасного реагування на кіберзагрози та забезпечення захисту критичної інфраструктури. В Україні механізми обміну інформацією між державою та приватним сектором у сфері захисту критичної інфраструктури лише розвиваються. Як зазначалось вище, ключову роль у цьому процесі відіграє ДССЗЗІ, яка координує взаємодію з об'єктами критичної інфраструктури через Національну систему кібербезпеки.

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які згідно із Конституцією, законами України виконують в установленому відповідні завдання. Основними напрямами співпраці є обмін інформацією про кіберінциденти, моніторинг та попередження кіберзагроз, а також навчання і тренінги з реагування на кіберінциденти. Національна система кібербезпеки України координує обмін інформацією через спеціалізовані центри кіберзахисту та попередження кіберінцидентів. ДССЗЗІ співпрацює з приватним сектором у забезпеченні моніторингу інформаційних систем і обміну оперативною інформацією про загрози. Центр кіберзахисту при ДССЗЗІ розробляє та поширює інформаційні рекомендації з кібербезпеки для державних установ і приватного сектору, а також забезпечує системи попередження про загрози. Інформаційні кампанії і спільні навчання із представниками бізнесу надають змогу українським підприємствам краще підготуватися до можливих загроз і вдосконалити свої плани реагування.

До прикладу, у США співпраця між державними агентствами та приватним сектором у питаннях кібербезпеки є досить розвиненою завдяки встановленим програмам обміну інформацією та численним механізмам взаємодії.

Information Sharing and Analysis Centers (ISACs) [75] - ці центри, створені за ініціативи уряду, забезпечують обмін даними про загрози між компаніями, що належать до критичних секторів, та державними органами. ISACs діють у таких галузях, як фінанси, енергетика, транспорт, охорона здоров'я тощо. Кожен центр ISAC спеціалізується на зборі, аналізі та передачі даних про загрози для конкретної галузі, надаючи актуальні попередження, звіти та технічні консультації.

CISA (Cybersecurity and Infrastructure Security Agency) [76] при Департаменті внутрішньої безпеки (DHS) координує співпрацю між державою і приватним сектором, надає рекомендації та інформацію про кіберзагрози, інциденти та уразливості. CISA також підтримує інформаційний обмін через Програму надання даних для попередження (Information Sharing Program), яка допомагає бізнесу отримувати актуальну інформацію про нові загрози та методи захисту.

Програма Automated Indicator Sharing (AIS) [77]. Ця програма дозволяє організаціям автоматично ділитися інформацією про кіберзагрози в режимі реального часу, допомагаючи швидко ідентифікувати нові загрози і надавати відповідні рекомендації для захисту. AIS забезпечує оперативний зв'язок між приватним сектором і урядовими установами, прискорюючи процес реагування на кіберзагрози.

Україна та США демонструють різні рівні розвитку систем інформаційного обміну, однак обидві країни прагнуть розвивати державно-приватне партнерство як основу для ефективного захисту критичної інфраструктури. Важливими елементами для обох держав є взаємний обмін оперативною інформацією, регулярні навчання і співпраця з міжнародними

організаціями, що сприяє підвищенню рівня безпеки в умовах зростаючих кіберзагроз.

Державне фінансування проектів у сфері безпеки критичної інфраструктури є ключовим інструментом для зміцнення стійкості об’єктів та підвищення кібербезпеки. Основними джерелами фінансування виступають гранти та інноваційні субсидії; субсидії для кіберстійкості; підтримка програм для навчання кадрів; фонди для модернізації та інфраструктурної стійкості; міжнародні фінансові інструменти тощо.

До прикладу, низка країн, як-то США, Великобританія, країни ЄС, надають гранти для досліджень і розробок нових технологій у сфері безпеки. У США, наприклад, Національний інститут стандартів і технологій (NIST) та Агентство з кібербезпеки та безпеки інфраструктури (CISA) фінансують ініціативи, спрямовані на вдосконалення захисту від кібератак. У Європі такі програми фінансуються Європейським Союзом через Horizon Europe, який націлений на інновації в кібербезпеці та технології моніторингу.

Уряди надають субсидії приватним компаніям для вдосконалення систем кібербезпеки, зокрема для секторів критичної інфраструктури. У США діє програма кіберстійкості в рамках CISA, що спрямована на захист енергетичних, комунікаційних і транспортних систем. Європейський Союз також підтримує кіберстійкість через регуляції та надання субсидій у рамках NIS2.

Навчання персоналу і підвищення кваліфікації в сфері кібербезпеки є важливим аспектом державно-приватного партнерства. У США, наприклад, працює CyberCorps: Scholarship for Service [78], програма, що забезпечує студентам можливість навчання та роботи у сфері кібербезпеки в державних установах. В Україні, на додаток до державних програм підготовки кадрів, навчальні програми реалізуються через ДССЗЗІ для підвищення кваліфікації співробітників критичних галузей.

Уряди багатьох країн створюють спеціальні фонди для модернізації фізичної інфраструктури. Такі фонди допомагають модернізувати старі об’єкти та вдосконалювати їхню стійкість до різних загроз. У США діє програма Homeland Security Grant Program (HSGP) [79], яка фінансує проекти в галузі захисту критичної інфраструктури, забезпечуючи зменшення ризиків для ключових об’єктів. У ЄС подібні проекти фінансуються на рівні держав-членів у рамках EPCIP (Європейська програма захисту критичної інфраструктури). Україна залучає підтримку міжнародних організацій, таких як Світовий банк, USAID, та інші агентства, що надають допомогу у зміцненні критичної інфраструктури.

ДПП у сфері захисту критичної інфраструктури є важливим механізмом для зміцнення безпеки держави, адже приватний сектор володіє або управляє значною частиною критичних об’єктів. Однак реалізація такого партнерства стикається з низкою викликів і бар’єрів, що ускладнюють його ефективність і стабільність.

Одним із найсуттєвіших з них є брак довіри між державними органами та приватними компаніями, яка стримує ефективну співпрацю між сторонами та призводить до обмеженого обміну інформацією про можливі загрози та ризики. Ризики кібербезпеки також є значущим бар’єром для ДПП, адже залучення приватних компаній до державних інфраструктурних проектів підвищує уразливість об’єктів через можливий доступ сторонніх суб’єктів. Приватні компанії, відповідальні за різні аспекти критичної інфраструктури, мають різні стандарти захисту та недостатній рівень готовності до протидії кібератакам, що здатне поставити під загрозу державну безпеку в цілому. Нерівномірний розподіл ресурсів і відповідальності між державою і приватним сектором є ще одним фактором, що ускладнює реалізацію ДПП. Державні органи можуть не мати достатніх ресурсів для фінансування всіх необхідних заходів безпеки, і розраховують, що приватні компанії вкладатимуть кошти в кібербезпеку, фізичний захист

та інші аспекти інфраструктури. Однак компанії не завжди є готовими до таких інвестицій або можуть мати інші пріоритети, зокрема, якщо інвестиції в безпеку не приносять безпосереднього прибутку. Конфіденційність та безпека даних є ще одним важливим аспектом, що ускладнює взаємодію. Відповідно до норм конфіденційності, компанії мають обмежений доступ до інформації про стан державної безпеки, що обмежує їхню можливість розробки повноцінних стратегій захисту. З іншого боку, держава також може обмежувати доступ до інформації з міркувань безпеки, що створює бар'єри для співпраці та інформованості про реальні загрози. Вважаємо, що ці бар'єри можна подолати через розробку нормативно-правової бази, яка чітко регламентує обов'язки і права кожної зі сторін, а також через регулярні тренінги та симуляції для відпрацювання сценаріїв реагування на надзвичайні ситуації.

Отже, ДПП відіграє критично важливу роль у забезпеченні безпеки критичної інфраструктури, оскільки ефективний захист від загроз неможливий без тісної співпраці між державними органами та приватними компаніями. Сучасні виклики, такі як тероризм, кіберзагрози та природні катастрофи, вимагають інтегрованого підходу, який забезпечується через обмін інформацією, розробку спільних стандартів безпеки та реагування на надзвичайні ситуації.

Ефективність ДПП в сфері захисту критичної інфраструктури залежить від узгоджених дій усіх учасників, що, у свою чергу, забезпечує не лише національну безпеку, але й стабільність економічної системи в цілому. Розробка і впровадження спільних ініціатив, активне співробітництво в управлінні ризиками та постійний обмін інформацією між державою і приватним сектором є необхідними умовами для подолання сучасних викликів у цій важливій сфері.

Завдання для самоконтролю

1. Визначте поняття критичної інфраструктури та її основні компоненти.
2. Які основні загрози для критичної інфраструктури ви можете виділити?
3. Розкрийте значення захисту критичної інфраструктури для національної безпеки.
4. Поясніть принципи захисту критичної інфраструктури.
5. Які ключові фактори визначають стійкість критичної інфраструктури?
6. Назвіть та проаналізуйте різні класифікації критичної інфраструктури.
7. Які міжнародні стандарти регулюють захист критичної інфраструктури?
8. Проаналізуйте вплив міжнародних стандартів на державну політику у сфері захисту критичної інфраструктури.
9. Які основні етапи розробки національних планів захисту критичної інфраструктури?
10. Охарактеризуйте роль державних органів у захисті критичної інфраструктури.
11. Розгляньте механізми взаємодії між державними та приватними секторами в контексті захисту критичної інфраструктури.
12. Які методи моніторингу критичної інфраструктури ви знаєте?
13. Які технології кібербезпеки використовуються для захисту критичної інфраструктури?
14. Які є ризики для фінансової інфраструктури в умовах глобальних загроз?
15. Як здійснюється оцінка ефективності заходів, спрямованих на захист критичної інфраструктури?
16. Визначте роль громадськості в забезпеченні безпеки критичної інфраструктури.
17. Які приклади успішних практик захисту критичної інфраструктури в інших країнах ви можете навести?
18. Як впливають технологічні інновації на захист критичної інфраструктури?
19. Які законодавчі акти регулюють питання захисту критичної інфраструктури в Україні?
20. Визначте основні цілі державної політики у сфері захисту критичної інфраструктури.
21. Проаналізуйте випадок про порушення безпеки критичної інфраструктури.
22. Яка роль міжнародних організацій у сфері захисту критичної

інфраструктури?

23. Розгляньте фактори, які впливають на прийняття рішень у сфері захисту критичної інфраструктури.

24. Які виклики постають перед державою у забезпеченні захисту критичної інфраструктури?

25. Як здійснюється управління ризиками в сфері захисту критичної інфраструктури?

26. Які є найбільш значущі проблеми у сфері захисту критичної інфраструктури в Україні?

27. Визначте роль державного контролю у захисті критичної інфраструктури.

28. Які є підходи до співпраці між країнами у сфері захисту критичної інфраструктури?

29. Обґрунтуйте необхідність розвитку державної політики у сфері захисту критичної інфраструктури.

30. Які існують методи навчання і підвищення кваліфікації фахівців у сфері захисту критичної інфраструктури?

Теми для самостійних робіт

1. Критична інфраструктура як складова національної безпеки: теоретичний аналіз.
2. Міжнародні стандарти у сфері захисту критичної інфраструктури: досвід та виклики.
3. Правові аспекти захисту критичної інфраструктури в Україні.
4. Роль державного-приватного партнерства в забезпеченні захисту критичної інфраструктури.
5. Сучасні технології в захисті критичної інфраструктури: можливості та загрози.
6. Оцінка ризиків у сфері критичної інфраструктури: методи та підходи.
7. Кейс-стаді: успішні практики захисту критичної інфраструктури в інших країнах.
8. Кібербезпека критичної інфраструктури: проблеми та рішення.
9. Соціальні аспекти захисту критичної інфраструктури: участь громадськості та організацій.
10. Виклики для критичної інфраструктури в умовах глобалізації.
11. Економічні наслідки порушення функціонування критичної інфраструктури.
12. Стратегічний підхід до захисту критичної інфраструктури: теорія та практика.

13. Взаємодія міжнародних організацій у сфері захисту критичної інфраструктури.
14. Інновації у сфері захисту критичної інфраструктури: шляхи впровадження.
15. Порівняльний аналіз законодавчих актів різних країн щодо захисту критичної інфраструктури.
16. Значення освіти та підготовки кадрів у сфері захисту критичної інфраструктури.
17. Роль інформаційних технологій у захисті критичної інфраструктури.
18. Національні плани захисту критичної інфраструктури: стратегія та реалізація.
19. Загрози для критичної інфраструктури: нові виклики та тенденції.
20. Психологічний аспект захисту критичної інфраструктури: вплив на суспільство.

Список рекомендованої літератури

1. Massive investment is needed in sustainable infrastructure to build climate change resilience. https://www.oecd.org/en/about/news/press-releases/2024/04/massive-investment-is-needed-in-sustainable-infrastructure-to-build-climate-change-resilience.html

2. Getting infrastructure right: the OECD framework for better governance. https://blogs.worldbank.org/en/ppps/getting-infrastructure-right-oecd-framework-better-governance

3. Критична інфраструктура. Нормативно-правова база у сфері захисту критичної інфраструктури. https://moz.gov.ua/uk/kritichna-infrastruktura

4. Закон України “Про внесення змін до деяких законодавчих актів України щодо уточнення повноважень суб’єктів забезпечення цивільного захисту, вдосконалення законодавства з питань захисту населення і територій від наслідків надзвичайних ситуацій, організації та проведення евакуації населення, забезпечення охорони життя та здоров’я громадян”;

5. Закон України “Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку”

6. Постанова Кабінету Міністрів України від 19.01.2024 № 50 “Про внесення зміни до пункту 2 переліку суб’єктів господарювання, галузей та окремих територій, які підлягають постійному та обов’язковому аварійно-рятувальному обслуговуванню на договірній основі”;

7. Постанова Кабінету Міністрів України від 23.01.2024 № 70 “Про затвердження Порядку організації та здійснення контролю виконання органами державної влади та органами місцевого самоврядування вимог законодавства у сфері цивільного захисту”;

8. Постанова Кабінету Міністрів України від 08.03.2024 № 270 “Про внесення змін до Положення про єдину державну систему цивільного захисту і Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв’язку у сфері цивільного захисту”;

9. Постанова Кабінету Міністрів України від 29.03.2024 № 355 “Деякі питання функціонування загальнодержавної автоматизованої системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій”;

10. Постанова Кабінету Міністрів України від 10.05.2024 № 535 “Деякі питання Державної служби з надзвичайних ситуацій”;

11. Постанова Кабінету Міністрів України від 07 червня 2024 р. № 740 “Деякі питання щодо створення, забезпечення функціонування та ведення реєстру територій, забруднених/імовірно забруднених вибухонебезпечними предметами”;

12. Розпорядження Кабінету Міністрів України від 16.02.2024 № 137-р “Про затвердження плану пріоритетних дій Уряду на 2024 рік”;

13. Розпорядження Кабінету Міністрів України від 01.03.2024 № 186-

р “Про подання до Верховної Ради України проекту Закону України “Про денонсацію Угоди між Урядом України і Урядом Російської Федерації про співробітництво в галузі попередження промислових аварій, катастроф, стихійних лих та ліквідації їхніх наслідків”;

14. Розпорядження Кабінету Міністрів України від 08.03.2024 № 215-р “Про подання до Верховної Ради України проекту Закону України “Про вихід з Угоди про поставки товарів для забезпечення національних гідрометеорологічних служб держав — учасниць Співдружності Незалежних Держав”;

15. Розпорядження Кабінету Міністрів України від 15.03.2024 № 237-р “Про подання до Верховної Ради України проекту Закону України “Про денонсацію Угоди між Кабінетом Міністрів України та Урядом Республіки Білорусь про співробітництво в галузі попередження надзвичайних ситуацій та ліквідації їх наслідків”;

16. Наказ Міністерства внутрішніх справ України від 10.01.2024 № 18 «Про внесення змін до Вимог щодо утримання та експлуатації захисних споруд цивільного захисту», зареєстрований у Міністерстві юстиції України 12 січня 2024 р. за № 66/41411;

17. Наказ Міністерства внутрішніх справ України від 15.01.2024 № 28 «Про внесення змін до Переліку закладів охорони здоров’я сфери управління Державної служби України з надзвичайних ситуацій», зареєстрований у Міністерстві юстиції України 29 січня 2024 р. за № 145/41490 ;

18. Наказ Міністерства внутрішніх справ України від 05.03.2024 № 137 «Про затвердження Методики визначення номенклатури та обсягів матеріальних резервів для запобігання виникненню надзвичайних ситуацій і ліквідації їх наслідків» , зареєстрований у Міністерстві юстиції України 03 квітня 2024 р. за № 484/41829;

19. Наказ Міністерства внутрішніх справ України від 18.04.2024 №

251 «Про затвердження Змін до Статуту дій у надзвичайних ситуаціях органів управління та підрозділів Оперативно-рятувальної служби цивільного захисту та Статуту дій органів управління та підрозділів Оперативно-рятувальної служби цивільного захисту під час гасіння пожеж», зареєстрований у Міністерстві юстиції України 25 квітня 2024 р. за № 602/41947

20. Розпорядження КМУ від 19 вересня 2023 р. № 825-р Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури. https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text

21. Постанова КМУ від 28 квітня 2023 р. № 415 Про затвердження Порядку ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього. https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text

22. Постанова КМУ від 9 жовтня 2020 р. № 1109 Деякі питання об’єктів критичної інфраструктури. https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

23. Постанова КМУ від 16 січня 2024 р. № 48 Про внесення змін до постанови Кабінету Міністрів України від 9 жовтня 2020 р. № 1109. https://zakon.rada.gov.ua/laws/show/48-2024-%D0%BF#Text

РОЗДІЛ 2
ПРАКТИЧНІ ПІДХОДИ ТА ТЕХНОЛОГІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ГЛАВА 4. Методи та технології захисту критичної інфраструктури

4.1. Системи моніторингу та контролю

У сучасних умовах забезпечення захисту критичної інфраструктури значною мірою залежить від ефективності систем моніторингу та контролю, які дозволяють своєчасно ідентифікувати, реагувати та запобігати потенційним загрозам. Системи моніторингу виконують важливу функцію безперервного відстеження показників безпеки, допомагаючи виявляти аномалії, оцінювати ризики та відстежувати стан критично важливих об’єктів у реальному часі. Ефективні системи контролю забезпечують керування всіма процесами, пов’язаними з безпекою, а також дають змогу інтегрувати новітні технології, зокрема штучний інтелект і великі дані, для підвищення точності і швидкості реагування.

Використання систем моніторингу та контролю є ключовим елементом у стратегіях управління ризиками для об’єктів критичної інфраструктури, забезпечуючи надійний бар’єр для протидії фізичним загрозам, кіберінцидентам тощо.

Системи моніторингу та контролю є центральним елементом в управлінні безпекою критичної інфраструктури, дозволяючи оперативно виявляти та реагувати на потенційні загрози. Головне призначення таких систем полягає в забезпеченні надійного захисту, запобіганні інцидентам і гарантуванні безперервності функціонування ключових об’єктів. Головна мета систем моніторингу полягає у своєчасному виявленні загроз, які можуть порушити роботу критичної інфраструктури, зокрема

кіберінцидентів, фізичних загроз чи технічних збоїв. Завдяки безперервному аналізу даних системи ідентифікують аномалії у функціонуванні, що свідчить про можливі проблеми. Для досягнення цього використовуються технології штучного інтелекту та машинного навчання, які дозволяють автоматично аналізувати великі обсяги даних, зібраних із сенсорів та інших джерел, і сигналізувати про потенційні загрози.

Оперативне виявлення потенційних загроз на ранніх стадіях дозволяє запобігати виникненню інцидентів, що можуть призвести до втрати ресурсів, інформації або збоїв у роботі. Системи моніторингу та контролю інтегруються в загальну інфраструктуру безпеки, що дозволяє вживати превентивних заходів ще до того, як проблема переросте в інцидент. Це особливо важливо в секторах, де найменший збій може мати значні наслідки для громадської безпеки або національної економіки.

У разі інциденту системи моніторингу та контролю забезпечують швидку локалізацію проблеми та розробку плану для її вирішення. Оперативність є ключовим фактором у забезпеченні безпеки, оскільки навіть короткочасні збої можуть спричинити масштабні негативні наслідки. Завдяки автоматизації процесів та централізованому управлінню, ці системи надають інформацію для прийняття негайних рішень та розгортання ресурсів для відновлення функціонування інфраструктури.

Системи моніторингу спрямовані на забезпечення безперебійної роботи критичної інфраструктури, що досягається за рахунок своєчасного виявлення і вирішення проблем. Вони підтримують стабільність процесів і сприяють тривалому функціонуванню об’єктів за будь-яких умов. Функції таких систем включають контроль за технічним станом обладнання, дотриманням вимог безпеки та виявленням змін, що можуть вплинути на ефективність операцій. Цілі та функції систем моніторингу та контролю захисту критичної інфраструктури наведені у таблиці 5.

Таблиця 5

Цілі та функції систем моніторингу та контролю захисту критичної інфраструктури

Призначення	Цілі	Функції
Виявлення загроз та аномалій	Своєчасно ідентифікувати потенційні загрози для інфраструктури	Автоматичний аналіз даних, моніторинг роботи систем, виявлення аномалій
Запобігання інцидентам	Запобігати ризикам для об’єктів інфраструктури шляхом превентивних дій	Інтеграція з системами безпеки, аналіз потенційних вразливостей і контроль за параметрами
Оперативна реакція на порушення	Забезпечити швидке реагування на критичні ситуації для мінімізації наслідків	Локалізація проблем, створення планів дій, оперативне інформування відповідальних органів
Підтримка надійності та безперервності роботи	Підтримувати стабільність та довготривалу роботу об’єктів критичної інфраструктури	Контроль технічного стану, моніторинг безпеки обладнання, своєчасне виявлення збоїв

Джерело: складено автором

Таким чином, системи моніторингу та контролю виконують низку важливих завдань у забезпеченні захисту критичної інфраструктури, забезпечуючи раннє виявлення загроз та підтримку безперервності функціонування. Вони є основою для створення надійної та безпечної інфраструктури, яка здатна протистояти сучасним загрозам та забезпечувати стабільність у разі виникнення інцидентів.

Системи моніторингу для захисту критичної інфраструктури охоплюють декілька основних типів [80], кожен з яких виконує специфічні завдання у виявленні та запобіганні загрозам.

Фізичний моніторинг. Ці системи забезпечують безпеку територій і об’єктів через використання технологій відеоспостереження, датчиків руху, теплових камер, біометричних систем доступу та інших засобів фізичного контролю. Камери та сенсори, розміщені по периметру стратегічних об’єктів, дозволяють відстежувати фізичні загрози, такі як проникнення на

територію, несанкціонований доступ, рух людей і транспортних засобів. Завдяки цьому персонал безпеки може оперативно реагувати на підозрілу активність або потенційні загрози на об’єкті.

Кібермоніторинг та інформаційна безпека. Кібермоніторинг спрямований на захист інфраструктури від загроз у кіберпросторі. Ці системи контролюють мережеву активність, використовуючи спеціальні програмні рішення для аналізу трафіку, виявлення аномалій і попередження про можливі кіберзагрози, такі як несанкціонований доступ, спроби злому, вірусні атаки. Системи раннього попередження відстежують потенційні загрози в реальному часі, дозволяючи своєчасно запобігти кіберінцидентам. Вказані технології часто базуються на штучному інтелекті та алгоритмах машинного навчання, що дозволяє системам адаптуватися до нових видів загроз.

Інтегровані системи. Для забезпечення комплексного захисту інфраструктури застосовуються інтегровані системи моніторингу, які поєднують фізичний та кібермоніторинг. Вони дозволяють отримувати централізовану інформацію про стан об’єкта, об’єднуючи дані з камер, датчиків фізичної безпеки, а також інформацію про мережеву активність. Інтеграція фізичних і кіберсистем забезпечує ефективну координацію безпеки, що дозволяє виявляти та реагувати на багатофакторні загрози, включаючи гібридні атаки. Це особливо важливо для об’єктів критичної інфраструктури, де фізичні та кіберзагрози можуть виникати одночасно. Завдяки різноманіттю цих систем моніторингова інфраструктура може бути налаштована відповідно до особливостей і потреб об’єктів, а також до специфічних ризиків, які характерні для кожного з них. Використання інтегрованих систем особливо підвищує ефективність безпеки, дозволяючи реагувати на комплексні загрози в режимі реального часу.

Сучасні технології моніторингу та контролю значно підвищують безпеку критичної інфраструктури, оскільки дозволяють швидко виявляти

та ефективно управляти ризиками. Технологічні рішення та інновації розглянемо детальніше у наступному підрозділі, однак коротко зупинимось на деяких із них.

Одним із центральних компонентів є аналіз великих даних, що допомагає виявляти шаблони та аномалії, які можуть сигналізувати про потенційні загрози. Завдяки аналітиці даних із сенсорів, камер спостереження та інших джерел системи можуть завчасно прогнозувати ризики, оперативно виявляти зміни й відповідно реагувати на них, що значно зменшує час на виявлення загроз.

Наступним компонентом є штучний інтелект (AI) і машинне навчання (ML), які забезпечують автоматизацію процесів моніторингу та підвищують їх ефективність. Ці технології дають системам можливість навчатися на основі отриманих даних, адаптуватися до нових загроз і знижувати кількість хибнопозитивних сигналів. За допомогою AI, системи можуть аналізувати зображення або мережевий трафік для виявлення аномальних дій, які можуть вказувати на фізичні або кіберзагрози, а ML-моделі, які постійно оновлюються, підвищують точність у прогнозуванні атак або збоїв у безпеці.

Інтернет речей (IoT) і смарт-сенсори забезпечують постійний збір даних у реальному часі з різних об’єктів, що дозволяє відслідковувати численні параметри, як-от температура, вібрації, стан обладнання тощо. Це дає можливість оперативно виявляти загрози або поломки, а завдяки підключенню IoT до централізованих панелей моніторингу можна швидко реагувати на будь-які зміни, що виникають в умовах реальної роботи об’єктів критичної інфраструктури.

Завдяки інтеграції цих технологій, сучасні системи моніторингу здатні забезпечити високий рівень безпеки, мінімізуючи ризики для критичних об’єктів та забезпечуючи стабільне їхнє функціонування. Наприклад, фізичні системи безпеки, зокрема камери спостереження та сенсори руху,

можуть працювати разом із системами кібермоніторингу, контролюючи мережеву активність і загрози в цифровому просторі. Завдяки комплексному підходу, коли фізичні та цифрові системи об'єднані в єдину інфраструктуру, можливе ефективніше виявлення загроз, які мають комбінований характер, таких як атаки на об'єкти інфраструктури з одночасним впливом на їхні цифрові мережі.

Для досягнення такого рівня інтеграції важливим є спільне використання даних між системами, що включає забезпечення синхронізації дій між державними та приватними структурами. Спільне використання даних дозволяє створити загальну картину ситуації, швидше ідентифікувати джерела загроз і реагувати на них. У випадку інциденту всі учасники: державні установи, приватні компанії, які володіють інфраструктурними об'єктами, можуть обмінюватися інформацією та координувати свої дії. Нагадаємо, що у США, наприклад, це реалізовано через центри інформаційного обміну та аналізу (ISAC), які створюють умови для координації дій різних суб'єктів та спільного реагування на інциденти.

Інтеграція вимагає узгодження технологій і стандартів, що є суттєвим викликом, адже різні організації використовують різноманітні платформи і програмне забезпечення. Застосування стандартів, таких як NIST Cybersecurity Framework, може значно сприяти узгодженню дій. Для приватних компаній інтеграція державних та приватних систем моніторингу вимагає дотримання вимог безпеки й конфіденційності даних, оскільки необхідно враховувати можливість витоку або зловживання інформацією. Як говорилось у попередньому підрозділі, у цьому контексті роль ДПП стає вирішальною для формування надійної бази обміну даними, адже ДПП дозволяє створити чіткі протоколи і зобов'язання з обох сторін щодо обробки і захисту інформації.

Таким чином, інтеграція систем моніторингу та контролю забезпечує комплексний підхід до захисту критичної інфраструктури, дозволяючи

державним і приватним суб’єктам узгоджено діяти під час кризових ситуацій та обмінюватися критично важливими даними для забезпечення ефективного і оперативного реагування.

4.2. Технологічні рішення та інновації

Захист критичної інфраструктури сьогодні неможливий без використання новітніх технологій, які адаптуються до зростаючих і різноманітних загроз. У сучасному середовищі, де загрози стають складнішими, технологічні рішення є основним інструментом для підвищення безпеки та стійкості важливих об’єктів. Впровадження інноваційних методів, таких як штучний інтелект, інтернет речей (IoT), блокчейн і системи прогнозної аналітики, дозволяє не лише забезпечити моніторинг і швидке реагування, але й передбачити потенційні ризики на основі аналізу великих даних.

Окрім захисту від фізичних і кіберзагроз, сучасні технології сприяють оптимізації ресурсів і зменшенню витрат на обслуговування інфраструктурних систем. Вони відкривають нові можливості для державно-приватного партнерства, сприяючи розвитку комплексних рішень та забезпечуючи інтероперабельність між різними секторами і державами.

Штучний інтелект (ШІ) відіграє важливу роль у захисті критичної інфраструктури завдяки своїй здатності аналізувати великі обсяги даних, виявляти аномалії та прогнозувати потенційні загрози. Ця технологія дозволяє здійснювати ефективний моніторинг, управління ризиками та оперативну реакцію на інциденти.

Однією з основних функцій ШІ в цій сфері є автоматизований аналіз даних. Завдяки алгоритмам машинного навчання системи можуть обробляти інформацію з різних джерел, таких як датчики, камери відеоспостереження та мережевий трафік. Це дозволяє системам виявляти шаблони поведінки,

які можуть свідчити про наявність загроз, таких як кібератаки, технічні збої чи фізичні порушення. Наприклад, технології глибокого навчання можуть бути використані для розпізнавання об’єктів і дій на відеозаписах, що забезпечує швидке реагування на підозрілі активності.

Штучний інтелект також застосовується для розробки систем раннього попередження. Аналізуючи історичні дані та поточні тенденції, ШІ може прогнозувати можливі загрози і попереджати про них операторів. Це дозволяє реалізувати превентивні заходи ще до виникнення інциденту. Наприклад, у сфері енергетики ШІ може допомогти у виявленні аномалій у роботі електричних мереж, що знижує ризики аварій.

Крім того, інтеграція ШІ в системи управління безпекою дозволяє автоматизувати рутинні процеси, такі як моніторинг стану обладнання, звітність і управлінські рішення. Це знижує навантаження на персонал і підвищує загальну ефективність реагування. Наприклад, у разі виявлення загрози система може автоматично ініціювати певні дії, такі як блокування доступу до критично важливих систем або сповіщення відповідних служб.

Важливо також зазначити, що, незважаючи на переваги, впровадження технологій штучного інтелекту в захист критичної інфраструктури стикається з деякими викликами (питання конфіденційності, етики використання даних та необхідність забезпечення безпеки самих систем ШІ від кібератак). Тому розробка відповідних стандартів і протоколів для використання ШІ в цій сфері є критично важливою.

Отже, технології штучного інтелекту надають потужні можливості для покращення захисту критичної інфраструктури, забезпечуючи автоматизований аналіз даних, виявлення загроз, оперативну реакцію на інциденти та підтримку безперервності функціонування об’єктів.

Інтернет Речей (IoT) є однією з інноваційних технологій, що активно використовуються для забезпечення безпеки критичної інфраструктури. Ця

технологія передбачає інтеграцію фізичних пристроїв, датчиків і систем у єдину мережу, що дозволяє їм взаємодіяти, збирати дані та здійснювати обробку інформації в реальному часі. Основні аспекти використання IoT у сфері захисту інфраструктури включають:

– *постійний моніторинг* (IoT-пристрої забезпечують безперервний моніторинг стану об’єктів критичної інфраструктури, таких як електричні мережі, транспортні системи та комунікаційні мережі; датчики відслідковують параметри, такі як температура, вологість, тиск і вібрації, що дозволяє своєчасно виявляти аномалії, які можуть свідчити про потенційні збої чи загрози);

– *аналіз даних у реальному часі* (дані з IoT-пристроїв передаються до центральних систем, де вони підлягають аналізу за допомогою алгоритмів штучного інтелекту та машинного навчання, виявляючи загрози, прогнозуючи можливі інциденти на основі попереднього досвіду); наприклад, у енергетичному секторі IoT-системи можуть передбачати навантаження на мережі, дозволяючи уникати аварійних ситуацій);

– *швидку реакцію на інциденти* (у разі виявлення загрози або збоїв у роботі системи, IoT дозволяє автоматично ініціювати процеси реагування, включати активацію резервних систем, сповіщення відповідних служб чи навіть автоматичне закриття небезпечних зон);

– *забезпечення зв’язку між пристроями* (Інтернет Речей створює мережу взаємозв’язаних пристроїв з можливістю комунікувати один з одним, що забезпечує високий рівень координації між різними елементами інфраструктури, такими як датчики, контрольні панелі та управлінські системи; наприклад, у транспортних системах IoT дозволяє обмінюватися інформацією між автомобілями та інфраструктурою, покращуючи управління трафіком та безпеку);

– *покращення управління ризиками* (завдяки інтеграції IoT у системи управління безпекою, організації здатні ефективніше ідентифікувати,

аналізувати та управляти ризиками, при цьому збір даних з різних джерел формує комплексну картину безпеки, що сприяє прийняттю обґрунтованих рішень і запобіганню інцидентам).

Отже, використання Інтернету Речей у сфері захисту критичної інфраструктури надає нові можливості для моніторингу, аналізу та реагування на загрози. Ця технологія забезпечує не лише ефективність, але й гнучкість у відповіді на виклики, що постають перед сучасними інфраструктурними системами. У поєднанні з іншими технологіями, такими як штучний інтелект і аналітика даних, IoT може значно підвищити загальний рівень безпеки та стійкості критичної інфраструктури.

Блокчейн є дистрибутивною базою даних, що забезпечує збереження інформації у формі блоків (системи розподілених реєстрів), які пов’язані між собою і захищені криптографічними методами. Ця технологія забезпечує незмінність даних, оскільки будь-яке внесення змін до інформації вимагає підтвердження від учасників мережі, що створює високу ступінь безпеки та прозорості, що є критично важливим для захисту інфраструктури. Завдяки своїй архітектурі, блокчейн забезпечує захист від несанкціонованого доступу та модифікацій даних. Відомо, що об’єкти критичної інфраструктури містять досить чутливі дані (наприклад відомості про енергетичні мережі або системи управління транспортом), використання блокчейну дозволяє гарантувати, що інформація залишиться цілісною і доступною лише для уповноважених осіб. Додавання шифрування до даних, що зберігаються в блокчейні, підвищує рівень їх безпеки.

Однією з ключових переваг блокчейн-технології є здатність забезпечувати прозорість операцій. Кожен учасник мережі має доступ до однакових даних, що виключає можливість фальсифікації. Це особливо корисно в контексті фінансових операцій і контрактів, де важливо мати можливість перевірити історію змін і підтвердити автентичність даних.

Блокчейн може бути використаний для управління ризиками в реальному часі, особливо в питаннях моніторингу критичних систем. Використання блокчейну у сфері захисту критичної інфраструктури також сприяє більш тісній співпраці між державними органами, приватними компаніями та міжнародними організаціями.

Однак, незважаючи на численні переваги, впровадження блокчейн-технології не позбавлене викликів. Це включає питання регуляції, стандартизації, а також інтеграції з існуючими системами. Потрібно враховувати, що для ефективної роботи блокчейну необхідні ресурси для підтримки мережі, а також необхідність у високих витратах на енергію та обчислювальні потужності.

Технологія блокчейн має великий потенціал у захисті критичної інфраструктури завдяки своїй здатності забезпечувати безпеку даних, прозорість та ефективність [81]. Його впровадження може стати важливим кроком у боротьбі з кіберзагрозами, підвищуючи загальний рівень захисту критичних об’єктів і систем. У той же час, для успішної інтеграції блокчейн-технології в цю сферу необхідно знайти ефективні рішення для регулювання та стандартизації.

Перехід до використання безпілотних систем, зокрема дронів, відкриває нові можливості для автоматизації моніторингу важкодоступних об’єктів. Оснащені камерами високої роздільної здатності, дрони здатні вести відеонагляд у реальному часі, що дозволяє швидко виявляти підозрілі активності, реагувати на них, аналізуючи пошкодження внаслідок стихійних лих або технічних аварій. Це забезпечує оперативне реагування на виникаючі проблеми та не лише знижує ризики для життя, але й підвищує точність виконання завдань, оскільки роботи та дрони здатні виконувати їх з високою точністю та без помилок.

Проте, впровадження таких інноваційних рішень стикається з численними викликами. По-перше, високі витрати на початкове

впровадження нових технологій, таких як автономні дрони або роботизовані системи, можуть бути суттєвим бар'єром для державних органів та приватних компаній, які мають обмежені бюджети. Окрім фінансових витрат, слід також враховувати оперативні витрати, пов'язані з обслуговуванням та оновленням технологій, які можуть вимагати додаткових ресурсів.

По-друге, інтеграція нових технологій з існуючими системами безпеки може бути ускладнена їх несумісністю. Багато організацій використовують усталені технології, які можуть не підтримувати нові рішення. Це вимагає детального налаштування та адаптації, що потребує часу та зусиль, а також може сповільнити процес впровадження. Крім того, адаптація нових технологій до специфіки критичних об'єктів є ще одним важливим викликом. Кожен об'єкт має свої унікальні характеристики та вимоги до безпеки, що може вимагати індивідуального підходу до впровадження технологій.

Отже, вказані інноваційні технології та рішення мають великий потенціал для підвищення ефективності захисту критичної інфраструктури. Розробка стратегій, що дозволяють подолати ці виклики, є важливим кроком для максимізації переваг від використання сучасних технологій у сфері безпеки.

4.3. Кібербезпека та захист інформації

Сектор критичної інфраструктури в багатьох випадках залишається залежним від застарілих технологій у промисловому та операційному середовищах, що суттєво збільшує потенційні наслідки успішних кібератак. Такі застарілі системи часто не оснащені необхідними функціями безпеки, що є критично важливими для захисту від сучасних кіберзагроз, і спираються на апаратне та програмне забезпечення, яке виробники більше

не підтримують. Це становить серйозну загрозу для суспільства і вимагає термінових ініціатив щодо зміцнення захисту та забезпечення здатності життєво важливих систем протистояти як поточним, так і майбутнім викликам у сфері кібербезпеки.

Тривале використання застарілих технологій ускладнює ефективне забезпечення кібербезпеки та технічного обслуговування, що призводить до зростання операційних ризиків і неефективності. Оскільки системи стають дедалі більш взаємопов'язаними, залежність від критичної інфраструктури зростає, а ймовірні наслідки збоїв, викликаних стихійними лихами, тероризмом чи кіберзагрозами, посилюються.

Взаємопов'язаний характер сучасної критичної інфраструктури означає, що порушення в одному секторі можуть мати каскадний ефект на інші. Ця взаємозалежність значно підвищує потенційний вплив кібератак та вимагає комплексного підходу до захисту критичної інфраструктури. Розуміння взаємозалежностей як всередині, так і між секторами інфраструктури є важливим для підвищення їхньої стійкості. Наприклад, залежність енергетичного сектору від «розумних технологій» ілюструє, як уразливості в одній сфері можуть викликати каскадні збої в інших. Інтеграція інформаційних технологій (IT), операційних технологій (OT) та безпосередньо фізичних об'єктів у енергетичних системах, таких як розумні мережі, підвищує ефективність і швидкість реагування, проте також створює нові вразливості.

Розумні електромережі є прикладом передових систем, що використовують IT та новітні технології для оптимізації виробництва, розподілу та споживання електроенергії. Проте їх цифрова природа робить їх вразливими до кібератак, які можуть призвести до порушень у розподілі енергії, впливаючи на житлові приміщення, а також на промислові операції.

Крім того, ефективність екстрених служб, таких як поліція, пожежна служба та медичні бригади, безпосередньо залежить від надійних мереж

зв’язку та електропостачання. Будь-які збої в енергетичному або комунікаційному секторах можуть перешкоджати роботі цих критично важливих служб, затримуючи час реагування і створюючи загрози для життя громадян.

Кіберзагрози для критичної інфраструктури є різноманітними і можуть походити з різних джерел, включаючи державні суб’єкти, злочинні організації, терористів та інші зловмисні групи. Ці загрози варіюються від складних кібератак, які спрямовані на дестабілізацію основних служб, до спроб викрадення конфіденційної інформації тощо. Наслідки таких атак можуть бути глибокими, потенційно призводячи до значних збоїв у функціонуванні державних послуг, економічної нестабільності та загрози національній безпеці.

Для успішної боротьби з кіберризиками та підвищення стійкості критичної інфраструктури необхідна ретельно продумана та узгоджена стратегія. Ця стратегія повинна включати розробку надійних структур кібербезпеки та методів управління ризиками, які захищатимуть від загроз і зменшуватимуть вплив інцидентів, коли вони виникають. Підприємства та організації повинні все більше орієнтуватися на спільний підхід до кібербезпеки, що включає інтеграцію їх IT, OT та фізичних інфраструктур. Глобальна співпраця та дотримання встановлених норм кібербезпеки відіграють вирішальну роль у цьому процесі. Цьому сприяють всесвітні дискусії про поведінку держав у кіберпросторі, а також регуляторні заходи, такі як вищезгадувана Директива Європейського Союзу NIS2.

Для забезпечення ефективного захисту критичної інфраструктури надзвичайно важливо розвивати культуру постійного контролю за кібербезпекою та впровадження стандартизованих правил у секторах і країнах. Цей підхід сприяє управлінню широкомасштабними наслідками кібератак, які можуть одночасно впливати на кілька секторів. Зростання потужних атак підкреслює необхідність постійного оновлення стратегій і

можливостей, зокрема вдосконалення технологій виявлення, сприяння обміну розвідувальними даними між критичними секторами та дотримання суворих інструкцій і рамок кібербезпеки.

Оскільки залежність суспільства від критичної інфраструктури зростає, посилюється й потреба в надійних заходах безпеки для захисту цих основних служб. Усунення вразливостей, модернізація або захист старіючих систем і сприяння спільному підходу до кібербезпеки дозволить забезпечити стійкість критичної інфраструктури, захищаючи економічну стабільність суспільства, громадське здоров'я та національну безпеку. У світлі цих викликів країни активно виробляють ефективні рішення для зміцнення своєї кіберстійкості, і однією з найважливіших ініціатив у цьому контексті стало оновлення стратегій у сфері операційних технологій.

У серпні 2024 року Агентство кібербезпеки Сінгапуру (CSA) представило оновлений Masterplan OT (Operational Technologies) 2024 [82] на четвертому форумі Сінгапурської групи експертів з кібербезпеки операційних технологій (Operational Technology Cybersecurity Expert Panel - OTCEP). Цей термін охоплює апаратні та програмні системи, які управляють, відстежують і автоматизують фізичні процеси в промислових середовищах, таких як енергетика, водопостачання, транспорт і виробництво. Документ містить національні ініціативи, спрямовані на підвищення технічних навичок і компетенцій у сфері кібербезпеки в секторі операційних технологій. Оновлений план передбачає зміцнення стійкого та безпечного кіберсередовища як для критичної, так і для некритичної інформаційної інфраструктури в умовах зростаючих загроз у сфері кібербезпеки.

Masterplan OT 2024 є стратегічним планом для подальшого зміцнення обороноздатності Сінгапуру, зосереджуючись на поліпшенні обміну інформацією та звітності, підвищенні стійкості кібербезпеки за межами критичної інформаційної інфраструктури, створенні Центру передового

досвіду кібербезпеки ОТ і забезпеченні безпечного розгортання систем ОТ протягом усього їх життєвого циклу.

Важливим аспектом розробки Masterplan 2024 стало співробітництво з екосистемою ОТ, що включає понад 60 організацій: консалтингові та професійні служби, навчальні заклади, власників CII (Critical Information Infrastructure), державні установи, виробників оригінального обладнання, системних інтеграторів та постачальників рішень у сфері кібербезпеки. Цей широкомасштабний підхід сприяє ефективній координації між усіма учасниками процесу.

Під час запуску Masterplan ОТ 2024 14 організацій, що належать до групи OEM-виробників і постачальників рішень для кібербезпеки, зобов'язалися дотримуватися принципів безпеки впродовж усього життєвого циклу управління. Спільні зусилля OEM-виробників, системних інтеграторів і операторів ОТ мають на меті створення кібервідмовостійкості в усій екосистемі.

В оновленому плані CSA зосереджується увага на впровадженні принципів безпеки під час розгортання, щоб захистити весь життєвий цикл систем ОТ. Це охоплює проектування, розгортання та обслуговування, що передбачає участь численних зацікавлених сторін. Як і в попередньому виданні, Masterplan ОТ 2024 висвітлює оновлення в сферах людей, процесів і технологій, які необхідні для покращення стану кібербезпеки в рамках постійних зусиль країни щодо підвищення кіберстійкості секторів, де впроваджуються системи та технології ОТ.

Загальна мета Masterplan ОТ 2024 полягає в приверненні уваги до проблем, з якими стикається спільнота ОТ, та у сприянні об'єднанню зусиль зацікавлених сторін для підвищення кіберстійкості. Також план спрямований на зміцнення партнерства з галуззю та зацікавленими сторонами для реалізації численних ініціатив у сфері кібербезпеки, що дозволить адресувати ключові виклики та нові кіберзагрози у середовищі

ОТ. Отже, Masterplan ОТ 2024 є важливим етапом у підвищенні кібербезпеки Сінгапуру, підкреслюючи необхідність інтеграції зусиль усіх учасників в умовах постійно змінюваного кіберсередовища [82].

Забезпечення кібербезпеки критичної інфраструктури є ключовим чинником, що визначає стійкість суспільства перед сучасними загрозами. Виклики, пов’язані з застарілими технологіями, та зростаюча взаємозалежність секторів інфраструктури створюють нагальну потребу в комплексному підході до кіберзахисту, який включає адаптацію новітніх технологій і вдосконалення методів управління ризиками. Важливість оновлення стратегій, таких як Masterplan ОТ 2024, підкреслює необхідність спільної роботи між різними учасниками екосистеми операційних технологій, що дозволить зменшити вразливості та підвищити загальний рівень захисту. Такі ініціативи сприяють не лише захисту конкретних систем, а й формуванню культури кібербезпеки в усіх секторах економіки, що є критично важливим для забезпечення безпеки критичної інфраструктури в умовах динамічно змінюваного кіберпростору.

ГЛАВА 5. Оцінка ефективності державних заходів захисту критичної інфраструктури

5.1. Методи оцінки ризиків

Оцінка ризиків є важливою складовою управління безпекою та стійкістю критичної інфраструктури. Систематичний підхід до оцінки ризиків дозволяє не лише виявляти потенційні загрози та вразливі місця в інфраструктурних системах, але й забезпечувати своєчасне реагування на можливі негативні події. Ефективна оцінка ризиків вимагає використання чітких методологій, які дозволяють комплексно враховувати всі чинники, що можуть вплинути на безпеку об’єктів та систем.

Одним з ключових етапів процесу оцінки ризиків є визначення та класифікація рівня ризику. Це завдання передбачає аналіз трьох основних компонентів: масштабу потенційної шкоди, рівня загрози та ступеня вразливості системи. Традиційно для цього застосовуються матриці ризиків, які дозволяють візуалізувати взаємозв'язок між цими компонентами та наочно визначати рівень ризику для прийняття управлінських рішень.

Щоб визначити рівень ризику, необхідно оцінити масштаб наслідків (збитків) від негативної події. Категорії пошкоджень можуть включати:

– *нематеріальні збитки* (наслідки проявляються у вигляді моральних, людських або інформаційних втрат);

– *матеріальні збитки* (наслідки полягають у матеріальних (фінансових) втратах певного масштабу.

В запропонованій матриці враховуються три основні чинники ризику: **шкода (Ш)**, **загроза (З)**, і **вразливість (В)**.

У процесі оцінки ризиків критичної інфраструктури визначення ключових чинників ризику є основоположним етапом, що дозволяє правильно оцінити потенційні небезпеки та їхні наслідки. У цьому контексті шкода, загроза та вразливість виступають трьома основними складовими, що дозволяють всебічно оцінити рівень ризику.

Шкода (Ш) являє собою міру можливих негативних наслідків, які можуть виникнути в результаті реалізації загрози. Вона охоплює як матеріальні збитки, так і нематеріальні втрати, такі як моральні, людські або інформаційні втрати. Шкода визначає рівень впливу на систему або об'єкт. Оцінка шкоди дозволяє визначити серйозність наслідків негативної події, та ранжувати за пріоритетами заходи з управління ризиками. Шкода може проявлятися у різних формах, включаючи фізичну (руйнування інфраструктури), фінансову (економічні втрати), соціальну (втрати життів) та інформаційну (втрата конфіденційних даних), що робить її універсальним показником для різних типів загроз.

Загроза (З) визначається як потенційне джерело небезпеки, яке може спричинити негативну подію або ситуацію, що матиме негативні наслідки для критичної інфраструктури. Це можуть бути як природні явища (землетруси, повені), так і антропогенні фактори (тероризм, кіберзагрози). Загроза є безпосереднім тригером, який може активувати вразливість системи та спричинити шкоду. Оцінка загрози дозволяє визначити ймовірність того, що певний негативний сценарій реалізується. Від природних катастроф до цілеспрямованих атак на системи — загрози можуть мати різну природу, і розуміння їх потенціалу є ключовим для оцінки ризиків та розробки захисних заходів.

Вразливість (В) відображає слабкі місця в системі або об’єкті, які можуть бути використані загрозами для спричинення шкоди. Вона включає фізичні слабкості, недоліки в управлінських процесах, або технологічні уразливості, що можуть посилити негативний вплив загрози. Вразливість показує, наскільки система або об’єкт готові протистояти потенційній загрозі. Вона дозволяє оцінити, чи є існуючі заходи безпеки достатніми для захисту від загрози. Зменшення вразливості через посилення захисних заходів - один із основних способів зниження загального рівня ризику. Вразливість є гнучким показником, який можна коригувати шляхом зміцнення системи або впровадження додаткових заходів безпеки.

Ці три чинники тісно взаємопов’язані і взаємодіють між собою в процесі формування рівня ризику. Наприклад, навіть при високій загрозі, низька вразливість системи може суттєво зменшити потенційну шкоду, тоді як велика вразливість при низькій загрозі все одно може призвести до значної шкоди через вразливість до інших факторів. Таким чином, для всебічної оцінки ризиків необхідно одночасно враховувати всі три чинники і розуміти, як вони взаємодіють у конкретних обставинах. Це дозволяє формувати більш точні і релевантні стратегії управління ризиками, забезпечуючи стійкість і безпеку критичної інфраструктури.

Матриця розроблена з урахуванням сучасних підходів до оцінки складних систем та інфраструктурних об’єктів та базується на класифікації шкоди, загроз та вразливості на трьох рівнях: низькому, середньому та високому. Такий підхід дозволяє більш детально враховувати різні сценарії розвитку подій та адаптувати методику до специфічних умов окремих об’єктів критичної інфраструктури (табл. 6).

Таблиця 6

Матриця оцінки ризиків критичної інфраструктури

Шкода/Загроза	**Низька (Н)**	**Середня (С)**	**Висока (В)**
Вразливість			
Низька (Н)	ДР (Дуже низький ризик)	НР (Низький ризик)	НР (Низький ризик)
Середня (С)	НР (Низький ризик)	СР (Середній ризик)	ВР (Високий ризик)
Висока (В)	НР (Низький ризик)	ВР (Високий ризик)	ДВР (Дуже високий ризик)

Джерело: складено автором

Деталізуємо.

Низька шкода (Н): Можливі незначні збитки, які мають мінімальний вплив;

Середня шкода (С): Можливі помірні збитки, що можуть вплинути на частину системи;

Висока шкода (В): Значні збитки, що можуть серйозно вплинути на систему або навіть її зруйнувати;

Низька загроза (Н): Малоймовірна подія, або подія, яка спричинить незначні наслідки;

Середня загроза (С): Імовірність події помірна, наслідки можуть бути відчутними;

Висока загроза (В): Висока ймовірність події, яка може спричинити серйозні наслідки;

Низька вразливість (Н): Система добре захищена, має резервні механізми;

Середня вразливість (С): Система має деякі захисні механізми, але все ще вразлива;

Висока вразливість (В): Система дуже вразлива, мало або зовсім немає захисних механізмів.

Вважаємо, що ця матриця є універсальним інструментом для оцінки

ризиків у різних контекстах, включаючи як фізичні, так і кібернетичні загрози. Її використання дозволяє не тільки оцінити поточний рівень ризику, але й формувати рекомендації щодо заходів, необхідних для зменшення вразливостей та підвищення стійкості критичної інфраструктури до різних загроз.

Захист критичної інфраструктури є комплексним процесом, який вимагає інтеграції організаційних, технічних і людських ресурсів з метою забезпечення стійкості і безпеки критично важливих об’єктів. Система захисту реалізується через різноманітні заходи, що спрямовані на недопущення загроз з негативними наслідками для функціонування об’єктів критичної інфраструктури. Основними завданнями цієї системи є виявлення, запобігання та реагування на різноманітні загрози, які можуть виникнути у разі надзвичайних ситуацій або терористичних актів.

Сучасні системи захисту критичної інфраструктури базуються на використанні різних засобів, які складаються з ключових компонентів. Серед них можна виділити механічні загородження, що забезпечують фізичний захист об’єктів. Окрім того, важливими складовими є системи контролю доступу, охоронної сигналізації та відеоспостереження. Кожен з цих елементів виконує свою функцію, але разом вони формують інтегрований підхід до забезпечення безпеки.

Система фізичного захисту, в свою чергу, є інтегрованою сукупністю реальних елементів, дій та процесів, що організовані у спосіб, який забезпечує безпеку об’єктів критичної інфраструктури у заданий час та просторі. У цьому контексті важливо підкреслити, що система фізичного захисту не є статичною; вона повинна бути адаптивною, щоб відповідати змінним умовам загроз. Вона має функціонувати як синергетична система, де різні компоненти співпрацюють для досягнення спільної мети – забезпечення безпеки.

Серед бажаних функцій системи фізичного захисту можна виділити декілька основних аспектів. По-перше, вона повинна бути здатною відлякувати потенційних зловмисників від здійснення атак на об’єкт. По-друге, система має забезпечувати виявлення порушень, що можуть відбутися в охоронюваних зонах, а також виявлення небезпечних ситуацій, що становлять небезпеку. Ці функції є критично важливими, оскільки вони формують основу для швидкого реагування на загрози.

Однак, реалізація системи захисту не є самоціллю; вона повинна бути спроектована таким чином, щоб максимально ефективно реагувати на конкретні загрози, які можуть вплинути на критичну інфраструктуру. Висока вразливість об’єкта до загроз, таких як тероризм чи природні катастрофи, вимагає більш детального та ретельного підходу до проектування заходів захисту. Взаємозв’язок між рівнем загроз, вразливістю та шкодою, що може бути завдана, є основою для аналізу ризиків, який слугує початковим етапом для проектування системи захисту.

Ефективна система захисту повинна також передбачати адаптацію до нових умов та загроз. При цьому проведення регулярного аналізу ризиків і корекція заходів захисту є необхідними для зниження ймовірності настання небезпечних подій. Наприклад, якщо оцінка ризику вказує на високий рівень загрози, але в той же час вразливість системи є низькою, то ймовірність завдання шкоди знижується. Проте у випадку високої вразливості навіть низький рівень загрози може призвести до значних наслідків, що свідчить про необхідність комплексного підходу до захисту.

На завершення, важливо зазначити, що критична інфраструктура охоплює всі матеріальні об’єкти, ресурси та системи, порушення яких можуть серйозно вплинути на безпеку суспільства. Тому система захисту критичної інфраструктури має бути спроектована так, щоб вона успішно протидіяла загрозам, відповідно до їхнього значення та потенційного впливу.

5.2. Показники ефективності захисту критичної інфраструктури

Ефективність державних заходів із захисту критичної інфраструктури значною мірою визначається здатністю цих заходів забезпечувати безперебійне функціонування об’єктів, знижувати ризики збоїв та протидіяти потенційним загрозам. Однак, оцінка результативності таких заходів вимагає використання чітких показників, які відображають різні аспекти впливу на захищеність інфраструктури. Обгрунтування індикаторів результативності заходів захисту критичної інфраструктури вимагає всебічного розгляду як кількісних, так і якісних показників, які відображають рівень досягнення захисних цілей та їхню ефективність у зниженні ризиків. Індикатори слугують базисом для оцінки і моніторингу діяльності та збереження високих стандартів безпеки, а також допомагають виявити слабкі місця у вже реалізованих заходах захисту.

До кількісних індикаторів результативності можна віднести статистичні дані, що відображають безпосередній вплив захисних заходів на інфраструктуру. До них варто віднести:

– рівень надійності інфраструктури; це може бути виражено як частота відмов у роботі критичних систем, кількість аварій чи збоїв, що мали місце за певний період. Високий рівень надійності свідчить про ефективність захисних заходів і стабільну роботу інфраструктури, що дозволяє уникати негативних наслідків для громадян та економіки;

– індекс доступності критичних об’єктів; цей індекс відображає, наскільки безперервно критичні об’єкти залишаються доступними для використання. Наприклад, у медичних установах або енергетичних об’єктах стабільна доступність може бути виміряна як відсоток часу, коли об’єкт забезпечує послуги без перебоїв;

– кількість інцидентів, пов’язаних із зовнішніми загрозами; вимірювання числа загроз (кіберінцидентів, фізичних атак, саботажів), яких

вдалося уникнути, завдяки заходам захисту, дозволяє оцінити ефективність безпекових політик і програм; зниження кількості таких інцидентів може свідчити про підвищену стійкість до зовнішніх загроз.

Якісні показники забезпечують більш комплексне розуміння результативності заходів, дозволяючи врахувати специфіку впливу захисту на інфраструктуру і зручність реалізованих заходів. Вони включають:

– рівень задоволеності користувачів інфраструктури; відгуки користувачів або внутрішніх структурних підрозділів можуть відображати ступінь задоволення захистом об’єктів і впровадженими заходами безпеки; цей показник є особливо важливим у випадку критичної інфраструктури, яка безпосередньо обслуговує громадські інтереси;

– стійкість до зовнішніх загроз; цей показник визначає рівень адаптивності інфраструктури до нових, постійно змінних загроз; якщо кіберсистема має здатність автоматично виявляти і блокувати нові види атак, це підвищує її загальну стійкість і готовність до змін;

– відповідність міжнародним стандартам безпеки; впровадження та дотримання міжнародних стандартів (наприклад, ISO 27001 для інформаційної безпеки або ISO 22301 для безпеки бізнес-процесів) [24; 25] свідчить про високий рівень захисту інфраструктури та може бути критерієм якості захисних заходів.

Синтетичні індикатори являють собою комплексні показники, що поєднують декілька аспектів оцінки одночасно, надаючи ширшу картину результативності захисних заходів:

– інтегральний показник стійкості інфраструктури; цей показник враховує одночасно надійність, доступність і стійкість об’єктів до різних типів загроз, що дозволяє отримати більш узагальнену оцінку ефективності заходів захисту;

– індекс відновлюваності інфраструктури; відображає здатність об’єктів до швидкого повернення до нормальної роботи після інцидентів.

Таблиця 7

Показники ефективності захисту критичної інфраструктури

Тип показника	Показник	Характеристика
Кількісні показники	Рівень надійності інфраструктури	частота відмов у роботі критичних систем, кількість аварій або збоїв за певний період; високий рівень надійності свідчить про ефективність захисних заходів
	Індекс доступності критичних об'єктів	відсоток часу, коли критичні об'єкти залишаються доступними для використання, наприклад, у медичних установах або енергетичних об'єктах
	Кількість інцидентів, пов'язаних із зовнішніми загрозами	вимірювання числа загроз, яких вдалося уникнути завдяки заходам захисту; зниження кількості інцидентів може свідчити про підвищену стійкість до загроз
Якісні показники	Рівень задоволеності користувачів інфраструктури	відгуки користувачів щодо захисту об'єктів і впроваджених заходів безпеки; важливий для критичної інфраструктури, яка обслуговує громадські інтереси
	Стійкість до зовнішніх загроз	рівень адаптивності інфраструктури до нових загроз; здатність кіберсистем автоматично виявляти та блокувати нові атаки підвищує стійкість
	Відповідність міжнародним стандартам безпеки	дотримання міжнародних стандартів (iso 27001, iso 22301) свідчить про високий рівень захисту інфраструктури
Синтетичні показники	Інтегральний показник стійкості інфраструктури	враховує надійність, доступність і стійкість до різних типів загроз, надаючи узагальнену оцінку ефективності заходів захисту
	Індекс відновлюваності інфраструктури	відображає здатність об'єктів до швидкого повернення до нормальної роботи після інцидентів

Джерело: складено автором

Таким чином, показники ефективності захисту критичної інфраструктури надають можливість системно оцінити, наскільки вдало реалізовані заходи сприяють підвищенню безпеки. Оптимальне поєднання кількісних та якісних показників дає змогу як врахувати конкретні ефекти заходів, так і розуміти їх загальне значення для стабільності та функціонування критично важливих об'єктів.

Оцінка ефективності державних заходів із захисту критичної інфраструктури є комплексним завданням, що вимагає багаторівневого підходу, зокрема, виокремлення рівнів безпеки для точнішого аналізу відповідності заходів певному рівню ризиків та їх реальної результативності. Виділення рівнів безпеки – наприклад, низького, середнього та високого – дозволяє структурувати систему захисту відповідно до конкретних ризиків, характерних для кожного рівня. Це сприяє створенню більш адаптивних стратегій захисту, які можуть бути змінені та оптимізовані на основі ситуаційних потреб і умов.

Рівні безпеки можна визначити як стратегічні показники загальної захищеності, що вказують на ступінь ризику і необхідний рівень реакції держави та відповідних структур. Розглянемо більш детально кожен з цих рівнів.

Низький рівень безпеки характеризується ситуаціями, коли ризики виникнення зовнішніх або внутрішніх загроз для критичної інфраструктури є мінімальними, що не потребує особливо складних та ресурсомістких заходів захисту. Для оцінки ефективності на цьому рівні доцільно використовувати мінімальні показники, такі як:

– частота інцидентів невеликої критичності, що легко контролюються і не призводять до значних втрат або порушень роботи інфраструктури;

– ступінь відновлення у разі виникнення загроз, який зазвичай повинен бути досить високим при низькому рівні безпеки;

– наявність базових політик захисту, які легко коригуються, але виконують необхідні превентивні функції, щоб уникнути посилення загроз.

Середній рівень безпеки відображає ситуації, за яких об’єкти критичної інфраструктури піддаються ризикам помірної складності, імовірність яких є вищою, ніж при низькому рівні, проте контрольованою. Тут вимоги до ефективності заходів захисту значно підвищуються,

з’являється необхідність у використанні комбінованих методів і процедур. Основні показники, що можуть застосовуватися для оцінки результативності на середньому рівні, включають:

– частота та ступінь впливу загроз середньої критичності, а також здатність системи швидко реагувати та нейтралізувати такі загрози;

– доступність резервних ресурсів та розподіл функцій серед підрозділів з безпеки, що дозволяє оперативно ліквідовувати наслідки інцидентів;

– наявність адаптованих стратегій резервування, таких як використання дублюючих мереж або ресурсів, що дозволяють стабільно функціонувати навіть під час певних збоїв чи атак.

Високий рівень безпеки – це рівень, який активується у випадках значних ризиків, коли критична інфраструктура може бути серйозно вражена, що потенційно загрожує національній безпеці, здоров’ю населення або економічній стабільності. На цьому рівні система захисту повинна бути здатна оперативно відповідати на загрози, що вимагає застосування високоефективних технологій і процедур. Основні показники ефективності для цього рівня включають:

– мінімізація кількості інцидентів високої критичності або їх повна відсутність, що свідчить про дієвість заходів високого рівня захисту;

– швидкість відновлення систем після надзвичайних подій або серйозних атак, що залежить від доступності резервних потужностей та швидкості реагування кризових служб;

– відповідність міжнародним та національним стандартам безпеки на найвищому рівні, що забезпечує готовність до комплексних загроз;

– показники інтеграції кіберзахисту з фізичними системами захисту об’єктів, що дозволяє реагувати на змішані загрози (наприклад, кібератаки, що можуть впливати на фізичні ресурси) (табл. 8).

Таблиця 8

Класифікація ефективності захисту критичної інфраструктури
за рівнями безпеки

Рівень безпеки	Характеристика рівня	Основні показники ефективності заходів
Низький рівень	низький ризик загроз для критичної інфраструктури, мінімальні заходи безпеки; потрібні базові захисні політики для попередження загроз	частота інцидентів невеликої критичності; ступінь відновлення після загроз – високий рівень повернення до нормальної роботи; наявність базових політик захисту, які легко коригуються та виконують превентивні функції
Середній рівень	помірний ризик загроз для критичних об’єктів, які можуть призвести до збоїв роботи; необхідність у комбінованих методах захисту та використанні резервних ресурсів	частота та ступінь впливу загроз середньої критичності; доступність резервних ресурсів для забезпечення безперебійної роботи; наявність стратегій резервування (дублюючі мережі/ресурси)
Високий рівень	високий ризик, загроза національній безпеці або стабільності; вимагає комплексних, інтенсивних заходів із забезпечення швидкої реакції та відновлення	мінімізація кількості інцидентів високої критичності; швидкість відновлення після серйозних атак завдяки кризовим службам; відповідність міжнародним та національним стандартам безпеки; показники інтеграції кіберзахисту із фізичними системами захисту, що дозволяє реагувати на змішані загрози

Джерело: складено автором

Застосування рівнів безпеки та відповідних їм ключових показників дозволяє не лише оцінювати ефективність державних заходів, але й створює базу для впровадження динамічної системи, яка може адаптуватися до змін у середовищі безпеки. Зокрема, розподіл ресурсів та визначення пріоритетів відповідно до рівня загроз забезпечують раціональне використання державних ресурсів, знижують витрати та підвищують гнучкість захисної інфраструктури.

Класифікація ефективності захисту за рівнями (низький, середній, високий) дає можливість детально оцінити, наскільки державні заходи відповідають вимогам безпеки для конкретних умов та інфраструктурних об’єктів, які мають різний ступінь вразливості.

Завдяки такій структурованій оцінці можна встановити, які конкретні індикатори слід застосовувати для кожного рівня безпеки та які заходи є найбільш релевантними для забезпечення ефективного функціонування критичної інфраструктури. Це також дозволяє визначити напрями для вдосконалення поточних заходів та ресурси, необхідні для підтримання належного рівня захисту в умовах постійного зростання складності загроз.

Коефіцієнт зниження ризиків є важливим індикатором, що відображає ефективність державних заходів із захисту критичної інфраструктури. Цей показник розраховується як відношення кількості загроз, які вдалося уникнути, до загальної кількості ризикових ситуацій за певний період. Він не лише дозволяє зрозуміти, наскільки ефективно функціонують заходи безпеки, але й дає змогу оцінити реальний стан захищеності критичних об’єктів.

Коефіцієнт зниження ризиків (К) можна представити формулою:

$$К = \frac{N_{успіх}}{N_{ризики}}$$

$N_{успіх}$ - *кількість успішно нейтралізованих загроз,*

$N_{ризики}$ - *загальна кількість ризикових ситуацій.*

Високий коефіцієнт (близький до 1) свідчить про те, що заходи захисту є ефективними, і велика частина загроз успішно нейтралізується. Це може бути результатом чіткої стратегії безпеки, належного фінансування, навчання персоналу та модернізації технологій.

Низький коефіцієнт (менше 0,5) вказує на те, що існує значний розрив між потенційними загрозами та можливостями їх нейтралізації. У цьому випадку необхідним є перегляд існуючих стратегій безпеки, їх адаптація до нових загроз або збільшення інвестицій у технології та навчання.

Коефіцієнт зниження ризиків слугує основою для прийняття управлінських рішень у сфері безпеки. Регулярний моніторинг коефіцієнта зниження ризиків є важливим елементом звітності для державних установ, які відповідають за забезпечення безпеки критичної інфраструктури. Публікація таких даних підвищує прозорість і довіру суспільства до державних заходів у цій сфері. Отже, коефіцієнт зниження ризиків є універсальним індикатором, що дозволяє оцінити ефективність заходів захисту критичної інфраструктури.

5.3. Коригувальні заходи щодо вдосконалення

На основі показників ефективності видається необхідним визначення, які саме компоненти системи захисту є найслабшими або малоефективними, що передбачає аналіз невідповідності в інфраструктурі, технологічній оснащеності та в управлінських підходах. Основним підходом у цьому процесі є глибокий аналіз ефективності окремих компонентів системи на основі ключових показників. Ось детальні етапи для успішного виявлення недоліків:

Аналіз показників ефективності. Щоб виявити недоліки в системі, спочатку потрібно дослідити основні показники її роботи, такі як час реагування на інциденти, кількість загроз, що було виявлено або пропущено, а також ефективність роботи обладнання та інформаційних систем. Використання таких індикаторів дає змогу точно ідентифікувати компоненти, що потребують вдосконалення.

Аудит інфраструктури та технологічного забезпечення. Щоб виявити технологічні та інфраструктурні прогалини, проводяться регулярні аудити та технічні перевірки. Під час цього процесу важливо оцінити, чи відповідає інфраструктура сучасним вимогам та стандартам. Якщо виявляються застарілі або неповноцінні технологічні рішення, це може вказувати на необхідність оновлення обладнання чи впровадження нових технологій для забезпечення більшої безпеки.

Оцінка управлінських підходів. Важливим аспектом вдосконалення є аналіз управлінських методів, що використовуються для координації захисних заходів. Недоліки в управлінні, такі як неефективна координація між відділами або недостатнє навчання персоналу, можуть призводити до прогалин у системі захисту. Регулярна оцінка управлінських процесів дозволяє зрозуміти, які підходи потребують оптимізації або навіть повної реорганізації.

Виявлення невідповідностей у нормативно-правовій базі. У разі зміни законодавства або стандартів безпеки необхідно переглядати відповідність системи захисту цим нововведенням. Якщо виявляються невідповідності, це сигналізує про необхідність оновлення процедур або впровадження додаткових заходів відповідно до нових вимог.

Використання симуляційних тестів та навчань. Проведення регулярних симуляцій допомагає виявити недоліки в оперативному реагуванні на інциденти та перевірити ефективність існуючих заходів. Такі навчання дозволяють випробувати систему в умовах, максимально наближених до реальних загроз, та визначити слабкі місця, що можуть залишитися непоміченими під час звичайних перевірок.

Загалом, виявлення недоліків в існуючій системі захисту є комплексним процесом, який охоплює аналіз технічних, інфраструктурних та управлінських аспектів, а також постійне оновлення системи відповідно до нових загроз і вимог. Це є ключовим елементом для забезпечення її

ефективності, гнучкості та здатності швидко адаптуватися до нових викликів.

Для розуміння та підвищення ефективності захисту критичної інфраструктури необхідно глибше оцінити наявні сильні та слабкі сторони, а також розглянути зовнішні фактори, які впливають на систему захисту. З цією метою доцільно застосувати SWOT-аналіз, який дозволить виявити як внутрішні можливості для вдосконалення системи, так і потенційні загрози, з якими можуть стикнутися державні та приватні структури у процесі захисту критичних об’єктів.

SWOT-аналіз допомагає ідентифікувати ключові компоненти поточної системи безпеки та виявити аспекти, які потребують коригувальних заходів або додаткових інвестицій. Дослідження сильних сторін дозволяє зрозуміти, які ресурси та технології вже працюють на високому рівні, а аналіз слабких місць підказує, де може знадобитися модернізація або реорганізація. Оцінка можливостей вказує на потенційні напрями розвитку, аналіз загроз допомагає підготуватися до зовнішніх ризиків, включаючи кіберзагрози, новітні типи атак, економічні виклики та інші фактори, що можуть вплинути на стабільність та безперервність функціонування критичної інфраструктури.

Сильні сторони системи захисту критичної інфраструктури включають її здатність швидко виявляти загрози завдяки застосуванню сучасних технологій, таких як штучний інтелект і аналітика великих даних. Ці системи забезпечують комплексний підхід, оскільки поєднують фізичний і кібермоніторинг. Важливу роль відіграє регулярна підготовка персоналу до надзвичайних ситуацій, що значно покращує оперативність реагування.

Слабкі сторони пов’язані з наявністю застарілих технологій та недостатньою координацією між різними організаціями, що може уповільнити прийняття рішень. Також існує ризик фінансових обмежень, які впливають на можливість оновлення технологій, а нормативна база зазвичай

повільно удосконалюється у порівнянні із новими технологічними змінами, що обмежує інтеграцію інноваційних рішень.

Можливості для вдосконалення системи захисту включають впровадження новітніх технологій, таких як IoT та блокчейн, які можуть покращити моніторинг та прозорість даних. Розширення державно-приватного партнерства сприяє кращому розподілу ресурсів та обміну технологіями, що є корисним для підвищення загальної стійкості інфраструктури. Також міжнародна співпраця відкриває нові можливості для обміну досвідом і впровадження кращих практик.

Загрози включають зростання кількості та складності кіберзагроз, які можуть перевищити поточні можливості системи. Фінансова нестабільність та економічні обмеження також негативно впливають на підтримку та розвиток інфраструктури. З огляду на швидкий розвиток нових видів загроз, як-от гібридні атаки, є ризик недостатньої адаптації системи до нових викликів (табл. 9).

Вказаний SWOT-аналіз підкреслює важливість балансу між підтримкою технологічного розвитку та організаційним підходом для ефективного захисту критичної інфраструктури, обумовлює комплексне розуміння поточної ефективності системи захисту критичної інфраструктури та є основою для подальшого планування та впровадження коригувальних заходів. Для посилення захисту критичної інфраструктури необхідно здійснити низку коригувальних заходів, які охоплюють три ключові аспекти: пропозиції з посилення захисту, розробка стратегії адаптації до змінних загроз, а також перегляд нормативних стандартів і процедур.

Таблиця 9

SWOT-аналіз ключових компонентів поточної системи безпеки критичної інфраструктури

Сильні сторони (Strengths)	**Слабкі сторони (Weaknesses)**
Висока швидкість виявлення загроз завдяки використанню сучасних технологій, таких як штучний інтелект і машинне навчання	Наявність застарілого обладнання або технологій, які не відповідають сучасним вимогам безпеки
Інтеграція кібер- та фізичного моніторингу, що забезпечує комплексний захист інфраструктури	Недоліки в координації між різними державними і приватними організаціями, що може уповільнити реагування на загрози
Використання великих даних для прогнозування ризиків і аналізу аномалій, що підвищує точність оцінки загроз	Відсутність достатніх фінансових ресурсів для оновлення інфраструктури і технологій захисту
Регулярні навчання та симуляційні тренінги для персоналу, що підвищують їх готовність до надзвичайних ситуацій	Невідповідність законодавчих вимог новітнім технологіям, що ускладнює їх інтеграцію
Можливості (Opportunities)	**Загрози (Threats)**
Впровадження нових технологій, таких як Інтернет речей (IoT) та блокчейн для підвищення надійності та безпеки системи	Зростання складності та частоти кіберзагроз, що може перевищити поточні можливості системи
Збільшення державно-приватного партнерства, що забезпечує обмін ресурсами і технологіями між державою і бізнесом	Економічна нестабільність, яка може вплинути на виділення коштів для підтримки інфраструктури
Підвищення рівня міжнародної співпраці, що дозволяє обмінюватися найкращими практиками та досвідом у сфері захисту інфраструктури	Поява нових видів загроз, таких як гібридні атаки, які вимагають швидкої адаптації та нових технологій

Джерело: складено автором

Перш за все, обґрунтування змін у захисних заходах має включати широкий спектр рекомендацій, зокрема необхідності посилення фізичного захисту, що передбачає оновлення або підвищення ефективності систем контролю доступу, встановлення більш надійних бар’єрів, а також використання сучасних технологій, таких як сенсори, відеонагляд і засоби контролю територій. Ключовим є також модернізація технічних систем, кіберзахисту, що передбачатиме інтеграцію сучасних рішень для виявлення

загроз, штучного інтелекту для аналізу великих обсягів даних і засобів запобігання кіберінцидентам. Важливим елементом цього процесу є вдосконалення процедурного захисту, яке включає оновлення правил і політик безпеки та забезпечення чіткого алгоритму дій під час потенційних загроз, покращення комунікаційних протоколів тощо.

З огляду на постійно змінюваний характер сучасних загроз, важливо також розробити стратегію адаптації до нових викликів та впровадити динамічні методи управління, які дозволяють системі швидко змінювати та оновлювати способи захисту. Застосування проактивних технологій стане в нагоді для прогнозування та оцінки потенційних загроз, а також для розробки планів для швидкого відновлення після інцидентів. Регулярний перегляд і тестування системи є критично важливими для визначення її здатності адаптуватися до змін. У цьому зв’язку використання аналізу ризиків, моніторинг інцидентів у реальному часі та проведення регулярних тренінгів сприятимуть створенню динамічної системи, яка відповідатиме сучасним вимогам безпеки.

Також важливим аспектом є перегляд нормативних стандартів і процедур, що є важливою складовою коригувальних заходів, спрямованих на вдосконалення захисту критичної інфраструктури. У світі, де загрози та технології постійно еволюціонують, регуляторна база повинна бути актуальною та відповідати поточним потребам. Це передбачає внесення змін до існуючих стандартів і створення нових інструкцій, які регулюють питання фізичної та кібербезпеки. Важливо також привести нормативи у відповідність до вимог міжнародних стандартів, таких як ISO або NIST, що забезпечить інтеграцію найкращих світових практик у національну систему безпеки.

Таким чином, здійснення цих коригувальних заходів допоможе не покращити захист критичної інфраструктури та забезпечити її стабільність та стійкість у довгостроковій перспективі.

ГЛАВА 6. Кращі практики захисту критичної інфраструктури

6.1. Аналіз успішних кейсів з різних країн

Європейський досвід у сфері ідентифікації та захисту секторів і об’єктів критичної інфраструктури є багатогранним і базується на різноманітних національних підходах, адаптованих до унікальних умов і потреб кожної країни. Наприклад, у Швеції система ідентифікації критичної інфраструктури отримала назву Vital Societal Functions, що охоплює рівні місцевого, регіонального та національного управління. Шведська модель використовує підхід «всі ризики/небезпеки», зосереджуючись переважно на управлінні кризами та стихійними лихами. Політичні та військові загрози не є основним фокусом, що дозволяє забезпечувати максимальну стійкість суспільства до різних типів ризиків і стихійних лих, таких як пожежі або повені [83]. У Фінляндії, навпаки, великий акцент зроблено на регіональних ініціативах, які беруть на себе значну частину відповідальності за аналіз ризиків. Тут пріоритетом є безпека енергетичних систем, тоді як загрози для громадського здоров’я розглядаються як другорядні, але також важливі [84].

У Нідерландах підхід до захисту критичної інфраструктури також будується навколо концепції «всі ризики/небезпеки», але з урахуванням географічних особливостей країни, яка знаходиться нижче рівня моря і постійно стикається з загрозами повеней. Тут оцінка загроз здійснюється на національному та регіональному рівнях, що дозволяє швидко реагувати на надзвичайні ситуації та залучати необхідні ресурси [86]. Це свідчить про прагнення Нідерландів залучити приватний сектор для забезпечення стійкості інфраструктури, хоча чітке визначення ролей і обов’язків ще потребує деталізації.

У країнах Південно-Східної Європи, які розташовані в регіоні Балканського півострова, а саме: Болгарія, Румунія, Сербія, Чорногорія, Північна Македонія, Албанія, Боснія і Герцеговина, Хорватія, а також

частково Греція, обізнаність про підхід «всі ризики/небезпеки» залишається на низькому рівні, особливо в приватному секторі, що ускладнює створення ефективних державно-приватних партнерств. В цих країнах модель управління критичною інфраструктурою, зокрема вказаний підхід, перебуває на етапі розвитку та адаптації, однак його впровадження ускладнюється обмеженими ресурсами [87], різною мірою розвитку приватного сектору в безпековій галузі, а також відносно невеликою часткою приватизації безпекових послуг.

Ключовими викликами для Південно-Східної Європи залишаються проблеми з адаптацією до сучасних стандартів безпеки та недосконаліть законодавчої бази. Почасти державно-приватна співпраця ускладнена недовірою між приватними операторами та урядовими структурами, а також різними підходами до оцінки ризиків і управління ними [88]. Це особливо актуально для Болгарії, Румунії та Сербії, де приватний сектор інколи не готовий прийняти на себе повноцінні зобов'язання у сфері кібербезпеки.

Суттєві проблеми також виникають у процесі публічних закупівель. Аутсорсинг приватних охоронних компаній може зменшити витрати на корпоративну безпеку, але вибір постачальника на основі найнижчої ціни часто веде до нових труднощів. У багатьох важливих компаніях, зокрема в енергетичному секторі, корпоративна безпека не займає належного місця в організаційній структурі та не вважається пріоритетом для вищого керівництва, що знижує її значення в процесах прийняття рішень.

В управлінні ризиками КІ державно-приватне партнерство може стикатися з додатковими перешкодами, оскільки приватні власники та оператори часто мають різне сприйняття загроз і пріоритети. Держава повинна визначити так званий «скелет базових загроз», за які відповідатимуть оператори КІ. У випадку складних загроз мають бути задіяні державні інституції. Держава також може розглядати можливість надання податкових

пільг для компаній, які демонструють успішність у виконанні завдань з безпеки та захисту.

Окрім того, ДПП може стати платформою для впровадження результатів наукових досліджень і дослідно-конструкторських проектів у практику операторів та власників КІ. Європейський Союз проводить численні дослідження в сфері безпеки. Незважаючи на те, що їх реалізація інколи стикається з труднощами, такі експериментальні ініціативи є важливими для успіху національних проектів.

Стосовно механізмів обміну конфіденційною інформацією в системі захисту критичної інфраструктури, часто постає питання, що може заподіяти більше шкоди: відмова від обміну інформацією чи ризик її передачі неавторизованим особам. Досвід країн ЄС у питанні обміну конфіденційною інформацією різниться. Наприклад, у Хорватії законодавство вимагає, щоб усі дані, пов’язані з критичною інфраструктурою, були засекречені, що створює додаткові проблеми, такі як ідентифікація інформації та необхідність отримання сертифіката безпеки для роботи з нею.

У Фінляндії діє чотири рівні конфіденційності: державна таємниця, таємниця, конфіденційна та інформація з обмеженим доступом. У рамках підприємств комерційна таємниця може класифікуватися як таємна, конфіденційна чи обмежена. Однак, відсутність стандартизованих практик призводить до різних підходів: деякі компанії в Фінляндії та Нідерландах застосовують систему маркування інформації кольорами, відому як «протокол світлофора», що спрощує верифікацію рівня конфіденційності. Інші ж сектори покладаються на довіру між працівниками. Нідерландський досвід показує, що в секторах критичної інфраструктури необхідно призначити відповідальних осіб за обмін інформацією, які залишатимуться на своїх посадах тривалий час, адже для формування довіри потрібен час.

Обмін конфіденційною інформацією є серйозною проблемою не лише, наприкла, в Сербії, а й у розвинених країнах, таких як Нідерланди, Фінляндія

та Швеція, через відсутність усталених процедур. Встановлення довіри між приватним і державним секторами є тривалим процесом, що може бути ускладнене, якщо активи критичної інфраструктури знаходяться під іноземною юрисдикцією [88].

Щодо створення національних центрів критичної інфраструктури, важливо чітко визначити їх функціональні можливості. Це стане першим кроком для вирішення питання про доцільність їх створення як частини існуючої установи або як незалежного органу. Національний центр критичної інфраструктури повинен включати координаційні, контрольні та дослідницькі аспекти. Процес створення такого центру має відбуватися у два етапи. На початковому етапі центр не зможе вирішити всі критичні питання, пов’язані з інфраструктурою, проте його діяльність має об’єднати бізнес, наукові установи та державний сектор.

На другому етапі, коли буде закладено фундамент, можна очікувати досягнення бажаних результатів. Створення таких структур є необхідним для забезпечення ефективного захисту критичної інфраструктури, оптимізації обміну інформацією та сприяння розвитку державно-приватних партнерств у цій важливій сфері.

Республіка Сербія та Республіка Хорватія є представниками європейської континентальної традиції в організації держави та правопорядку, де держава виступає центральним регулятором відносин, визначаючи повноваження та відповідальність інститутів. Важливим аспектом цієї діяльності є управління та забезпечення функціонування системи захисту критичної інфраструктури.

Обидві країни мають досвід у забезпеченні безпекового середовища для контролю ключових об’єктів, установ і процесів, необхідних для функціонування суспільства. Багато аспектів захисту критичної інфраструктури охоплюють заходи, пов’язані з охороною об’єктів, важливих для оборонних операцій та специфічних установ, які підпадають під

законодавче визначення обов'язкового захисту. Важливими також є норми, що регулюють цивільний захист і управління наслідками стихійних лих.

Проте, у багатьох країнах з перехідною економікою, в тому числі в Сербії та Хорватії, існує недостатнє розуміння терміну «критична інфраструктура» і супутніх процесів. Належне усвідомлення значення цих процесів, яке до недавнього часу почало формуватися, стало ключовим фактором для прискорення заходів з регулювання захисту критичної інфраструктури. У період переходу до ринкової економіки з'являється новий стейкхолдер - приватний капітал, що відіграє важливу роль в управлінні критичною інфраструктурою [90].

Таким чином, ефективні моделі державно-приватного партнерства стають запорукою успіху системи захисту критичної інфраструктури. Успішна система може бути створена лише за умови взаємовигідної співпраці всіх зацікавлених сторін, які усвідомлюють позитивні аспекти регулювання системи та готові вкладати зусилля і ресурси для її розвитку. Створення належної системи державно-приватного партнерства у сфері захисту критичної інфраструктури є безперервним процесом, який ніколи не закінчується. Цей компонент є вкрай необхідним для ефективного функціонування системи захисту критичної інфраструктури та забезпечення її стійкості в умовах сучасних викликів.

ДПП набуває особливої актуальності в умовах сучасних викликів безпеки, оскільки воно може забезпечити ефективний механізм захисту критичної інфраструктури. КІ визначається як об'єкти та системи, від функціонування яких залежить життєдіяльність суспільства і забезпечення національної безпеки. Відомо, що в розвинутих західних країнах близько 80% КІ знаходиться у приватній власності, що підкреслює значення приватного сектору у забезпеченні її захисту. Водночас, в умовах Південно-Східної Європи, зокрема в Сербії та Хорватії, цей показник, безсумнівно, є нижчим, що вимагає особливої уваги.

З огляду на глобальні тенденції лібералізації ринку, можна очікувати, що частка приватних інвестицій у критичну інфраструктуру зросте. Відповідно, постає потреба у вдосконаленні нормативно-правової бази, що регулює ДПП, зокрема в контексті захисту КІ. Проблема вимагає системного підходу до регулювання, який включав би розробку концепцій, механізмів та інструментів для ефективного співробітництва між державними та приватними партнерами.

Великим викликом для ДПП є процес державних закупівель та аутсорсингу у сфері безпеки. Окрім підвищення обізнаності про критичну інфраструктуру, важливо ввести положення, які б наголошували на необхідності дотримання високих стандартів у постачанні товарів і послуг. Такі підходи забезпечать не лише якість, а й надійність у захисті критично важливих об’єктів.

У міжнародній практиці спостерігається різний підхід до захисту критичної інфраструктури. Наприклад, у Франції активи КІ визначаються таким чином, щоб їх можна було захистити на належному рівні. У Фінляндії діє система з понад двох тисяч пріоритетних компаній, а в Нідерландах, незважаючи на відсутність спеціального закону про КІ, успішно реалізується концепція «мережі та довіра» [90]. Ці приклади свідчать про те, що ефективна співпраця між державними та приватними партнерами є критично важливою для забезпечення надійного захисту критичної інфраструктури.

Для успішного захисту критичної інфраструктури в умовах сучасних викликів необхідно повною мірою використовувати механізми державно-приватного партнерства. Важливо розвивати нормативно-правову базу, впроваджувати інноваційні підходи до управління ризиками та забезпечити активну співпрацю між державою та приватним сектором. Відтак, такий спосіб дозволить досягти належного рівня безпеки, що стане запорукою стабільності та розвитку суспільства.

ДПП є ключовим механізмом у захисті критичної інфраструктури та потребує комплексного підходу з боку держави для стимулювання участі приватного сектору в забезпеченні національної безпеки. Приватні компанії можуть бути залучені до цього процесу через систему стимулів, яка включає надання необхідних знань, досвіду та керівництва. Одним із пріоритетів для державного сектору є забезпечення приватних партнерів даними про потенційні ризики та загрози, надання консультацій щодо стандартів безпеки та новітнього обладнання, а також роз'яснення складових інформаційних систем попередження. Завдяки доступу до міжнародного досвіду та інформації, зібраної в результаті співпраці з інституціями ЄС та іншими країнами, державний сектор може надавати приватним компаніям актуальну інформацію для впровадження стандартів, що відповідають глобальним вимогам.

Розширення можливостей для приватного сектору передбачає створення мереж, які сприяють взаємодії та обміну інформацією між різними зацікавленими сторонами, що, у свою чергу, сприяє підвищенню ефективності безпеки критичних об'єктів. Крім того, проведення спільних тренінгів та навчальних заходів допомагає розвинути навички, необхідні для запобігання сучасним загрозам. Такі заходи сприяють формуванню стійкості до ризиків у кіберпросторі та інших сферах, підвищують рівень обізнаності та готовності приватних компаній до кризових ситуацій.

Окреме значення має передача результатів науково-дослідних та дослідно-конструкторських проектів до операторів критичної інфраструктури. Через ДПП національні та міжнародні дослідження у сфері безпеки можуть досягти практичної реалізації на місцях. Саме в цьому контексті експериментальні можливості є надзвичайно важливими, оскільки вони дають змогу випробувати нові технології та підходи до забезпечення безпеки у реальних умовах.

Однак, для забезпечення ефективної співпраці необхідно, аби стратегічні та законодавчі засади ДПП були чітко регламентовані. Максимально широке залучення пропозицій від учасників процесу, визначення повноважень та відповідальних осіб сприятиме побудові довіри між усіма сторонами. Така прозорість і структурованість закладає основи для тривалої співпраці і підвищує ефективність захисту критичних об’єктів.

Практика демонструє, що державно-приватне партнерство в цій сфері може бути як добровільним, так і обов’язковим. При добровільній формі важливо запровадити регуляторні рамки для обміну інформацією між учасниками національного форуму захисту критичної інфраструктури.

Одним із важливих аспектів є культурний вимір обміну важливою інформацією, яка не призначена для широкої громадськості. Просте ухвалення законодавчих актів для регулювання цього питання не є достатнім, оскільки довіра в обміні критичною інформацією потребує також культурних засад і чіткої етичної позиції учасників.

Окремо варто відзначити, що інформація, яка підлягає захисту, поділяється на дві категорії: дані, які мають вирішальне значення для національної безпеки, та дані, що важливі для бізнесу й можуть впливати на конкурентні переваги компаній, які управляють критичною інфраструктурою. Державний сектор має враховувати обидва типи інформації, щоб забезпечити адекватний рівень захисту та водночас не порушити інтереси приватних учасників партнерства.

Отже, успішне державно-приватне партнерство є основою для ефективного захисту критичної інфраструктури в умовах сучасних ризиків. Лише за умов розширеного доступу до міжнародного досвіду, активної інформаційної підтримки, проведення спільних тренувань, забезпечення експериментальних проектів та чітких регуляторних рамок можливе досягнення високого рівня стійкості критичних об’єктів до загроз.

6.2. Рекомендації для впровадження кращих практик

Основні рекомендації щодо захисту та стійкості критичної інфраструктури зосереджуються на низці важливих напрямів: від концептуальних засад співпраці між державним і приватним секторами до освітньої роботи і навчання. Основою для успішної взаємодії державного і приватного секторів є чітко визначена концепція співпраці, яка сприятиме підвищенню рівня стійкості критичної інфраструктури (КІ) у країні. У рамках такої співпраці приватні партнери зможуть отримувати від держави критичні знання та інструкції щодо сучасних стандартів захисту, що є необхідною умовою для ефективного реагування на загрози. Крім того, державний сектор забезпечує нормативно-правову підтримку, яка допомагає врегулювати питання безпеки у межах КІ. Нормативна база повинна враховувати стимули для інвестицій та розвитку, забезпечуючи належні умови для реалізації проєктів і створення нових цінностей у сфері КІ.

Державні інститути і приватні компанії мають працювати над визначенням і пріоритезацію об’єктів критичної інфраструктури. Для цього важливо залучити якомога ширше коло зацікавлених сторін і врахувати думку різних інститутів, щоб уникнути ризику централізованого «зверху вниз» підходу. Таким чином, рекомендується створити національний форум як платформу для обговорення пріоритетів ідентифікації та захисту об’єктів КІ, що включатиме представників державного і приватного секторів, академічної спільноти та дослідницьких організацій. Подібний форум забезпечить відкритість і сприятиме обміну знаннями серед учасників. Окрім того, створення та вдосконалення нормативної бази допоможе розв’язати організаційні та правові питання співпраці, чітко розподіливши відповідальність між учасниками процесу і сприяючи підвищенню рівня довіри та захищеності інформації.

Проєкти державно-приватного партнерства (ДПП) є одним із найважливіших інструментів посилення захисту і стійкості критичної інфраструктури. Вони дозволяють державному сектору передати частину ризиків приватному, що сприяє залученню додаткових ресурсів та підвищенню ефективності заходів захисту. Крім того, ДПП сприяє передачі ризиків та фінансового навантаження, дозволяючи приватному сектору брати участь у модернізації, обслуговуванні та захисті КІ об’єктів. Важливо враховувати, що ДПП не є універсальною моделлю і може бути оптимальною лише для певних видів проєктів, однак така співпраця надає можливість для розбудови нових потужностей і підтримки стійкості вже існуючих об’єктів КІ. Держава повинна прагнути до розширення інноваційного фінансування за участі приватних партнерів, забезпечуючи їм прозорі та взаємовигідні умови.

Окрему роль у забезпеченні безпеки КІ відіграють державні закупівлі, які часто перебувають під контролем академічних, професійних і громадських організацій. Удосконалення практики закупівель допоможе уникнути корупційних ризиків та підвищить ефективність використання державних коштів. Крім того, підвищення обізнаності про концепцію захисту КІ є важливим завданням, яке вимагає освітніх і просвітницьких заходів. Академічні установи у співпраці з державними органами повинні забезпечувати регулярне навчання і тренінги, організовувати семінари, майстер-класи та інші заходи для практиків із захисту КІ. Такі заходи допоможуть покращити рівень обізнаності серед осіб, що приймають рішення, і сприятимуть інтеграції новітніх знань і передового досвіду у національні практики захисту КІ.

У рамках системи ДПП рекомендується також розробити три ключові процеси: підготовка та аудит моделей ДПП, ініціювання проєктів співробітництва і моніторинг реалізації проєктів у сфері КІ. Ці процеси повинні бути узгоджені із загальною системою державного управління та

інтегровані в діяльність національного форуму. Зокрема, включення координаторів секторальної безпеки та представників академічної спільноти сприятиме забезпеченню прозорості та ефективності управління проєктами. Також важливо зазначити, що найефективнішим ДПП є тоді, коли його координатором є Національний центр критичної інфраструктури, який має виступати ключовим центром системи захисту КІ.

Ідентифікація критичної інфраструктури та визначення методології оцінки ризиків є важливими елементами стратегії, що включає планування, використання ресурсів і проведення заходів із забезпечення безпеки. Для цього необхідно залучати координаторів секторальної безпеки та керівників КІ, які відповідатимуть за інтеграцію планів у межах їхніх секторів. Оскільки захист критичної інфраструктури вимагає високої кваліфікації, особливо важливим є процес навчання. Він охоплює всі рівні учасників – від керівників до технічних фахівців, тому рекомендовано впроваджувати різноманітні форми тренінгів, включно з електронним навчанням. Важливою складовою є регулярне оновлення змісту навчальних програм відповідно до змін у середовищі безпеки.

Консультування є додатковою цінністю у системі захисту КІ, особливо у випадках, коли потрібні спеціальні знання для вирішення специфічних проблем. Залучення зовнішніх експертів і забезпечення взаємодії з науково-дослідними установами сприятиме успішному впровадженню ефективних заходів безпеки. Поряд із консультаціями, важливу роль відіграють навчання та тренування – практичне відпрацювання процедур і планів у реальних умовах. Виконання тренувальних вправ дозволяє підвищити готовність різних структур до надзвичайних ситуацій, тому важливо, щоб вони ґрунтувалися на реальних сценаріях, максимально наближених до можливих загроз.

Таким чином, комплексний підхід, що охоплює співпрацю, нормативно-правове забезпечення, пріоритезацію об’єктів, проєкти ДПП,

вдосконалення закупівель, навчання та консультування, є необхідною умовою для ефективного захисту критичної інфраструктури та забезпечення національної безпеки.

Налагодження механізмів обміну чутливою інформацією між учасниками системи захисту критичної інфраструктури є надзвичайно важливим аспектом сучасної державної політики безпеки. У світлі швидкої інформатизації та загроз, пов’язаних із кібербезпекою, захист конфіденційних даних стає ключовою складовою державного управління, що впливає на стійкість та функціональність критичної інфраструктури [91].

Ефективний обмін інформацією в межах КІ передбачає комплексний підхід, що включає три базові аспекти інформаційної безпеки: конфіденційність, цілісність та доступність.

Конфіденційність передбачає суворе обмеження доступу до інформації, так, щоб вона була доступною лише авторизованим користувачам. Це означає і належний рівень засекречення самої авторизації, що знижує ризик доступу сторонніх осіб та можливих витоків інформації.

Цілісність даних полягає у забезпеченні захисту від змін як у формі, так і в змісті інформації без дозволу власника даних. Це запобігає ризикам маніпуляції інформацією, що може мати негативні наслідки для об’єктів КІ.

Доступність стосується можливості авторизованих користувачів отримати адекватну інформацію тоді, коли це необхідно. Система має гарантувати своєчасний доступ до даних, що критично важливо в умовах кризи чи надзвичайної ситуації.

Будь-яка невідповідність цим вимогам може призвести до серйозних ризиків, адже порушення у функціонуванні інформаційних систем КІ може загрожувати національній безпеці та створювати катастрофічні наслідки.

З метою належної координації та посилення ефективності захисту КІ доцільно розглянути створення Національного центру критичної інфраструктури. Даний центр має стати центральним координаційним

органом, який буде об’єднувати всі процеси, пов’язані з безпекою критичних об’єктів та організацій.

Функції Національного центру КІ мають включати: координацію зусиль між різними галузями, що використовують критичну інфраструктуру; консультації з питань безпеки та обміну інформацією; дослідження для підвищення стійкості систем до нових видів загроз.

Окрім цього, важливо забезпечити спадковість управлінських рішень, тож розумною стратегією буде створення центру в межах існуючого державного органу, що вже реалізував певні заходи у сфері захисту критичної інфраструктури. Це дозволить зменшити витрати на впровадження нової структури та використати вже напрацьовані механізми захисту й управління.

Процес створення Національного центру КІ може відбуватися в два основні етапи: перший етап має передбачати створення платформи для обміну досвідом і даними між бізнесом, дослідницькими установами та урядовими структурами; на цьому етапі центр слугуватиме як формальною, так і неофіційною платформою для об’єднання зусиль різних секторів; другий етап пов’язується із досягненням повноцінного функціонування центру з повним спектром можливостей, необхідних для гарантування безпеки критичної інфраструктури, включаючи розробку рекомендацій щодо запобігання кризовим ситуаціям та реагування на них.

Однією з найскладніших проблем у роботі Національного центру КІ буде розробка єдиних підходів до обміну чутливою інформацією між зацікавленими сторонами. Незважаючи на критичну важливість цього аспекту, на практиці механізми обміну досі недостатньо регламентовані, а стандарти різняться. Відсутність ефективного обміну інформацією ускладнює взаємодію між суб’єктами, що призводить до неузгодженості дій та виникнення ризиків.

Тому необхідно створити стандартизовані процедури обміну інформацією для всіх учасників системи захисту КІ. Такий підхід сприятиме підвищенню безпеки й дозволить ефективніше координувати зусилля у випадку виникнення загроз або надзвичайних ситуацій. Розвиток механізмів обміну інформацією є ключовою передумовою для функціональної системи захисту критичної інфраструктури. Національний центр критичної інфраструктури зможе стати ядром такої системи, об'єднуючи зусилля різних секторів та забезпечуючи реалізацію національної стратегії безпеки у цій сфері.

6.3. Перспективи розвитку державної політики у сфері захисту критичної інфраструктури

Перспективи розвитку державної політики у сфері захисту критичної інфраструктури передбачають обгрунтування нових можливостей для посилення державної політики в умовах сучасних викликів, які потребують адаптації і впровадження інновацій. Оскільки загрози стають дедалі складнішими й мінливими, виникає необхідність у розробці та реалізації сучасних підходів, що не тільки посилять захист, а й розширять ресурси для підтримки стабільності критичної інфраструктури. У зв'язку з цим варто звернути увагу на інноваційні рішення в галузі фінансування та економічної підтримки, які забезпечать додаткову гнучкість у фінансуванні заходів із захисту критично важливих об'єктів.

У світлі зростаючих викликів, пов'язаних із забезпеченням безпеки критичної інфраструктури, традиційні механізми фінансування стають недостатніми, що вимагає нових економічних підходів. Однією з перспективних можливостей є використання краудфандингу для залучення фінансових ресурсів.

Зокрема, краудфандинг може бути інструментом підтримки інноваційних стартапів у сфері кібербезпеки та інших технологій, спрямованих на захист критичної інфраструктури, що дозволить невеликим технологічним компаніям та дослідникам залучати фінансові ресурси безпосередньо від суспільства та інвесторів, які зацікавлені у безпеці. Такий підхід не лише забезпечує необхідне фінансування для розробки новітніх рішень, але й підвищує обізнаність громадськості щодо важливості захисту критично важливих об’єктів.

Іншим напрямом є розширення моделей страхування для компенсації збитків, пов’язаних із надзвичайними ситуаціями. Страхування критичної інфраструктури може охоплювати як фізичні загрози, такі як природні катастрофи, так і кіберінциденти, що стають все більш поширеними. Впровадження цих моделей дозволяє розподілити фінансове навантаження між державою, приватними інвесторами та страховими компаніями, що сприяє стабільності фінансових ресурсів, необхідних для швидкого реагування та відновлення інфраструктури після інцидентів.

Такі інноваційні підходи до фінансування є перспективними і мають значний потенціал для підвищення ефективності політики захисту критичної інфраструктури, особливо у випадках, коли обсяги державного фінансування обмежені. Вони сприяють посиленню партнерства між державою і приватним сектором, забезпечуючи нові механізми підтримки, які здатні покращити загальну безпеку об’єктів критичної інфраструктури.

Для підвищення ефективності захисту критичної інфраструктури сучасна державна політика дедалі частіше звертається до ідеї залучення громадськості, що базується на використанні соціальних технологій. Одним із перспективних напрямів у цій сфері є розробка систем раннього попередження та спостереження, в яких ключову роль відіграють громадяни, що дозволяє створити багаторівневу систему безпеки, де інформація надходить як від професійних служб, так і від місцевого

населення.

Соціальні технології можуть значно посилити моніторинг і реагування на інциденти, оскільки завдяки мобільним додаткам, платформам збору даних та соціальним мережам громадяни можуть швидко і зручно повідомляти про підозрілі ситуації або потенційні загрози. Наприклад, мобільні додатки, призначені для повідомлення про надзвичайні ситуації, дозволяють користувачам швидко фіксувати й надсилати дані про пожежі, затори, витоки або інші порушення на об’єктах критичної інфраструктури. Такий інтерактивний підхід допомагає зменшити час реагування відповідних служб, оскільки дозволяє виявляти загрози в реальному часі і відразу передавати інформацію фахівцям для подальшого аналізу та усунення проблеми.

Важливо також зазначити, що соціальні мережі відіграють значну роль у поширенні інформації про заходи безпеки та формуванні суспільної обізнаності щодо ризиків і необхідності активної участі громадян. Використання платформ на зразок Twitter або Facebook для оповіщення про ризики, надання інструкцій або інформування про загрози дозволяє оперативно доводити інформацію до широкої аудиторії. Такі платформи також можуть виконувати функцію збору даних від громадян: за їх допомогою люди можуть оперативно ділитися інформацією про загрози з відповідними органами або повідомляти про підозрілі об’єкти чи інциденти.

Залучення громадськості до процесів моніторингу також відкриває можливості для використання краудсорсингових даних, відтак держава може розробляти інтегровані програми, які дозволяють збирати інформацію про стан об’єктів критичної інфраструктури від самих користувачів, що особливо корисно для віддалених або важкодоступних об’єктів. Таким чином, краудсорсинг стає потужним інструментом для отримання оперативних даних і покращення захисту інфраструктури, надаючи додаткову інформацію, яку можуть використовувати служби безпеки.

Загалом, впровадження соціальних технологій і активна участь громадськості у забезпеченні безпеки критичної інфраструктури мають великий потенціал, дозволяючи розширити можливості державної політики у сфері захисту та реагування на сучасні виклики.

Залучення громадськості до систем захисту критичної інфраструктури через соціальні технології стає важливим фактором у покращенні спроможності виявляти і реагувати на загрози. Участь громадян у системах раннього попередження та наглядових програмах може значно посилити можливості захисту критичної інфраструктури. Це не лише активізує ресурсний потенціал суспільства, але й забезпечує необхідну інформацію для своєчасного реагування на надзвичайні ситуації.

Однак, для того щоб система захисту критичної інфраструктури була ефективною, вона повинна також враховувати глобальні виклики, зокрема екологічні та кліматичні фактори, які можуть суттєво впливати на стійкість інфраструктури. У цьому контексті важливо дослідити, як інтеграція політики захисту критичної інфраструктури з екологічними ініціативами може сприяти підвищенню її стійкості до природних катастроф.

Зміни клімату та їх наслідки, такі як збільшення частоти природних катастроф (повеней, землетрусів, ураганів), вимагають від держав і організацій нового підходу до захисту критичної інфраструктури. Підвищення екологічної стійкості стає одним із ключових елементів стратегій безпеки, які забезпечують не лише захист від загроз, але й адаптацію до нових умов, що постійно змінюються. Адаптація об’єктів критичної інфраструктури до змін клімату передбачає переосмислення їх конструктивних і функціональних характеристик. Це може включати використання нових технологій, таких як інноваційні матеріали, що витримують екстремальні температури, або конструкцій, які забезпечують стійкість до паводків і землетрусів.

Крім того, перепроектування існуючих споруд з урахуванням

прогнозованих змін клімату може вимагати змін у проектуванні мостів, дамб або енергетичних станцій. Важливим аспектом також є інтеграція природних елементів, таких як зелені дахи або водоутримувальні системи, які допомагають зменшити ризики від затоплень.

Налагодження зв'язків між політикою захисту критичної інфраструктури та екологічною політикою може здійснюватися через спільні програми управління ризиками. Розробка таких програм, які об'єднують зусилля в боротьбі з кліматичними ризиками та забезпеченні безпеки об'єктів інфраструктури, включає моніторинг ризиків і їх прогнозування на основі сучасних даних про зміни клімату. Інтеграція екологічних стандартів у нормативних актах, що регулюють проектування і будівництво об'єктів критичної інфраструктури, також є необхідною умовою для забезпечення відповідності сучасним викликам.

Необхідність підготовки до природних катастроф стає дедалі актуальнішою. Важливі складові цієї підготовки включають регулярні навчання з метою підготовки до можливих надзвичайних ситуацій, викликаних природними катастрофами, що допоможуть знизити ризики і забезпечити ефективну реакцію. Створення та постійне вдосконалення планів дій на випадок надзвичайних ситуацій, які враховують сценарії, пов'язані з кліматичними змінами, стає основою для швидкого реагування на катастрофи.

Таким чином, впровадження глобальних екологічних та кліматичних ініціатив у систему захисту критичної інфраструктури є необхідним кроком до забезпечення її стійкості. Соціальні технології та залучення громадськості, в поєднанні з інтеграцією екологічних принципів у стратегії захисту, можуть створити комплексну систему, здатну протистояти викликам сучасності. Синергія цих підходів забезпечить більш ефективний захист критичної інфраструктури та підвищить рівень безпеки суспільства в цілому.

Як зазначалось у попередніх підрозділах, гібридні загрози, які поєднують у собі кібернетичні, інформаційні та фізичні атаки, становлять серйозну небезпеку для критичної інфраструктури. В умовах, коли технологічний прогрес супроводжується новими формами агресії, розробка стратегій, спрямованих на забезпечення захисту, стає пріоритетом для держав і організацій. Цей підхід включає не лише зміцнення інформаційних систем, але й підвищення загальної кіберстійкості, що особливо важливо для протидії інформаційно-психологічним загрозам, які можуть порушити не лише функціонування інфраструктури, а й суспільну довіру.

У цьому контексті важливим аспектом є розвиток людського капіталу, який є ключовим для забезпечення ефективної протидії гібридним загрозам. Інвестиції в професійну підготовку та навчання фахівців, здатних реагувати на нові виклики, стають необхідними для зміцнення системи захисту критичної інфраструктури. Розширення інноваційних програм професійного навчання, створення нових сертифікаційних програм дозволить оперативно готувати висококваліфікованих фахівців, здатних адаптуватися до динамічних умов безпеки та впроваджувати нові технології для захисту інформаційних систем.

Вказане демонструє важливість людського ресурсу у вирішенні проблем безпеки. Стратегії, які зосереджуються на посиленні технологічної складової захисту, повинні супроводжуватися активними зусиллями у підготовці кадрів. Лише за умови, що фахівці мають необхідні знання і навички, можна забезпечити надійний захист критичної інфраструктури від комплексних загроз, які можуть виникати в результаті технологічних і соціальних змін.

Таким чином, інтеграція навчальних програм і стратегій захисту від гібридних загроз є ключовою для формування стійкої системи безпеки, здатної до швидкої адаптації та ефективної реакції на сучасні виклики.

Вищезазначене дозволяє зробити висновок про необхідність

комплексного підходу до перспектив розвитку державної політики у сфері захисту критичної інфраструктури, який об’єднує інноваційні рішення, активне залучення громадськості та врахування екологічних викликів. З огляду на зростаючу складність і мінливість загроз, адаптація стратегій захисту стає вкрай важливою.

Пропоновані механізми фінансування, такі як краудфандинг і розширені моделі страхування, можуть стати основою для залучення додаткових ресурсів, необхідних для зміцнення захисту критично важливих об’єктів. Соціальні технології, у свою чергу, є важливим елементом у системах раннього попередження і моніторингу, оскільки активна участь громадян дозволяє оперативно виявляти загрози та знижувати час реагування. Проте, для підвищення ефективності захисту критичної інфраструктури, ці механізми мають бути інтегровані з екологічними ініціативами, що підвищить стійкість інфраструктури до природних катастроф, які дедалі частіше стають наслідком зміни клімату.

Окрім того, розвиток людського капіталу через програми професійного навчання і сертифікації є необхідною умовою для ефективного реагування на нові виклики. Підготовка кваліфікованих фахівців, здатних адаптуватися до динамічного середовища безпеки, стає критично важливою для створення стійкої системи захисту критичної інфраструктури.

Таким чином, синергія між інноваційними фінансовими рішеннями, соціальними технологіями та розвитком людського капіталу є ключовою для забезпечення надійного захисту критичної інфраструктури в умовах сучасних викликів. Реалізація таких стратегій не лише підвищить загальний рівень безпеки, але й зміцнить довіру суспільства до державних інститутів у вказаній сфері.

Завдання для самоконтролю

1. Які основні методи моніторингу та контролю критичної інфраструктури використовуються в сучасній державній політиці?
2. Які технологічні рішення впроваджуються для підвищення захисту критичної інфраструктури?
3. Які основні складові кібербезпеки в контексті захисту критичної інфраструктури?
4. Які критерії використовуються для оцінки ризиків у сфері захисту критичної інфраструктури?
5. Як визначаються показники ефективності державних заходів захисту критичної інфраструктури?
6. Які коригувальні заходи можуть бути застосовані для вдосконалення існуючих методів захисту?
7. Які кращі практики захисту критичної інфраструктури були реалізовані в інших країнах?
8. Які ключові фактори впливають на ефективність систем моніторингу та контролю?
9. Як впливають інноваційні технології на захист критичної інфраструктури?
10. Які загрози можуть виникнути у результаті недотримання кібербезпеки?
11. Як державні органи можуть співпрацювати з приватним сектором у сфері захисту критичної інфраструктури?
12. Які приклади успішних кейсів у сфері захисту критичної інфраструктури можна навести?
13. Які методи оцінки ризиків є найбільш ефективними в умовах сучасних викликів?
14. Як громадськість може бути залучена до процесу захисту критичної інфраструктури?
15. Які етапи включає в себе процес оцінки ефективності заходів захисту?
16. Як зміна клімату впливає на стійкість критичної інфраструктури?
17. Які новітні технології використовуються для покращення кіберзахисту?
18. Як оцінюються ризики, пов’язані з фізичними загрозами критичній інфраструктурі?
19. Які стратегії можуть бути реалізовані для підвищення обізнаності населення про загрози?

20. Які рекомендації можуть бути запропоновані для вдосконалення державної політики у сфері захисту критичної інфраструктури?
21. Які особливості реалізації систем раннього попередження у різних країнах?
22. Яким чином соціальні технології можуть сприяти захисту критичної інфраструктури?
23. Як інтеграція екологічних ініціатив може підвищити стійкість критичної інфраструктури?
24. Які бар'єри існують у впровадженні нових технологій захисту критичної інфраструктури?
25. Які елементи повинні бути включені до планів дій на випадок надзвичайних ситуацій?
26. Яка роль навчання та підготовки кадрів у забезпеченні захисту критичної інфраструктури?
27. Які аспекти економічного фінансування можуть бути вдосконалені для підтримки заходів захисту?
28. Як соціальні мережі можуть використовуватися для моніторингу загроз?
29. Які міжнародні стандарти впливають на політику захисту критичної інфраструктури?
30. Які інструменти можуть бути застосовані для моніторингу ефективності державних заходів?

Теми для самостійних робіт

1. Аналіз систем моніторингу критичної інфраструктури в Україні.
2. Технологічні інновації в захисті критичної інфраструктури: світовий досвід.
3. Роль кібербезпеки у забезпеченні безпеки критичної інфраструктури.
4. Методи оцінки ризиків у сфері захисту критичної інфраструктури.
5. Показники ефективності державних заходів у сфері захисту критичної інфраструктури.
6. Впровадження кращих практик з захисту критичної інфраструктури в Україні.
7. Аналіз успішних кейсів захисту критичної інфраструктури в міжнародному контексті.
8. Виклики та можливості для партнерства між державою і приватним сектором.

9. Роль громадськості у забезпеченні безпеки критичної інфраструктури.
10. Соціальні технології як інструмент підвищення захисту критичної інфраструктури.
11. Взаємозв'язок між екологічними ініціативами та захистом критичної інфраструктури.
12. Інтеграція принципів сталого розвитку у політику захисту критичної інфраструктури.
13. Методології для оцінки ефективності державних заходів захисту.
14. Вплив змін клімату на стійкість критичної інфраструктури.
15. Аналіз методів раннього попередження загроз для критичної інфраструктури.
16. Кіберзагрози як фактор ризику для критичної інфраструктури: аналіз.
17. Розвиток навчальних програм для фахівців у сфері захисту критичної інфраструктури.
18. Бар'єри та шляхи впровадження інноваційних технологій у захист критичної інфраструктури.
19. Соціальні мережі як інструмент моніторингу загроз для критичної інфраструктури.
20. Оцінка міжнародних стандартів у політиці захисту критичної інфраструктури.

Список рекомендованої літератури

1. Green Paper On A European Programme For Critical Infrastructure Protection http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf

2. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf

3. COUNCIL DIRECTIVE 2008/114/EC of 8 December on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

4. Закон України від 08.06.2000 № 1805-III «Про охорону культурної спадщини» https://zakon.rada.gov.ua/laws/show/1805-14#Text

5. Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical infrastructure protection in the fight against terrorism (COM/2004/702 final). http://eur-lex.europa.eu/

6. Communication from the Commission on a European Programme for Critical Infrastructure Protection (COM/2006/786 final). http://eur-lex.europa.eu/

7. Green paper on a European programme for critical infrastructure protection (COM/2005/576 final). http://eur-lex.europa.eu/

8. Proposalfor a Directive of the Council on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection (COM/2006/787 final). – http://eur-lex.europa.eu/

9. Council Directive 2008/114/EC "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection". http://eur-lex.europa.eu/

10. Commission staff working document – Accompanying document to the proposal for a Council decision on creating a Critical Infrastructure Warning Information Network (CIWIN) – Impact assessment (SEC/2008/2702). http://eur-lex.europa.eu/

11. Кодекс цивільного захисту України http://zakon1.rada.gov.ua/laws/show/5403-17/page4

12. Положення про функціональну підсистему єдиної державної системи запобігання і реагування на надзвичайні ситуації техногенного та природного характеру «Безпека об'єктів ядерної енергетики» http://www.snrc.gov.ua/nuclear/uk/publish/article/14050

ГЛОСАРІЙ

Безпека критичної інфраструктури - стан захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури;

Державна програма захисту критичної інфраструктури - офіційний документ, що визначає цілі, стратегії та заходи для забезпечення захисту критичної інфраструктури;

Життєво важливі функції та/або послуги - функції та/або послуги, реалізація яких забезпечується органами державної влади, органами місцевого самоврядування, установами, суб'єктами господарювання та організаціями будь-якої форми власності, збої, переривання та порушення надання яких призводять до швидких негативних наслідків для національної безпеки;

Загроза безпеці критичної інфраструктури - подія або умова, що може призвести до шкоди об'єктам критичної інфраструктури або порушити їх функціонування;

Захист критичної інфраструктури - всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації;

Ідентифікація об'єкта критичної інфраструктури - процедура віднесення об'єкта інфраструктури до об'єктів критичної інфраструктури;

Інцидент безпеки критичної інфраструктури - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного,

технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки несанкціонованого втручання в функціонування об’єкта критичної інфраструктури, які становлять загрозу його безпеці, системі управління технологічними процесами об’єкта критичної інфраструктури, створюють ймовірність порушення штатного режиму функціонування такого об’єкта (у тому числі зриву та/або блокування роботи, та/або несанкціонованого управління його ресурсами), ставлять під загрозу його захищеність;

Категоризація об’єктів інфраструктури - віднесення об’єктів інфраструктури до категорій критичності об’єктів інфраструктури;

Категорія критичності (критерії) об’єкта критичної інфраструктури - ступінь (відносний рівень) важливості об’єкта критичної інфраструктури, класифікована (категоризована) залежно від його впливу на виконання життєво важливих функцій та/або надання життєво важливих послуг;

Комплексний захист критичної інфраструктури - інтегрований підхід до забезпечення безпеки об’єктів критичної інфраструктури, що охоплює фізичні, інформаційні та кібернетичні аспекти;

Кризовий план реагування - документ, що описує процедури та заходи, які мають бути вжиті у разі виникнення кризової ситуації;

Кризова ситуація - порушення або загроза порушення штатного режиму функціонування критичної інфраструктури чи окремого її об’єкта, реагування на яке потребує залучення додаткових сил і ресурсів;

Критична інфраструктура - сукупність об’єктів критичної інфраструктури;

Критична технологічна інформація - дані, що обробляються (приймаються, передаються, зберігаються) в системах управління

технологічними процесами об’єктів критичної інфраструктури;

Масштабування загроз - процес оцінки та класифікації загроз на основі їх потенційного впливу та ймовірності реалізації;

Надзвичайна ситуація - подія, що може загрожувати безпеці населення, державі чи критичній інфраструктурі та вимагає термінових заходів реагування;

Національна система захисту критичної інфраструктури - сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій - у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури;

Несанкціоноване втручання - незаконні дії, що створили загрозу безпечному функціонуванню об’єкта критичної інфраструктури та призвели до одного або декількох з таких наслідків: порушили його безперервність і стійкість; створили реальні чи потенційні загрози для населення, суспільства, соціально-економічного стану, національної безпеки і оборони України;

Обґрунтування інвестицій у безпеку - аналіз витрат і вигод, пов’язаних із впровадженням заходів безпеки для критичної інфраструктури;

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;

Оператор критичної інфраструктури - юридична особа будь-якої форми власності та/або фізична особа - підприємець, що на правах

власності, оренди або на інших законних підставах здійснює управління об’єктом критичної інфраструктури та відповідає за його поточне функціонування;

Охорона об’єктів критичної інфраструктури - комплекс режимних, інженерних, інженерно-технічних та інших заходів (крім заходів із захисту інформації та кіберзахисту об’єктів критичної інформаційної інфраструктури), які організовуються і проводяться суб’єктами національної системи захисту критичної інфраструктури з метою запобігання та/або недопущення чи припинення протиправних дій (актів несанкціонованого втручання) на об’єктах критичної інфраструктури;

Паспорт безпеки - документ встановленої форми, який містить відомості про об’єкт критичної інфраструктури, а також комплекс заходів, що вживаються для захисту цього об’єкта від визначених для нього видів загроз (відомості, що містяться у паспорті безпеки, є інформацією з обмеженим доступом);

План дій з відновлення - набір заходів, які мають бути вжиті для відновлення функціонування критичної інфраструктури після інциденту;

Проектна загроза об’єкту критичної інфраструктури - документ встановленої форми, який визначає властивості, характеристики реальних і потенційних загроз об’єкту критичної інфраструктури, на зниження ймовірності реалізації яких має бути спрямовано функціонування системи захисту критичної інфраструктури;

Протидія кіберзагрозам - заходи, що вживаються для захисту інформаційних систем від несанкціонованого доступу, атак або інших кібернетичних загроз;

Реєстр об’єктів критичної інфраструктури - автоматизована система, що містить перелік найбільш важливої для життєдіяльності

суспільства та держави критичної інфраструктури, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості і здійснюється моніторинг їх дотримання;

Режим функціонування критичної інфраструктури - визначені оператором умови та вимоги до функціонування критичної інфраструктури залежно від стану і динаміки розвитку ситуації (штатний режим функціонування; режим функціонування у кризовій ситуації; режим відновлення);

Ризик-менеджмент - процес ідентифікації, оцінки та управління ризиками, пов'язаними з безпекою критичної інфраструктур;

Рівень критичності об'єкта критичної інфраструктури - відносна міра важливості об'єкта, якою враховується його вплив на можливість виконання життєво важливих функцій та надання життєво важливих послуг;

Сектор критичної інфраструктури - сукупність об'єктів критичної інфраструктури, які належать до одного сектору (галузі) економіки та/або мають спільну функціональну спрямованість;

Секторальний орган у сфері захисту критичної інфраструктури - державний орган, визначений законодавством відповідальним за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури;

Системи раннього попередження - технології та методи, які використовуються для виявлення загроз до їх появи, що дозволяє вжити заходів для запобігання або зменшення їхнього впливу;

Стійкість критичної інфраструктури - стан критичної інфраструктури, за якого забезпечується її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого

виду;

Технологічні ризики - загрози, пов’язані з впровадженням нових технологій у функціонування критичної інфраструктури;

Функціональний орган у сфері захисту критичної інфраструктури - державний орган, визначений відповідальним за функціонування окремих державних систем захисту та реагування;

Цілісність системи - стан, при якому всі елементи критичної інфраструктури працюють узгоджено, забезпечуючи належний рівень безпеки та функціональності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про національну безпеку України: Закон України URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text

2. Про критичну інфраструктуру: Закон України URL : https://zakon.rada.gov.ua/laws/show/1882-20#Text

3. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. К. : НІСД, 2019. 224 с. URL : https://niss.gov.ua/sites/default/files/2019-05/Dopov_Suchodolya_print.pdf

4. Стійкість економіки: оцінювання та забезпечення : монографія / А. В. Бойко, Д. Б. Шкуропадська, Ю. А. Гладка та ін. ; за ред. А. В. Бойко. Київ : Київ. нац. торг.-екон. ун-т, 2021. 444 с. URL : https://knute.edu.ua/file/MjIxNw==/8974d7afa9740e16576b1e121674144c.pdf

5. Глобалізація та розвиток інноваційних систем: тенденції, виклики, перспективи : матеріали II Міжнар. наук.-практ. конф., 14-15 березня 2024 р. Держ. біотехнологічний ун-т. Харків, 2024. 565 с. URL : https://biotechuniv.edu.ua/wp-content/uploads/2024/04/conf-14-15-03-24-mater.pdf

6. UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001. URL : https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

7. Кизим М. О., Хаустова В. Є., Трушкіна Н. В. Сутність поняття «критична інфраструктура» з позицій національної безпеки України. *Бізнесінформ № 12 2022.* URL : https://www.business-inform.net/export_pdf/business-inform-2022-12_0-pages-58_78.pdf

8. A. Alexandru, A.V. Vevera. National Security and Critical Infrastructure Protection. International conference «Knowledge-based organization». June 2019. URL : https://www.researchgate.net/publication/334677561_National_Security_and_Critical_Infrastructure_Protection

9. МОЗ. Критична інфраструктура. Нормативно-правова база у сфері захисту критичної інфраструктури. URL : https://moz.gov.ua/uk/kritichna-infrastruktura

10. Суспільно-політичні процеси в умовах пандемії: особливості та виклики : тези доповідей Всеукр. наук.-практ. конф. (Київ, 16 квітня 2021 р.) / відп. ред. А. А. Кравченко. Київ : Київ. нац. торг.-екон. ун-т, 2021. 184 с. URL : https://knute.edu.ua/file/MjIxNw==/34c36a90231954f5803db34d9096a6c5.pdf

11. Звіт про прямі збитки інфраструктури від руйнувань внаслідок військової агресії росії проти України за рік від початку повномасштабного вторгнення. URL : https://kse.ua/wp-content/uploads/2023/03/UKR_Feb23_FINAL_Damages-Report-1.pdf

12. Національна рада з відновлення України від наслідків війни. Проект Плану відновлення України Матеріали робочої групи «Аудиту збитків, понесених внаслідок війни» URL : https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/audit-of-war-damage.pdf

13. A. Shaji George, T. Baskar. Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. URL : https://www.researchgate.net/publication/378078435_Cyber_Threats_to_Critical_Infrastructure_Assessing_Vulnerabilities_Across_Key_Sectors

14. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О. М. Суходолі. Київ: НІСД, 2020. 28 с.

15. Massive investment is needed in sustainable infrastructure to build climate change resilience. URL : https://www.oecd.org/en/about/news/press-releases/2024/04/massive-investment-is-needed-in-sustainable-infrastructure-to-build-climate-change-resilience.html

16. Getting infrastructure right: the OECD framework for better governance. URL : https://blogs.worldbank.org/en/ppps/getting-infrastructure-right-oecd-framework-better-governance

17. 63 FR 41804 - Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators. URL : https://www.govinfo.gov/app/details/FR-1998-08-05/98-20865

18. The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. URL : https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

19. Critical National Infrastructure. URL : https://www.npsa.gov.uk/critical-national-infrastructure-0

20. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. URL : https://www.coe.int/en/web/cybercrime/the-budapest-convention

21. Second additional protocol to the convention on cybercrime on enhanced co-operation and disclosure of electronic evidence. Special edition dedicated to the drafters of the Protocol. URL : https://rm.coe.int/special-edition-second-protocol-en-2021/1680a69930

22. Communication from the commission to the european parliament and the council. First Progress Report on the EU Security Union Strategy. Brussels, 09.12.2020. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0797

23. Домарацький М. Б. Специфіка державного регулювання критичної інфраструктури в Україні. *Публічне управління та митне адміністрування*. 2020. № 2(25). С. 24-46.

24. ISO 22301:2019. Security and resilience — Business continuity management systems - Requirements. URL : https://www.iso.org/standard/75106.html

25. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems. URL : https://www.iso.org/standard/27001

26. ISO 9001:2015. Quality management systems. URL : https://www.iso.org/standard/62085.html

27. UNDP. Risk assessment. https://www.undp.org/tag/risk-assessment

28. Parliamentary Handbook On. Security Council resolution 1373 (2001). URL : https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/oct_pe_handbook.pdf

29. International Civil Aviation Organisation (ICAO). URL : https://www.globeair.com/g/international-civil-aviation-organisation-icao

30. Safety standards. IAEA. URL : https://www.iaea.org/resources/safety-standards

31. The Protection of Critical Infrastructure Against Terrorist Attacks. Compendium of Good Practices. 2022 Update. URL : https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf

32. Cybersecurity and New Technology. Conducting Terrorist Threat Assessment: The Use of New Technologies for Terrorist Purposes. United Nations Office of Counter-Terrorism (UNOCT), United Nations Office of Counter-Terrorism, United Nations Headquarters. New York 2023. URL : https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_conducting_terrorist_threat_web.pdf

33. NATO 2022 STRATEGIC CONCEPT. URL : https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-

concept.pdf

34. ISO 14090:2019. Adaptation to climate change — Principles, requirements and guidelines. URL : https://www.iso.org/standard/68507.html

35. NIST. Cybersecurity Framework. URL : https://www.nist.gov/cyberframework

36. ENISA. URL : https://www.enisa.europa.eu/

37. ISO 22316:2017. Security and resilience — Organizational resilience — Principles and attributes. URL : https://www.iso.org/standard/50053.html

38. Critical Infrastructure Information Act. URL : https://www.dhs.gov/publication/critical-infrastructure-information-act

39. Homeland Security Grant Program. URL : https://www.fema.gov/grants/preparedness/homeland-security

40. Schutz Kritischer Infrastrukturen. URL : https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/schutz-kritischer-infrastrukturen/schutz-kritischer-infrastrukturen-node.html

41. Das Bundesministerium des Innern und für Heimat. URL : https://www.bmi.bund.de/DE/ministerium/ministerium-node.html

42. Sicherheitspartnerschaften. URL : https://www.mi.niedersachsen.de/startseite/themen/innere_sicherheit/polizei_niedersachsen/zusammenarbeit_der_polizei_mit_anderen/sicherheitspartnerschaften/-60364.html

43. IT-Grundschutz. URL : https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

44. Civil Contingencies Act 2004. URL :https://www.legislation.gov.uk/ukpga/2004/36/contents

45. The National Cyber Security Centre. URL :https://www.ncsc.gov.uk/

46. The Protection of Critical Infrastructure Against Terrorist Attacks Compendium of Good Practices 2022 Update. URL :

https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf

47. Critical infrastructure protection. URL : https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en

48. COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection. URL : https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

49. Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC. URL : https://www.europeansources.info/record/proposal-for-a-directive-on-the-resilience-of-critical-entities/

50. What is NIS2? URL : https://nis2directive.eu/what-is-nis2/

51. Joint Cyber Unit. URL : https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit

52. Horizon Europe. URL : https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

53. OECD Policy Framework on Digital Security. URL : https://www.oecd.org/en/publications/oecd-policy-framework-on-digital-security_a69df866-en.html

54. The Directive on security of network and information systems (NIS Directive). URL : https://digital-strategy.ec.europa.eu/en/library/directive-security-network-and-information-systems-nis-directive

55. Деякі питання об’єктів критичної інфраструктури: Постанова КМУ від 9 жовтня 2020 р. № 1109. URL : https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

56. Про затвердження Порядку ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього: Постанова КМУ від 28 квітня 2023 р. № 415

https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text

57. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 22.07.2022 №821. URL : https://www.kmu.gov.ua/npas/pro-zatverdzhennia-poriadku-prove-a821

58. Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури: Постанова Кабінету Міністрів України від 14.10.2022 №1174. URL : https://www.kmu.gov.ua/npas/pro-zatverdzhennia-rehlamentu-obminu-informatsiieiu-mizh-subiektamy-natsionalnoi-t141022

59. Урядовий портал. URL : https://www.kmu.gov.ua/

60. Міністерство енергетики України. URL : https://www.kmu.gov.ua/catalog/minekoenergo-ukraini

61. Про енергетичну ефективність: Закон України URL : https://zakon.rada.gov.ua/laws/show/1818-20#Text

62. Міністерство розвитку громад та територій України. URL : https://www.kmu.gov.ua/catalog/ministerstvo-infrastrukturi-ukraini

63. Міністерство охорони здоров'я України. URL : https://www.kmu.gov.ua/catalog/ministerstvo-okhoroni-zdorovya-ukraini

64. Державна служба з питань безпеки харчових продуктів та захисту споживачів. URL : https://dpss.gov.ua/

65. Державна служба України з надзвичайних ситуацій. URL : https://dsns.gov.ua/diyalnist-sluzhbi

66. Державна служба спеціального зв'язку та захисту інформації України. URL : https://cip.gov.ua/ua

67. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України URL : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

68. Служба безпеки України. URL : https://ssu.gov.ua/

69. Національна поліція України. URL : https://www.npu.gov.ua/

70. Про державно-приватне партнерство: Закон України URL : https://zakon.rada.gov.ua/laws/show/2404-17#Text

71. Про основні засади забезпечення кібербезпеки України: Закон України. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text

72. «Деякі питання об'єктів критичної інформаційної інфраструктури»: Постанова Кабінету Міністрів України №943. URL : https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n13

73. EPCIP. European Programme for Critical Infrastructure Protection. URL : https://www.gie.eu/wp-content/uploads/filr/3217/20161116%20CIP%20in%20Europe.pdf

74. Cybersecurity Information Sharing Act of 2015. URL : https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Information%2520Sharing%2520Act%2520of%25202015.pdf

75. ISACs. Information Sharing and Analysis Centers. URL : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

76. CISA. (Cybersecurity and Infrastructure Security Agency). URL : https://www.cisa.gov/

77. AIS. (Automated Indicator Sharing). URL : https://www.cisa.gov/topics/cyber-threats-a

78. CyberCorps: Scholarship for Service. URL : https://sfs.opm.gov/

79. HSGP (Homeland Security Grant Program). URL : https://www.dhs.gov/homeland-security-grant-program-hsgp

80. А. В. Жилін, О. М. Шаповал, О. А. Успенський. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с. URL : https://ela.kpi.ua/server/api/core/bitstreams/d99a0045-e907-4d17-afc1-5431f67d2444/content

81. Терлюк О. Технологія Blockchain в контексті можливостей цифровізації ефективного публічного адміністрування. *Вісник Національного університету «Львівська політехніка».* Серія: «Юридичні науки». 2022, № 9 (1) с. 121-128.

82. Singapore updates OT Masterplan 2024 to bolster national cybersecurity defense. URL : https://industrialcyber.co/industrial-cyber-attacks/singapore-updates-ot-masterplan-2024-to-bolster-national-cybersecurity-defense/

83. Christine Große. Multi-Level Planning for Enhancing Critical Infrastructure Resilience against Power Shortages-An Analysis of the Swedish System of Styrel. URL : https://www.mdpi.com/2412-3811/6/5/71

84. C. Pursiainen. Challenges for protecting Europe's critical infrastructure, Journal of European Integration, 2009. Issue 31/6, p. 721-739.

85. В.О. Хрутьба, В.І. Зюзюн, Д.С. Нєвєдров. Огляд науково-теоретичних аспектів безпеки об'єктів критичної інфраструктури транспорту. *Вісник Національного технічного університету "ХПІ". Серія: Стратегічне управління, управління портфелями, програмами та проектами*. Харків: ХПІ 2019. № 2 (1327). С. 60-65.

86. OECD. Належне врядування для забезпечення стійкості критичної інфраструктури, Огляди політики управління ризиками OECD, Публікація OECD, 2019. Париж. URL : https://doi.org/10.1787/02f0e5a0-en

87. Stankova, M., Kaleychev, S. Balkans – safe and secure destination for tourism. *Tourism & Hospitality Industry*. 2022, Congress Proceedings, pp. 281-293.

88. Towards Testing Critical Infrastructure Resilience. JRC Publications Repository. URL : https://publications.jrc.ec.europa.eu/repository/handle/JRC89209

89. Krister Pursiainen and Eero Kyutomaa. From European critical infrastructure protection to the resilience of European critical entities: what does

it mean? *Sustainable and Resilient Infrastructure*, 2023. 8:sup1, 85-101, DOI: 10.1080/23789689.2022.2128562

90. Myriam Dunn and Victor Mauer (eds.) INTERNATIONAL CIIP HANDBOOK 2006 VOL. II ANALYZING ISSUES, CHALLENGES, AND PROSPECTS Series Editors Andreas Wenger and Victor Mauer Center for Security Studies, ETH Zurich. URL : https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-2006-2.pdf

91. Peter Grindrod. The National Risk Register 2023: some reasoned reflections. URL : https://www.tandfonline.com/doi/full/10.1080/23789689.2024.2404277?src=exp-la#abstract

Навчально-методичне видання

ЗАПОРОЖЕЦЬ Тетяна Володимирівна

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Навчальний посібник

Для студентів Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка, які навчаються за освітніми програмами за спеціальністю 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону»

Підписано до друку 20.11.2024 р. Формат 60×84/16. Папір офсетний.

Гарнітура Times. Друк різографія.

Умов. друк. арк. 10,81. Обл.-вид. арк. 9,34 Наклад 300 прим. Зам. № 2011/1

Видавництво та друк ТВО «ДКС-Центр»

вул. Дорогожицька, 18, м. Київ, тел. (050) 381-81-81

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру

ДК № 3457 від 08.04.2009 р.