МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЕКОЛОГІЧНОЇ БЕЗПЕКИ, ІНЖЕНЕРІЇ ТА ТЕХНОЛОГІЙ
КАФЕДРА ЦИВІЛЬНОЇ ТА ПРОМИСЛОВОЇ БЕЗПЕКИ
ІМЕНІ ГЕРОЯ УКРАЇНИ ЧУБА ОЛЕКСАНДРА СЕРГІЙОВИЧА

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____Б.Д. Халмурадов
«_____» _____2024 р.

КВАЛІФІКАЦІЙНА РОБОТА (ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРАЗА СПЕЦІАЛЬНІСТЮ 263 «ЦИВІЛЬНА БЕЗПЕКА»

Тема: «Підвищення стійкості об'єктів критичної інфраструктури»

Виконавець: студент групи 413 ЦБ Прохоров Юрій Романович

Керівник: _д.т.н., професор Третьяков Олег Вальтерович

Нормоконтролер: _____ Козлітін О.О.____

КИЇВ 2024

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет екологічної безпеки, інженерії та технологій
Кафедра цивільної та промислової безпеки імені Героя України Чуба Олександра Сергійовича
Спеціальність 263 «Цивільна безпека»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____Б.Д.Халмурадов
«___»_____2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Прохорова Юрія Романовича

1. Тема роботи «**Підвищення стійкості об’єктів критичної інфраструктури**» затверджена наказом ректора від «17» квітня 2024 року № 579/ст.
2. Термін виконання роботи з 20.05.2024 по 16.06.2024.
3. Вихідні дані роботи:
    - Аналіз та класіфікація потенційних загроз для критичної інфраструктури.
    - Визначення загроз та ризиків критичної інфраструктури.
    - Аналіз сучасних підходів до підвищення стійкості об'єктів критичної інфраструктури.
    - Оцінка існуючих заходів та розробка рекомендацій можливих методів зазихисту об’єктів критичної інфраструктури на існуючих прикладах .
    - Зформування висновків та рекомендацій щодо підвищення стійкості критичної інфраструктури.

4. Зміст пояснювальної записки: оцінка загальних відомостей, літературних та інших джерел кваліфікаційної роботи. Аналіз сучасних підходів до підвищення стійкості об'єктів критичної інфраструктури. Вивчення існуючих заходів з захисту та підвищення стійкості критичної інфраструктури від різних типів загроз. Розробка рекомендацій щодо підвищення стійкості критичної інфраструктури.

5. Календарний план-графік

№ з/п	Завдання	Термін виконання	Підпис керівника
1	2	3	4
1	Аналіз теми кваліфікаційної роботи	20.05.2024-22.05.2024	
2	Збір інформаційних даних та Аналіз літературних джерел	22.05.2024-24.05.2024	
4	Робота з написання розділу №1	24.05.2024-28.05.2024	
5	Робота з написання розділу №2	28.05.2024-02.06.2024	
6	Підготовка, оформлення і друк пояснювальної записки	03.06.2024-06.06.2024	
7	Оформлення презентації в Power Point	07.06.2024-08.06.2024	
9	Підготовка до захисту роботи	09.06.2024-10.06.2024	

6. Дата видачі завдання: «20» травня 2024 р.

Керівник кваліфікаційної роботи: _____ _____

Завдання прийняв до виконання: _____ Прохоров Ю. Р.

РЕФЕРАТ

Кваліфікаційна робота складається із вступу, основної частини, що містить 2 розділи, висновку й списку літератури. Загальний обсяг роботи – 63сторінки. Список бібліографічних посилань включає 40 джерел.

Ключові слова: Критична інфраструктура, забезпечення стійкості, безпека.

Об’єкт дослідження це стійкість критичної інфраструктури, яка включає в себе найважливіші сектори життєзабезпечення держави.

Предмет дослідження – рівень досягнень провідних країн світу у сфері забезпечення стійкості об’єктів інфраструктури.

Мета роботи –аналіз запроваджених рішень з підвищення безпеки та стійкості критичної інфраструктури України, на базі існуючих методичних рекомендацій.

Методи, застосовані в кваліфікаційній роботі: теоретичні та емпіричні методи дослідження небезпек, аналіз стійкості та захищеності об’єктів критичної інфраструктури.

Наукова новизна постановлення пріоритетів при загрозах різного рівня для зниження ризиків; розробка стратегій захисту об’єктів приватного та державного секторів.

ЗМІСТ

ВСТУП 6
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 8
1.1 Поняття та класифікація об'єктів критичної інфраструктури 8
1.2 Загрози та ризики для об'єктів критичної інфраструктури 18
1.3 Сучасні підходи до підвищення стійкості об'єктів критичної інфраструктури 23
РОЗДІЛ 2. ПРАКТИЧНІ АСПЕКТИ ПІДВИЩЕННЯ СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 29
2.1 Аналіз існуючого стану захищеності об'єктів критичної інфраструктури в Україні 29
2.2 Розробка рекомендацій щодо підвищення стійкості об'єктів критичної інфраструктури 41
2.3 Оцінка ефективності запропонованих заходів щодо підвищення стійкості об'єктів критичної інфраструктури 49
ВИСНОВКИ 55
СПИСОК РЕФЕРОВАНОЇ ЛІТЕРАТУРИ 55

ВСТУП

Критична інфраструктура будь-якої держави − це велика складна система стратегічного масштабу, яка є сукупністю значної кількості елементів різного типу, об'єднаних зв'язками різної природи і яка володіє загальною властивістю (призначенням, функцією), відмінною від властивостей окремих елементів усієї сукупності. Необмежена кількість об'єктів і параметрів системи, які постійно варіюються, та важко прогнозована поведінка об'єктів з великою кількістю взаємозв'язків є основними причинами труднощів виявлення об’єктів критичної інфраструктури держави.

Критична інфраструктура є одним із найважливіших аспектів національної безпеки будь-якої країни. Він включає об’єкти та системи, належне функціонування яких має важливе значення для економічного розвитку, безпеки та добробуту громадян. Критична інфраструктура включає енергетичні системи, водопостачання, транспорт, зв’язок, фінансові установи, охорону здоров’я, харчову промисловість та інші ключові галузі.

Важливість критичної інфраструктури полягає в тому, що це може мати серйозні наслідки для їх роботи, як для окремих регіонів, так і для країни в цілому. Напади на критичну інфраструктуру, стихійні лиха, техногенні катастрофи, тероризм та інші загрози можуть завдати серйозної шкоди, порушити громадські операції та підірвати національну безпеку.

У сучасному світі підвищення стабільності критичних компонентів інфраструктури є особливо актуальним питанням. Це зумовлено подальшим ускладненням інфраструктурних систем, збільшенням кількості можливих загроз і ризиків, необхідністю забезпечення стабільного функціонування економіки та соціальної діяльності в світлі глобальних викликів.

Підвищення стабільності компонентів критичної інфраструктури є складним завданням, яке вимагає поєднання різних стратегій, методів і підходів. Це включає розробку та застосування новітніх захисних технологій, удосконалення законодавчої бази, підвищення кваліфікації персоналу та створення ефективних систем управління ризиками та небезпеками. Розробка

стратегії кібербезпеки потребує особливої уваги, оскільки сучасні інфраструктурні системи значною мірою залежать від інформаційних технологій.

Об'єктом дослідження є критична інфраструктура як сукупність взаємопов'язаних систем та об'єктів, що забезпечують життєво важливі функції для суспільства та держави.

Предметом дослідження є методи, засоби та підходи до підвищення стійкості об'єктів критичної інфраструктури в умовах загроз різного характеру.

Завдання:

1. Розглянути поняття та класифікація об'єктів критичної інфраструктури.

2. Визначити загрози та ризики для об'єктів критичної інфраструктури.

3. Проаналізувати сучасні підходи до підвищення стійкості об'єктів критичної інфраструктури.

4. Провести аналіз існуючого стану захищеності об'єктів критичної інфраструктури в Україні.

5. Розробити рекомендацій щодо підвищення стійкості об'єктів критичної інфраструктури.

6. Оцінити ефективність запропонованих заходів щодо підвищення стійкості об'єктів критичної інфраструктури.

Структура роботи: вступ, два розділи, висновок, список використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Поняття та класифікація об'єктів критичної інфраструктури

Критичні інфраструктури є основою рухомих суспільств. Однак ми все більше залежимо від функціонуючих послуг, навіть якщо кліматичні ризики та глобальні потрясіння виявляють уразливість наших систем. Останніми роками руйнівні землетруси, урагани і навіть глобальна пандемія показали, що без належного захисту нашої інфраструктури наслідки катастроф загострюються, погіршуючи страждання людей і навколишнього середовища. Визнання ключової ролі, яку відіграють інфраструктури в нашому повсякденному житті, і вжиття заходів для мінімізації ризиків для них ніколи не було настільки важливим.

Розвиток цивілізації разом з економічною глобалізацією, урбанізацією та широким використанням інформаційних технологій зумовили велику залежність людей і суспільства від послуг, що надаються енергетичними, телекомунікаційними, транспортними та іншими інфраструктурними системами. Сьогодні доступність цих послуг вважається одним із показників якості життя. Тільки країни з розвиненою інфраструктурою можуть розвинутися в сучасні економічні центри, які розвивають і концентрують економічні, промислові та інтелектуальні ресурси у своєму регіоні.

Водночас спостерігається значна тенденція до посилення негативних природних, штучних і соціально-політичних процесів (у всьому світі зростає кількість і масштаби наслідків стихійних лих, виникають нові військові конфлікти). дим і горить, тероризм постійно вчиняється, кількість кібератак зростає дуже швидко), які є прямою та постійною загрозою безперервному функціонуванню згаданих інфраструктур, таким чином гарантуючи їхню велику місію «повного захисту. «навіть у випадку економічно розвинених країн.

Саме необхідність спрямування ресурсів на захист критичної інфраструктури призвела до розробки та впровадження концепції критичної

інфраструктури (КІ) як частини систем національної безпеки деяких провідних країн світу. У Сполучених Штатах інформаційна інфраструктура – це унікальний набір систем, мереж і засобів, збій або знищення яких може мати величезні, навіть незворотні, негативні наслідки для національної економіки, добробуту та здоров'я, а також для подальшого розвитку народного господарства [1].

Подібне визначення можна знайти в директиві 786 Європейської Комісії від 2006 року [24], згідно з якою загальноєвропейський кредитний рейтинг сприяють національні кредитні установи держав-членів ЄС, які мають такий ефект. занепокоєння, небезпечних умов. або шкідливе втручання, що поширюється від країни, де розташована ця установка, до принаймні однієї іншої країни ЄС. Концепція захисту інтелектуальної власності також була введена в розвинених країнах, таких як Канада, Австралія та Великобританія.

Враховуючи процеси поступової модернізації сектору безпеки в Україні та наше прагнення стати повноправним учасником європейсько-атлантичного безпекового простору, питання подання ідеї оборони ІС стає все більш актуальним.

Сказати, що захисту критичних систем, мереж і об'єктів в Україні приділяється мало уваги, було б неправильно. Навпаки, в державі паралельно діє єдина система запобігання, реагування та припинення актів тероризму, єдина державна система запобігання та реагування на надзвичайні ситуації антропогенного та природного походження, яка трансформувалася в єдину державну систему забезпечення громадського захисту населення і території [25].

В Україні охорона об'єктів, які згідно з міжнародною практикою класифікуються як «критична інфраструктура», регулюється численними нормативно-правовими актами та законами, більшість з яких відомчі. Така ситуація виникла природно: кожен відділ бачив конкретну загрозу своїм об'єктам і мав певні інструменти та ресурси для забезпечення безпеки цих об'єктів.

Так, чинне законодавство визначає декілька категорій об'єктів, для яких встановлюються особливі умови забезпечення охорони:

- підприємства, що мають стратегічне значення для економіки та безпеки держави;

- продукція, занесена до державного реєстру потенційно небезпечних об'єктів;

- об’єкти підвищеної небезпеки (у тому числі перелік особливо небезпечних підприємств, які потребують вжиття заходів щодо запобігання заподіянню шкоди життю та здоров’ю громадян, майну, об’єктам та навколишньому середовищу;

- важливі державні установи;

- товари, що підлягають примусовій охороні підрозділів Державної служби охорони згідно з договорами;

- об'єкти, що підлягають охороні та захисту під час надзвичайних ситуацій та особливого періоду;

- основні електротехнічні установки;

- важливі спеціальні частини нафтогазової промисловості;

- Національна секретна система зв'язку;

- платіжні системи;

- система швидкої медичної допомоги;

- аварійно-рятувальні служби;

- постійні об’єкти культурної спадщини [19].

Проте, незважаючи на значну кількість локально визначених категорій критичних об’єктів та їх відповідних переліків, в Україні відсутня детальна (уніфікована) оцінка ризиків втрати або пошкодження цих об’єктів. Чинне законодавство досі не дає визначення терміну «критична інфраструктура», хоча в оновленому плані національної безпеки серед іншого згадуються шляхи підвищення енергетичної безпеки: «ефективний захист критичної інфраструктури енергетичного комплексу та енергетики з точки зору середовище і життя «уражена та шкідлива діяльність», а один із засобів забезпечення інформаційної безпеки визначено так: «забезпечення безпеки інформаційно-електронної системи, що діє на користь держави, забезпечення

потреб Держава оборони та безпеки, кредитні банки та інші сектори економіки, система контролю важливої інфраструктури».

Зрозуміло, що поняття «критична інфраструктура» не може бути додано до українського законодавства як кінцева мета сама по собі. Концепція критичної інфраструктури має бути покладена в основу ефективної системи координації дій органів влади для запобігання втраті чи непоправному пошкодженню найважливіших для життєдіяльності держави структур з урахуванням впливу негативних чинників, у тому числі стан будь-якого людського, природного чи соціально-політичного походження або будь-якої їх комбінації.

Також визначення «критичної інфраструктури» в законодавстві не створює автоматичного переліку таких об'єктів. Це видно з досвіду ідентифікації об'єктів КІ в США, де відповідальний підрозділ, навіть за наявності значних матеріальних та організаційних засобів для виконання такого завдання, поставив проблему розробки методології, не кажучи вже про це. потреба. . для обробки величезних обсягів даних про об'єкти (з понад 33 000 об'єктів-кандидатів 3 000 об'єктів, пов'язаних з 18 життєвими доменами, було призначено СІ [21].

У 2005 році в ЄС була спроба визначити Ініціативу Співтовариства шляхом створення «Зеленої книги», згідно з якою Ініціатива Співтовариства включена до 11 сфер[22]. Пізніше Директива 114 Європейської Комісії від 2008 року визначила лише два сектори як пріоритетні: енергетика (електромережі та станції для виробництва та передачі електроенергії; нафтовидобувна та переробна промисловість, трубопроводи та зберігання нафти; газовидобувна промисловість, газопроводи, скраплений газ). АЗС) і транспорт (автомобільний транспорт; залізничний транспорт; повітряний транспорт; річковий флот; океанський і морський флот).

При визначенні елементів КІ будується ієрархія критеріїв, яка включає такі основні групи: фінансова забезпеченість (значна частка продукту на ринку, велика кількість працівників, великий платник податків); безпека життя та здоров'я мешканців (забезпечення роботи аварійно-рятувальних формувань, невідкладна допомога мешканцям; запобігання техногенним аваріям на

регіональному чи національному рівнях); безпеки і оборони держави (недопущення порушень державного управління, зниження боєздатності збройних сил, розголошення секретної інформації); самоповага та державний імідж нації (збереження культурних цінностей, державної влади).

Відповідно до прийнятого ним порядку встановлено такі категорії компонентів критичної інфраструктури:

У категорії критичних - особливо важливі питання державного значення, значний вплив на інші ланки критичної інфраструктури та порушення їх роботи призводить до кризи загальнодержавного значення;

ІІ критична категорія – важливі питання, невиконання яких спричиняє кризову ситуацію регіонального значення;

Критична категорія ІІІ – товари першої необхідності, якщо їх несправність призводить до кризи локального значення;

Критична категорія IV – істотні проблеми, які не призводять до кризової ситуації локального значення.

Уповноважені сторони:

Перелік галузей (підсекторів) визначає основні послуги критичної інфраструктури, компоненти критичної інфраструктури галузей (підсекторів) критичної інфраструктури;

Їхні сектори (підсектори) критичної інфраструктури, а також оператори базових послуг здійснюють класифікацію компонентів критичної інфраструктури відповідно до методу класифікації компонентів критичної інфраструктури.

Уповноважені особи вносять інформацію про створені та обслуговувані ними об’єкти критичної інфраструктури, віднесені до І, ІІ, ІІІ та IV категорій пріоритету.

Відомості про важливі об’єкти інфраструктури, які містяться в Державному реєстрі важливих об’єктів інфраструктури та у польових переліках важливих об’єктів інфраструктури, є обмежено доступною інформацією, охорона якої гарантується відповідно до вимог закону про сферу охорони даних.

Критична інфраструктура – це об’єкти та послуги, життєво важливі для основних операцій суспільства. Сектори, які вважаються «критично важливою інфраструктурою», відрізняються в різних країнах, але більшість із них включає: енергетику, воду, продовольство, транспорт, телекомунікації, охорону здоров’я, а також банківську справу та фінанси. Однак загальновизнаного визначення не існує, оскільки кожна країна визначає його на основі національних пріоритетів. Багато країн мають національні стратегії захисту своєї критичної інфраструктури від природних і антропогенних ризиків, таких як кіберзагрози.

Доступ і доступність критично важливих інфраструктур, таких як енергетика, є важливими для розвитку, але суттєво відрізняються між країнами. Наприклад, у Німеччині 100 відсотків населення має доступ до безпечних служб питної води, тоді як у 2022 році 2,2 мільярда людей у всьому світі не мали безпечної питної води. Ця цифра свідчить про те, що в країнах, що розвиваються, залишаються значні проблеми. Однак серйозні збої також можуть виникнути в країнах з високонадійними інфраструктурними системами [40].

Критична інфраструктура охоплює всі активи, системи та мережі (як фізичні, так і віртуальні), які є життєво важливими для належного функціонування економіки суспільства, національного здоров’я чи безпеки, безпеки чи будь-якої комбінації цих факторів. Це широке визначення включає різні сектори, важливі для підтримки добробуту та безпеки нації.

Приклади секторів критичної інфраструктури можуть включати [32]:

Харчування та сільське господарство

Транспортні системи (наприклад, дороги, залізниці, шосе, аеропорти)

Інтернет і мобільні мережі

Критична інфраструктура має важливе значення для задоволення основних життєвих потреб, і хоча вона має схожість у різних країнах, конкретна інфраструктура, яка вважається критичною, може відрізнятися залежно від унікальних потреб нації, ресурсів і рівня розвитку. У Сполучених Штатах велика

частина цієї фізичної та кіберінфраструктури належить і управляється приватним сектором, хоча деяка частина належить федеральним, державним або місцевим органам влади.

Згідно з постановою Кабінету Міністрів України від 09.05.2023 р. N 455, до секторів критичної інфраструктури входять [27]:

1. Паливно-енергетичний сектор:

1) електроенергетика;

2) вугільно-промисловий комплекс;

3) торфодобування;

4) нафтова промисловість;

5) газова промисловість;

6) ядерна енергетика;

7) енергетичне машинобудування.

2. Цифрові технології:

1) електронні довірчі послуги та електронна ідентифікація

2) електронні комунікації

3) електронне урядування

3. Захист інформації

4. Харчова промисловість та агропромисловий комплекс

5. Державний матеріальний резерв

6. Охорона здоров'я

1) медична допомога

2) громадське здоров'я

3) фінансове забезпечення у сфері охорони здоров'я

4) інформаційні технології у сфері охорони здоров'я

5) фармацевтична промисловість

7. Ринки капіталу та організовані товарні ринки

8. Фінансовий сектор

9. Транспорт і пошта

1) авіаційний транспорт

2) автомобільний та міський електричний транспорт

3) метрополітен

4) залізничний транспорт

5) морський та внутрішній водний транспорт

6) поштовий зв'язок

10. Системи життєзабезпечення (комунальні послуги)

11. Промисловість

1) хімічна промисловість

2) металургійна промисловість

3) оборонна промисловість

4) космічна промисловість

5) авіаційна промисловість

6) суднобудівна промисловість

12. Сектор громадської безпеки

1) громадська безпека

2) екстрена допомога населенню за єдиним телефонним номером 112

13. Цивільний захист населення і територій (атестовані аварійно-рятувальні служби згідно із законодавством)

14. Охорона навколишнього природного середовища

1) управління, використання та відтворення поверхневих водних ресурсів, розвиток водного господарства

2) поводження з радіоактивними відходами

3) охорона, раціональне використання і відтворення об'єктів природно-заповідного фонду

15. Сектор оборони (зберігання ракет, боєприпасів та вибухових речовин)

16. Правосуддя

17. Виконання кримінальних покарань, тримання під вартою та утримання військовополонених

18. Державна реєстрація (інформаційні технології у сфері державної реєстрації)

19. Наукові дослідження та розробки (дослідницька інфраструктура наукових установ та закладів вищої освіти)

20. Фінансовий сектор

1) банківська система

2) ринок небанківських фінансових послуг (крім ринків капіталу та організованих товарних ринків)

3) ринок платіжних послуг

21. Вибори та референдуми

22. Соціальний захист

1) пенсійне забезпечення

2) соціальне страхування

3) соціальна допомога і соціальні послуги

4) інформаційна система соціальної сфери

5) реабілітація

23. Інформаційний сектор (медіа)

24. Державна влада та місцеве самоврядування

У Європі сектори критичної інфраструктури визначаються Європейською програмою захисту критичної інфраструктури (EPCIP), яка узгоджується з ЄС COM(2006) 786. У Сполученому Королівстві політика та готовність до критичної інфраструктури контролюються Національним захисним органом безпеки (NPSA) [23].

Хоча активи та регуляторні ландшафти можуть відрізнятися, між членами Організації економічної координації та розвитку (OECP) існує широкий консенсус щодо спільних секторів критичної інфраструктури, політики та слабких рамок. Ця угода підкреслює спільне визнання важливості захисту критичної інфраструктури, незважаючи на різноманітні активи та зміну нормативних вимог у різних країнах.

Відповідність відіграє вирішальну роль у сфері критичної інфраструктури, де уряди та регулюючі органи втручалися, щоб встановити керівні принципи та мандати, спрямовані на забезпечення практики кібербезпеки. Три важливих

нормативних акта: Директива ЄС-NIS (Мережі та інформаційні системи Європейського Союзу), DFARS (Додаток щодо федеральних закупівель для оборони) і NERC-CIP США (Захист критичної інфраструктури Північноамериканської корпорації з електричної надійності) мають глобальні наслідки для критичної інфраструктури [17].

Директива EU-NIS, запропонована в 2013 році та прийнята в серпні 2016 року, спрямована на досягнення високого загального рівня кібербезпеки для критичної інфраструктури в країнах-членах Європейського Союзу. Він встановлює цілі щодо покращення національних можливостей кібербезпеки, посилення співпраці між державами-членами та зобов'язує операторів основних послуг (OES) і постачальників цифрових послуг (DSP) вживати відповідних заходів безпеки. Під його дію входять такі організації, як постачальники електроенергії, транспорту, води, енергії, охорони здоров'я та послуг цифрової інфраструктури. Невиконання вимог може призвести до значних штрафів.

У Сполучених Штатах промисловість критичної інфраструктури підлягає галузевому саморегулюванню або державним нормам, специфічним для кожного сектора. NERC CIP, зосереджена на кібербезпеці, виділяється більш ніж 100 стандартами та вимогами щодо захисту критично важливих інфраструктурних активів у великих електричних системах країни. Недотримання стандартів NERC CIP може призвести до значних санкцій, із можливістю штрафу до 1 мільйона доларів США на день за кожне порушення. Доступність системи має пріоритет, впливаючи на вибір технологій і методів кібербезпеки, які використовуються в критичних інфраструктурах [11].

Міністерство оборони (DoD) США наголошує на захисті федеральної інфраструктури, вимагаючи від усіх підрядників, які обробляють, зберігають або передають контрольовану несекретну інформацію (CUI), дотримання мінімальних стандартів безпеки DFARS. NIST 800-171 забезпечує основу для компаній, які ведуть бізнес з Міністерством оборони, щоб захистити CUI. Дотримання вимог має вирішальне значення для виконання контрактів

Міністерства оборони, оскільки воно становить значну частину річного доходу багатьох компаній [7].

1.2 Загрози та ризики для об'єктів критичної інфраструктури

Дослідження UNU-EHS показує, що функціонуюча інфраструктура — це більше, ніж просто наявність технологій та обладнання. Йдеться також про людей, які керують інфраструктурою, а також про їхні потужності та доступ до робочих місць у разі катастрофи. Наприклад, під час пандемії лікарням та іншим критично важливим медичним закладам було важко працювати. Персонал не міг дістатися до своїх робочих місць через закриті кордони або сімейні зобов’язання, оскільки школи були закриті. Стійкість інфраструктури повинна враховувати не лише фізичне оновлення об’єктів, а й тих, хто в них працює [1].

Критична інфраструктура стикається з новими загрозами, які можуть зруйнувати її роботу та створити загрозу громадській безпеці та економічній стабільності. Розширені загрози включають:

- Кібератаки

Зловмисники можуть атакувати системи керування, мережі та вразливі місця програмного забезпечення, щоб отримати несанкціонований доступ, порушити роботу, викрасти конфіденційну інформацію або завдати фізичної шкоди.

- Фізичні атаки [2]

Саботаж, тероризм або вандалізм можуть безпосередньо пошкодити об'єкти, перервати роботу та поставити під загрозу життя. Ці атаки можуть бути спрямовані на комерційні об’єкти, транспортні системи, критичні виробничі операції чи інші активи.

- Стихійні лиха

Урагани, землетруси, повені, лісові пожежі та суворі погодні явища можуть порушити роботу основних служб. Системи, засновані на історичних

кліматичних моделях, можуть зіткнутися з проблемами через збільшення частоти та інтенсивності екстремальних погодних явищ.

- Пандемії та надзвичайні ситуації у сфері охорони здоров'я [18]

Пандемії та спалахи захворювань можуть спричинити нестачу робочої сили, збої в роботі та підвищення попиту на медичні послуги, що може негативно вплинути на служби охорони здоров'я та загальну стійкість системи.

- Вразливості ланцюга поставок

Уразливі місця в ланцюжку постачання, такі як скомпрометовані або підроблені продукти, можуть створити слабкі місця, які можуть бути використані для порушення операцій або порушення цілісності системи.

- Технологічні залежності [33]

Оскільки критична інфраструктура стає все більш взаємопов'язаною та залежить від передових технологій, залежність від складних систем і програмного забезпечення зростає.

Забезпечення захисту критичної інфраструктури потребує комплексного підходу, включаючи надійні заходи кібербезпеки, плани готовності до стихійних лих і реагування на них, стійку конструкцію інфраструктури, безпеку ланцюга постачання, державно-приватну взаємодію, постійний моніторинг та оцінку ризиків.

Слід зазначити, що провідні країни світу виходять з необхідності забезпечення захисту критичної інфраструктури від усіх видів загроз. У той же час, завдяки усвідомленню можливості високого рівня захисту всієї критичної інфраструктури від усіх можливих загроз, підхід до безпеки був зосереджений на «вибірковому захисті конкретного об'єкта CI від обмеженої кількості».

Наказ 648/2012 пов'язаний з деякими відомими та відносно передбачуваними загрозами в Європейській економічній зоні, в якому визначені пріоритети певної інфраструктури відповідно до рівня «критичності» та зосереджено головним чином на ризиках [3].

Існують різні методи визначення ризику1. Проте загальний підхід до оцінки ризику КІ включає [8]:

- ідентифікацію та класифікацію загроз, оцінку ймовірності (точніше частоти) кожної загрози;

- оцінка вразливості будь-якого виду небезпеки/атаки (визначення ймовірності пошкодження з урахуванням частоти небезпеки);

- оцінка наслідків (виправданий песимістичний сценарій).

Слід зазначити, що навіть якщо визначений підхід, заснований на оцінці ризику, використовується для управління безпекою людини та навколишнього середовища, не завжди можливо адекватно виміряти та порівняти ризики з СІ. Це пов'язано з невизначеністю, зокрема неточністю та недостатньою інформацією, необхідною для правильної оцінки частоти загроз (що є найвпливовішим фактором невизначеності терористичної загрози), а також багатовимірністю та характером доступних варіантів. а також наслідки [4].

Крім того, ключовим аспектом оцінки ризику ІС є необхідність брати до уваги численні взаємозв'язки та взаємозалежності, які можуть бути чіткими (залежними від діяльності) і неоднозначними (наприклад, під час визначення (стан інформації системи, функціонування системи). Це вимагає використання інших методів, у тому числі методів нечіткої логіки та експертних оцінок [6].

З іншого боку, коли ми говоримо про захист штучного інтелекту, постає питання не лише «як захищати», а й «як захищати»: об'єкт чи діяльність? Слід зазначити, що існує різниця в захисті цих елементів КІ, оскільки у випадку з об'єктами він в основному спрямований на зниження ризику та вразливості об'єктів, мінімізацію наслідків, а у випадку запасів – на зменшення рівня загрози та вразливості безперервність постачання і натомість відновлення у разі розривів [17].

Параметри оцінки критичності мають різний тип і описують вплив кризової ситуації на об'єкт КІ (її наслідки) з різних точок зору. Вони можуть бути представлені в якісній або кількісній формі [6]. Для визначення параметрів оцінки на критичному рівні використовуються фактори і характеристики, зазначені в Зеленій книзі [2], яка використовується в більшості країнах [18].

Зелена книга [2], яка враховує Директиву 2008/114/ЄС, визначає необхідність аналізу таких характеристик:

- їх протяжність (географічна протяжність територій, де втрата елемента, завдає значної шкоди, була пов’язана з критичною інфраструктурою);

- зв'язки між критичними компонентами інфраструктури;

- тривалість впливу (як і коли саме збиток пов'язаний із втратою або несправністю критичної інфраструктури, несправністю або порушенням роботи);

- чутливість об'єкта до дії небезпечних факторів;

- тяжкість можливих наслідків за показниками таких основних груп:

- економічна безпека (вплив на ВВП, розмір прямих і непрямих економічних втрат, частка продукції на ринку, чисельність працівників, податкові надходження до бюджету);

- безпека життя та здоров'я населення (кількість постраждалих, загиблих, важкопоранених та евакуйованого населення, забезпечення роботи аварійно-рятувальних формувань, надання екстреної допомоги населенню);

- внутрішньополітична та державна безпека (втрата довіри до ефективності влади, органів державної влади, порушення державного управління);

- обороноздатність (зниження боєздатності збройних сил, розголошення секретних даних);

- екологічна безпека (вплив на природне середовище).

Так, в Ізраїлі ідентифікація об'єктів КІ враховує три критерії [21]:

- символічне значення (ідеологічні, історичні чи культурні об'єкти);

- залежність найважливіших процесів життєдіяльності суспільства від інфраструктури - складні взаємозв'язки та залежність від неї між інфраструктурними спорудами.

Слід зазначити, що культурна спадщина Ізраїлю (музеї, архіви, релігійні об'єкти та інші місця) є пріоритетною. А у США зачинили свої двері близько 33 тисяч закладів. в національній базі даних критичного аналізу, з яких приблизно 2000 класифікуються як критичні інфраструктури [9].

Ці об’єкти поділяються на три категорії:

- копалини (атомні електростанції, гідроелектростанції та великі гідроелектростанції, стратегічні сховища нафти та газу, небезпечні хімічні та нафтохімічні виробництва, сховища ядерних матеріалів та боєприпасів);

- водні (водогони, метрополітен, системи водопостачання та каналізації, магістральні трубопроводи);

- зв'язок (порти, очисні споруди, автомобільні та залізні дороги, великі аеропорти, вузли зв'язку тощо).

Взагалі при оцінці критичності об'єкта в США його ступінь прийнято ділити на три категорії: високий, середній і низький. Слід зазначити, що методи управління безпекою, засновані на оцінці ризику, також використовуються в Сполучених Штатах, і, зокрема, що оцінка ризику оцінюється на основі експертної оцінки за п'ятибальною шкалою від слабкого до серйозного. Аналогічний метод використовується для визначення п’яти рівнів готовності: червоний (високий), помаранчевий (високий), жовтий (високий), синій (потенційний) і зелений (низький) [22].

Подібні характеристики використовуються для визначення можливих факторів ІК у США [9]:

- масштаб;

- взаємодія елементів інфраструктури;

- тривалість впливу;

- час відновлення;

- ступінь можливих наслідків за такими основними групами:

- економіка;

- економічність;

- навколишнє середовище;

- безпека життя і здоров'я людей;

- технічне середовище.

Крім того, враховується символічне значення матеріалу, збиток, завданий обороноздатності країни, і можливі другорядні питання національної безпеки.

Цікавою є також методика класифікації частин американського військово-промислового комплексу – модель визначення пріоритетів військово-промислового комплексу (The Asset Priority Model) [10]. Усі елементи ранжуються за 16 факторами, зваженими від 16 до 1 і «важливістю» від 1 до 3 (іноді 5), і розраховується загальний індекс ризику.

Ці фактори враховують вплив на плани великомасштабного виробництва, боєздатність (величину виробництва), фінансову спроможність підприємства, економічну життєздатність, потенціал відновлення, кількість людей, які проживають поблизу, побічний збиток, спричинений хімічними/біологічними впливами. хімічні речовини, що використовуються для нападів/радіація та вибухові речовини тощо. Варто також зазначити, що з 2007 року найважливіші об'єкти були визначені як найважливіші об'єкти управління великими виробничими програмами військової промисловості, а раніше вони вважалися найбільш вражаючими в сучасній промисловості.

1.3 Сучасні підходи до підвищення стійкості об'єктів критичної інфраструктури

Питання удосконалення діяльності сектору безпеки України також стало актуальним як у теоретичній, так і практичній площині. На сьогодні постало питання застосування принципово нових методів та інструментів діяльності сектору безпеки, що і зумовлює питання прийняття Концепції його реформування. При цьому, суттєвий вплив на процес трансформації завдань для сектору безпеки і оборони здійснюють кращі світові сучасні підходи щодо забезпечення національної стійкості, зокрема захист критичної інфраструктури [4].

Саме тому, на сьогодні, у процесі є реформування сектору безпеки необхідно проаналізувати пріоритетні напрями уточнення функцій та повноважень державних органів сектору безпеки виходячи із сучасних концепцій забезпечення національної стійкості. Концепція захисту критичної

інфраструктури в системі забезпечення національної стійкості. Слід відзначити, що «вимушеність» реформування сектору безпеки в Україні внаслідок неготовності до гібридної війни не є унікальним недоліком країни. Зміни в пріоритетах системи забезпечення національної безпеки внаслідок подій, які демонструють неадекватність діючої на визначений час системи, траплялись в інших країнах також. Зокрема відзначимо події 2001 та 2005 років, які суттєво вплинули на становлення концепції захисту критичної інфраструктури у світі. Саме у відповідь на трагічні події 11 вересня 2001 року в Нью-Йорку у США, на доповнення до Стратегії національної безпеки США була розроблена та затверджена Національна стратегії внутрішньої безпеки (липень 2002 р.) завданням якої була мобілізація та організація американського суспільства для цілей захисту [28].

Усвідомлення зростання терористичних загроз (атака на транспортній інфраструктурі Іспанії в 2004 році) зумовили активізацію дій і в ЄС. Європейська Комісія розробила та у листопаді 2005 р. оприлюднила Зелену книгу щодо Європейської програми захисту критичної інфраструктури, а згодом (2006 р.) була прийнята Європейська програма захисту критичної інфраструктури [14]. Особливості підходу ЄС, як об'єднання суверенних держав, у подальшому знайшли своє відображення у Директиві 2008/114/ЕС щодо визначення об’єктів критичної інфраструктури та оцінки потреб у підвищенні рівня їхнього захисту (2008 р.).

Стратегія національної безпеки України (2015 року), поряд із завданнями реформування сектору безпеки, також визначає захист критичної інфраструктури (ЗКІ) у якості пріоритетного напряму безпекової політики. У свою чергу, оновленні доктринальні і концептуальні документи сектору безпеки і оборони України (Воєнна доктрина України, Концепція розвитку сектору безпеки і оборони України, Стратегія кібербезпеки України) формують завдання щодо реалізації цього напряму державної політики. У розвиток Стратегії національної безпеки, Національним інститутом стратегічних досліджень розроблено Зелену Книгу з питань захисту критичної

інфраструктури, яка розкриває теоретично-методологічні засади формування державної системи ЗКІ та окреслює пріоритети системи державної влади у цій сфері [5].

Концепція захисту критичної інфраструктури держави дає можливість сформувати необхідну базу для функціонування спеціального правоохоронного органу держави відповідно до сучасних теоретичних засад та кращої світової практики. Та перш ніж перейти до детальнішого аналізу пріоритетів удосконалення нормативно-правової бази діяльності сектору безпеки з питань забезпечення ЗКІ слід поглянути на роль КІ для забезпечення національної безпеки, а також місце та роль сектору безпеки у забезпеченні стійкості функціонування суспільства та держави з системних позицій. Системний підхід до визначення предмету діяльності сектору безпеки у сфері захисту критичної інфраструктури.

Для кращого розуміння публікації наведемо ряд визначень, що визначають зміт діяльності у сфері захисту критичної інфраструктури: Критична інфраструктура (КІ) – системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки; критичність – це відносна міра важливості даної інфраструктури, що враховує вплив раптового припинення її функціонування, або функціонального збою на безпеку постачання, тобто забезпечення суспільства важливими товарами і послугами [39].

Захист КІ – всі види діяльності, спрямовані на забезпечення функціональності, безперервності та цілісності критичної інфраструктури з метою недопущення, пом'якшення та нейтралізації загроз, ризиків та вразливостей. Загрози КІ – чинники які потенційно можуть призвести до припинення КІ виконання функцій та надання послуг. Безпека критичної інфраструктури - стан критичної інфраструктури, коли дія зовнішніх та внутрішніх чинників не призводить до аварій чи інших порушень її

функціонування; стійкість інфраструктури – здатність надійно функціонувати у нормальному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після аварій та технічних збоїв, зловмисних дій, природних лих та небезпечних природних явищ.

Категорія «безпека» нерозривна із категорією «суб'єкт», оскільки саме явище безпеки є рефлексією суб'єкта; суб'єкт існує на матеріалі «об'єкта», і лише існування матеріалу у визначеній формі та якості гарантує існування суб'єкта та визначає його «безпеку»; суб'єкт завжди «охоплює» об'єкт, тобто усвідомлює можливості та має інструменти підпорядкування об'єкта і, тим самим, управляє ним (забезпечує його «розвиток» і «безпеку») [15].

Якщо суб'єкт на має впливу на ту чи іншу частину об'єкта, він не є суб'єктом для цієї частини; глобалізація обумовлює конкуренцію «суб'єкт–об'єктних» системних утворень та проблеми їх взаємовідносин. При конкуренції виграє той із суб'єктів, хто перетворив конкурента на свій об'єкт оперування, здійснюючи тим самим вплив на процеси, які відбуваються в його «суб'єкт–об'єктній» системі; суб'єкт визначає безпечність існування через оцінку свого місця та ролі в навколишньому середовищі, також конкурентних переваг над іншими суб'єкт-об'єктними системами.

Враховуючи основні положення концепції захисту критичної інфраструктури, предметом діяльності сектору безпеки має стати – визначення, аналіз та оцінка ефективності застосування методів та інструментів впливу однієї системи на іншу (однієї країни на іншу), а також розробка методів та інструментів запобігання, стримування, нейтралізації або пом'якшення наслідків такого впливу та сприяння посиленню готовності, своєчасного реагування та швидкого відновлення штатного режиму функціонування системи.

Для подальшого уточнення предмету діяльності сектору безпеки слід додатково відзначити ряд важливих позицій [34]:

- у сучасному глобалізованому світі методи та інструменти впливу постійно змінюються (поява методів «гібридної війни»), що потребує відповідно реагування з боку системи безпеки, а саме постійної своєрідної

«інвентаризації» зазначених методів та інструментів, перевизначення їх предмету та механізму дії;

- предмет діяльності та механізми впливу суб'єкта визначаються ідентифікацією основних процесів життєдіяльності окремої «суб'єкт-об'єктної» системи (на визначеному проміжку її життєдіяльності), на які спрямовані зазначені впливи;

- структурно-функціональне відображення основних процесів, в рамках методології системного підходу, є критичної інфраструктурою (КІ) життєдіяльності «суб'єкт-об'єктної» системи;

- загрози стійкості функціонування КІ системи є фактично загрозами національної безпеки.

Введенні «процеси», які є визначальними для подальшого аналізу, потребують додаткового розкриття. Розкриття об'єкта як системи, з виділенням, поряд із традиційними складниками (елементи, зв'язки, структура), також її матеріального та процесуального складників дає змогу зняти ряд недоліків існуючого підходу.

Необхідність розширення змісту категорії «система» за рахунок включення «процесуальності» існування системи, де поряд із такими складниками категорії «система», як «елемент», «структура», «функція», враховується «матеріал» і «процеси» системи, обґрунтовано у роботах багатьох дослідників [38].

Хоча у знаковій формі показати процеси життєдіяльності системи досить важко, їх «схоплення» суб'єктом дослідження (управління) є дуже важливим, оскільки саме процеси функціонування системи визначають предмет управлінської діяльності. Саме виділення процесів, дозволяє подолати неадекватний сьогоденню підхід щодо акценту на статичному стані системи через виділення набору окремих індикаторів та їх цільових значень (переліків об'єктів захисту, фізичної охорони, наявності ресурсів визначеного обсягу тощо) та внести в управлінську діяльність необхідність врахування динаміки системи.

У свою чергу, врахування динаміки дозволяє виходити на проектування «майбутнього» системи, задачу формування конкурентних переваг у конкурентній боротьбі «суб'єкт-об'єктних систем». Виділення процесів, дозволяє акцентувати увагу на адаптації системи, тобто спроможності перебудувати структуру зв'язків та змінити властивості елементів системи відповідно до нових вимог середовища. Саме до такого ж висновку прийшло розвідувальне співтовариство США, яке у доповіді Національної Розвідувальної Ради (National Intelligence Council) наголошує що в умовах несформованого глобального ландшафту, багатого сюрпризами і різкими змінами, найбільш пристосованими до використання таких можливостей будуть стійкі держави і організації, що дозволить їм адаптуватися до умов, що змінюються, витримувати вплив несподіваних несприятливих факторів і вживати заходів для швидкого відновлення. Вони будуть вкладати кошти в інфраструктуру, знання і відносини, які дозволять їм витримувати потрясіння - економічні, екологічні, соціальні або кібернетичні.

РОЗДІЛ 2. ПРАКТИЧНІ АСПЕКТИ ПІДВИЩЕННЯ СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Аналіз існуючого стану захищеності об'єктів критичної інфраструктури в Україні

Враховуючи сучасні виклики та загрози, які можуть виникнути внаслідок стихійних лих, кібератак, терористичних загроз чи геополітичних конфліктів, захист критичної інфраструктури є важливим завданням для забезпечення національної безпеки країни.

Закони та нормативні акти, пов’язані з безпекою критичної інфраструктури, визначають стандарти безпеки, зобов’язання власників і користувачів об’єктів, а також методи реагування на потенційні загрози.

15 грудня 2021 року набув чинності дуже важливий закон про «критичну інфраструктуру». Закон визначає правові та організаційні основи створення та функціонування критичної інфраструктури та є частиною законодавства України у сфері національної безпеки. Він містить базові визначення та разом із ухваленими постановами Ради Міністрів України є основою комплексного захисту критичної інфраструктури [12].

Аспекти захисту об’єктів критичної інфраструктури в умовах надзвичайного та воєнного стану, особливого часу, регулюються Законами України «Про правову систему про надзвичайні ситуації», «Про правову систему про надзвичайні ситуації», «Про правову систему надзвичайних ситуацій», «Функціонування єдиної транспортної системи України в особливий час» та «Про оборону України «Спеціальний закон про забезпечення кіберзахисту та кібербезпеки критичної інфраструктури», який ґрунтується на таких принципах:

1) визнання необхідності забезпечення безпеки та стабільності критичної інфраструктури,

2) принципи захисту критичної інфраструктури, визначення завдань та стратегічних підходів,

3) визначення послідовності суб'єктів у національній системі захисту критичної інфраструктури, свої повноваження та принципи відповідальності,

4) створюють умови та впроваджують заходи для ефективного зменшення та управління ризиками безпеки, зменшення ризику того, що потенційні загрози стануть реальністю, усунення та/або мінімізації наслідків реалістичних загроз, криз та інших їх форм,

5) створити інфраструктуру; системи раннього виявлення загроз критичній інфраструктурі,

6) забезпечує міжнародне співробітництво у сфері захисту критичної інфраструктури,

7) створити умови для швидкого відновлення постачання важливих функцій і важливих послуг у разі виникнення загроз і збоїв у роботі критичної інфраструктури [35].

Глобальні тенденції до посилення природних та техногенних загроз, зростання терористичних загроз, зростання кількості та складності кібератак, а також пошкодження інфраструктури на сході та півдні України, а також наслідки збройного нападу Російської Федерації призвела до руйнування систем, засобів, необхідних для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки та реального захисту ресурсів [19].

Тому метою державної політики у сфері захисту важливих об'єктів інфраструктури є забезпечення безпеки важливих об'єктів інфраструктури, запобігання несанкціонованому втручанню в їх роботу, передбачення та запобігання небезпечним ситуаціям на важливих об'єктах інфраструктури.

Серед завдань щодо розроблення та реалізації державної політики у сфері захисту критичної інфраструктури є [16]:

1) запобігання несанкціонованому втручанню в її роботу, прогнозування та запобігання небезпечним ситуаціям на об'єктах критичної інфраструктури;

2) запобігати небезпечним ситуаціям, які ставлять під загрозу безпеку критичної інфраструктури;

3) створює, запроваджує, розвиває та забезпечує національну систему захисту критичної інфраструктури, у тому числі визначення уповноваженого органу у сфері захисту критичної інфраструктури в Україні, а також визначення компетенції у сфері захисту критичної інфраструктури від інших Інфраструктура. зміст національної системи захисту критичної інфраструктури;

4) розробити нормативно-правову та нормативно-технічну базу для забезпечення безпеки об'єктів критичної інфраструктури;

5) розробляє та реалізує загальнодержавні цільові програми захисту критичної інфраструктури;

6) розробити комплекс заходів щодо управління ризиками безпеки та виявлення, запобігання та усунення наслідків збоїв у безпеці критичної інфраструктури;

7) визначає обов'язкові умови для забезпечення безпеки критичних частин інфраструктури, їх безпеки на всіх етапах життєвого циклу, у тому числі під час створення, введення в експлуатацію та модернізації;

8) аналіз викликів і загроз, що впливають на стабільність критичних інфраструктур, оцінка безпекової ситуації;

9) розробляє методологію аналізу ефективності державної політики у сфері захисту критичної інфраструктури;

10) підготовка, перепідготовка, підвищення кваліфікації та навчання персоналу національної системи захисту критичної інфраструктури;

11) забезпечує взаємодію національної системи захисту життєво важливої інфраструктури з відповідними міжнародними системами, зокрема європейською та євроатлантичною.

З метою врегулювання захисту розроблено окремі загальнодержавні рівні захисту, які набрали чинності на загальнодержавному рівні та адмініструються уповноваженим органом у сфері захисту критичної інфраструктури України Радою Міністрів України, державні органи відповідно до розподілу повноважень згідно із Законом «Про критичну інфраструктуру України», інші органи та установи державної виконавчої влади, Центральний банк України. Кожен рівень

був поділений на окремі сектори, від регіонального рівня до рівня контролю міжнародних установ.

Згідно з розпорядженням Кабінет Міністрів України від 19 вересня 2023 р. № 825-р «Національний План захисту та забезпечення безпеки та стійкості критичної інфраструктури» включає в себе [13]:

Мета 1. Правовий нагляд за діяльністю суб'єктів національної системи охорони важливих об'єктів інфраструктури.

1. Удосконалити законодавство, що регулює діяльність суб'єктів системи захисту критичної інфраструктури:

1) визначає умови, зміст і терміни процесу створення перепустки безпеки для важливих інфраструктурних цілей для банків, інших юридичних осіб, які здійснюють діяльність на ринку фінансових послуг з державним наглядом та здійснюють діяльність під наглядом Центрального банку, платіжних компаній, учасників; в платіжних системах, операторах послуг платіжної інфраструктури;

2) покращити процес моніторингу рівня безпеки для об'єктів критичної інфраструктури;

3) удосконалити порядок віднесення важливих об'єктів інфраструктури та методику класифікації важливих об'єктів інфраструктури;

4) утворити Міжвідомчу комісію з питань захисту критичної інфраструктури при Раді Міністрів України;

5) готує проекти програмних документів щодо забезпечення безпеки та стабільності критичної інфраструктури, здійснення їх захисту.

2. Встановлювати вимоги та контролювати рівень захисту критичної інфраструктури [29]:

1) створити та підтримувати план об'єктів критичної інфраструктури;

2) створення та ведення переліків об'єктів критичної інфраструктури;

3) готує пропозиції щодо внесення об'єктів інфраструктури до реєстру важливих об'єктів інфраструктури;

4) видає заяви про внесення відомостей про створення об'єктів критичної інфраструктури до реєстру об'єктів критичної інфраструктури;

5) готує та затверджує пропуски для охорони об’єктів критичної інфраструктури;

6) погодження перепусток безпеки для встановлення критичної інфраструктури;

7) розробити та посилити вимоги, стандарти та правила для захисту критичної інфраструктури;

8) розробляє, оновлює та надає цільові плани заходів із забезпечення безпеки та стабільності критичної інфраструктури, правила управління ризиками безпеки, плани розміщення та утилізації наслідків аварій та заходів із забезпечення безпеки мережі;

9) створити будівельні блоки для захисту критичної інфраструктури;

10) утворити спеціальний організаційний підрозділ або призначити особу, яка буде відповідати за планування охорони важливої інфраструктури та забезпечувати постійний зв’язок з відповідними суб’єктами національної системи захисту важливої інфраструктури;

11) видає рекомендації щодо визначення умов забезпечення захисту та стабільності сектору критичної інфраструктури відповідно до категорій об’єктів критичної інфраструктури;

12) надає рекомендації операторам критичної інфраструктури щодо захисту критичної інфраструктури та обов’язкових умов для усунення причин та умов, що послаблюють стійкість критичної інфраструктури;

13) здійснювати моніторинг рівня безпеки критичної інфраструктури;

14) погоджує плани контролю за рівнем безпеки важливих об'єктів інфраструктури;

15) розробляє критерії оцінки стану безпеки об’єктів критичної інфраструктури, їх показники та методи оцінки стану безпеки об’єктів критичної інфраструктури;

16) розробляє та затверджує умови охорони важливих споруд.

3. Контролювати дотримання правових вимог і звітувати про захист критичної інфраструктури [20]:

1) готує та подає щорічний звіт щодо забезпечення захисту об’єктів критичної інфраструктури на території, що викликає загрозу;

2) готує та подає щорічний звіт про виконання повноважень, визначених Законом «Про критичні інфраструктури України»;

3) Міністр України поінформував про стан виконання закону про критичну інфраструктуру України.

Мета 2. Створити систему координації та комунікації між людьми, які є суб’єктами національної системи захисту критичної інфраструктури [31].

1. Удосконалити порядок взаємодії суб’єктів національної системи захисту критичної інфраструктури:

1) підготувати план взаємодії суб’єктів національної системи захисту критичної інфраструктури;

2) перевірка плану взаємодії суб’єктів системи захисту критичної інфраструктури;

3) організовує взаємодію між суб’єктами національної системи охорони життєво важливої інфраструктури з використанням системи центру охорони життєво важливої інфраструктури;

4) у разі необхідності утворює консультативні ради з питань захисту критичної інфраструктури за участю експертів із захисту критичної інфраструктури.

2. Реалізація планів взаємодії суб’єктів системи захисту критичної інфраструктури на національному рівні для забезпечення сталості надання критичних функцій та/або послуг [37]:

1) розробляє та затверджує у відповідних областях плани зв’язку та обслуговування критичних функцій і послуг у ситуаціях порушення критичної інфраструктури;

2) розробляє та затверджує регіональні та галузеві плани та плани боротьби із загрозами для критичної інфраструктури, включаючи плани дій у надзвичайних ситуаціях, плани дій у надзвичайних ситуаціях, плани взаємодії,

плани відновлення об’єктів критичної інфраструктури, плани підготовки та тренування;

3) готує та затверджує плани взаємодії установ, що здійснюють діяльність у сфері захисту критичної інфраструктури, у сферах, актуальних для всіх завдань життєво важливої інфраструктури.

3. Удосконалення процедур обміну інформацією між учасниками національної системи захисту критичної інфраструктури у разі порушення роботи компонентів критичної інфраструктури:

1) здійснює заходи щодо забезпечення ефективності системи інформаційного обміну та зв’язку відповідних секторів критичної інфраструктури між суб’єктами національної системи захисту критичної інфраструктури;

2) удосконалити систему інформаційного обміну між суб’єктами національної системи захисту життєво важливої інфраструктури.

Мета 3. Впровадити управління ризиками критичної інфраструктури [30].

1. Оцінка ризиків і загроз для критичної інфраструктури:

1) оцінка загроз критичній інфраструктурі на національному рівні та оцінка загроз національній безпеці, викликаних загрозами критичній інфраструктурі;

2) підготовка пропозицій щодо ризиків та загроз для критичної інфраструктури на національному рівні та щорічних оцінок ризиків та загроз для критичної інфраструктури на національному рівні;

3) організовує оцінку загроз та небезпек, пов’язаних з критичною інфраструктурою у відповідних районах;

4) провести оцінку ризиків критичної інфраструктури;

5) створює бази даних загроз і вразливостей критичної інфраструктури.

2. Керувати рівнем захисту та розвиток здатності реагувати на загрози:

1) розробляти та впроваджувати критичні загрози інфраструктури у сфері промисловості;

2) розробляти та впроваджувати загрози місії, пов’язані з критичною інфраструктурою на рівні установки.

3. Розвивати спроможність учасників національної системи захисту критичної інфраструктури реагувати на нові загрози критичній інфраструктурі.

1) затверджує програми навчання для забезпечення стабільності та захисту критичної інфраструктури;

2) забезпечує захист персоналу критичної інфраструктури, планує та здійснює заходи щодо евакуації мешканців у разі виникнення надзвичайної ситуації;

3) організація проведення об'єднаних командних штабів, тактико-спеціальних навчань, спільних тренувань і курсів з охорони, охорони, запобігання злочинності, небезпечним ситуаціям та кібератакам.

Мета 4. Зміцнити стабільність важливої системи захисту інфраструктури на національному рівні [24]:

1. Розробити методи співпраці на місцях і на регіональному рівні в кризових ситуаціях, щоб забезпечити споживачів визначеним мінімальним рівнем надання важливих заходів та/або послуг: створювати та використовувати необхідні фінансові та матеріальні ресурси для реагування на і покласти край кризам, додають вони. їх наслідки.

2. Запровадимо систему постійного підвищення кваліфікації адміністраторів критичної інфраструктури:

1) підвищити комплекс знань, умінь та навичок працівників та керівників операторів критичної інфраструктури, які здійснюють діяльність із забезпечення безпеки об'єктів критичної інфраструктури та реагування на небезпечні інциденти на цих об'єктах;

2) проводити навчання та навчання, навчати та контролювати персонал, відповідальний за безпеку та захист критичної інфраструктури;

3) проводить науково-дослідну роботу щодо доповнення переліку знань і спеціальностей, за якими здобувають здобувачі вищої освіти, затвердженого постановою Ради Міністрів України № 266 від 29 квітня 2015 року з новим записом у цьому полі, забезпечити стабільність і захист інфраструктури.

3. Розробка найкращих практик для забезпечення безпечного середовища та мінімізації наслідків надзвичайної ситуації для критичної інфраструктури [26]:

1) готує та затверджує план роботи аварійно-рятувальних служб, протипожежної охорони та штучного захисту важливих споруд та огляд;

2) організація та забезпечення критичної протипожежної інфраструктури в порядку, визначеному Радою Міністрів України.

4. Розвивати спроможність муніципалітетів самостійно підтримувати мінімально важливі функції та/або важливі послуги:

1) розробляти та затверджувати місцеві плани щодо забезпечення безпеки та стабільності критичної інфраструктури, плани, спрямовані на підвищення стійкості муніципалітетів у кризових ситуаціях, що є наслідком призупинення або погіршення надання послуг, важливих для їх основної діяльності чи ефективності важливих заходів;

2) обговорювати, погоджувати та затверджувати плани з місцевими зацікавленими сторонами щодо відносин між сторонами в кризовій ситуації для підтримки критичних операцій і надання критичних послуг, планів відновлення роботи критичної інфраструктури;

3) приймає плани навчання населення за результатами погоджень з відповідними установами для забезпечення захисту у разі кризи та налагодження нормальної роботи системи;

4) визначити структуру, відповідальну за здійснення важливих заходів захисту інфраструктури з числа раніше створених.

5. Впровадження системи державної підтримки реалізації дій, спрямованих на підвищення стійкості населення у разі збоїв у роботі критичної інфраструктури: створення системи інформування населення та бізнесу на критичні періоди небезпеки та кризи об'єктыв інфраструктури [40].

Мета 5. Створення міжнародної співпраці

1. Взаємодія національних систем захисту критичної інфраструктури з відповідними міжнародними системами, переважно європейськими та євроатлантичними:

1) співробітництво у сфері захисту критичної інфраструктури з іноземними державами, їх правоохоронними органами та спеціальними службами, а також міжнародними організаціями для боротьби з міжнародною злочинністю і тероризмом;

2) розвивати міжнародне співробітництво з питань безпеки та стабільності критичної інфраструктури;

3) участь у здійсненні спільних дій, спрямованих на забезпечення захисту об'єктів критичної інфраструктури, у тому числі в організації спільної підготовки слухачів безпеки та оборони щодо спільного виконання захисних заходів відповідно до вимог законодавства України.

Регіональний рівні, у віданні яких визначені відповідно до закону центральні та місцеві органи влади, відповідають за формування та реалізацію державної політики у сфері захисту критичної інфраструктури у певній галузі та за окрему роботу систему захисту та реагування на критичний стан. Місцевий рівень, де управління здійснюють місцеві органи виконавчої влади (військово-цивільна адміністрація – у випадку організації), органи місцевого самоврядування в межах їх компетенції. Частковий рівень, яким керує оператор критичної інфраструктури на основі законодавчих і нормативних заходів, пов'язаних із захистом критичної інфраструктури.

Розподіл рівнів контролю затверджено статтею 7 Закону «Про критичну інфраструктуру України», яка визначила роль кожного рівня національного плану захисту. Об'єкти критичної інфраструктури на основі набору критеріїв, які визначають їх соціальне, політичне, економічне та екологічне значення для захисту країни, громадян, суспільства, державного та громадського порядку, особливо у правоохоронній сфері під час виконання життєво важливих завдань і послуг, щоб показати, що для них існує небезпека, що небезпечна ситуація може виникнути через несанкціоноване переривання операцій, переривання операцій,

людський фактор або стихійні лиха, періоди роботи щоб припинити ці наслідки до повного встановлення нормальної системи контролю.

Ці критерії включають [36]:

1) здійснення заходів, спрямованих на забезпечення важливих національних інтересів;

2) можуть виникнути виклики та загрози, пов’язані з критичною інфраструктурою;

3) ймовірність того, що це завдасть значної шкоди нормальним умовам життя населення.

Класифікація об’єктів критичної інфраструктури регулюється частиною 10 статті 262 Закону «Про критичну інфраструктуру України», яка визначає вимоги до забезпечення захисту об’єктів критичної інфраструктури за їх значенням у забезпеченні певних критичних функцій. у сфері критичної інфраструктури.

Організації у сфері захисту критичної інфраструктури бізнесу здійснюють класифікацію компонентів критичної інфраструктури відповідно до спеціалізацій, галузевих законодавчих вимог і чотирьох визначених категорій важливості та критичності компонентів. В Україні охорона об’єктів, віднесених до «критичної інфраструктури» згідно з міжнародними угодами, регулюється численними нормативно-правовими актами, які мають переважно внутрішньовідомчий характер.

Ситуація виникла закономірно: кожна окрема служба виявила певну загрозу для підлеглих їй інсталяцій і мала власні інструменти та ресурси для забезпечення їх безпеки. Таким чином, чинне законодавство України визначає низку речей, які підлягають особливим умовам охорони, зокрема підприємства, які мають стратегічне значення для економіки та безпеки держави; особливо важливі сектори в електроенергетиці та нафтогазовій промисловості; потенційно небезпечні об'єкти, об'єкти підвищеної небезпеки; об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони, а також об'єкти, що підлягають охороні в надзвичайних ситуаціях і протягом певного часу; для інших цілей і систем, таких як системи зв’язку, платіжні системи тощо [4].

Довгий перелік документів, що регулюють певні аспекти кібербезпеки, є результатом дублювання, неоднорідності, суперечностей і, подекуди, відсутності вимог кібербезпеки в окремих секторах критичної інфраструктури, що є причиною багатьох наступних випадків, зокрема великий перелік сфер/секторів критичної інфраструктури, давнє спеціальне законодавство та заходи щодо кіберзахисту критичної інфраструктури, відсутність вимог, а також чіткий перелік із уповноважених суб'єктів, перелік їх досвіду та проектів у сфері інфраструктура. захист ключів, відсутність координації та злагодженості органів влади, низький рівень впровадження державно-приватного співробітництва тощо.

Через російське вторгнення в умовах надзвичайної ситуації в Україні питання забезпечення належного захисту критичної інфраструктури є особливо актуальним, тому в країні виникнуть нормативно-правові, адміністративні проблеми порядку, координації та, звичайно, економічного характеру чекатимуть вирішення [25].

Враховуючи досвід провідних країн світу, а також напрацювання українських фахівців із захисту критичної інфраструктури, можна виділити такі напрямки подальшого розвитку державної системи захисту критичної інфраструктури в Україні:

- розвиток та регулярне перегляд нормативно-правової бази;

- визначити завдання центрального координаційного органу держави у цій сфері;

- удосконалити методичний підхід, на основі якого визначається перелік об'єктів критичної інфраструктури;

- підготувати кваліфікований персонал у сфері захисту критичної інфраструктури;

- організувати обмін інформацією та передовим досвідом у формі міжнародних та державних приватних організацій [21].

Доцільно зосередити увагу на наступних кроках у розвитку та впровадженні системи захисту критичної інфраструктури в Україні в найближчому майбутньому:

1. Розробка стратегії та планування: Україна має розробити та постійно вдосконалювати комплексну стратегію захисту критичної інфраструктури та плани дій у надзвичайних ситуаціях. Таким чином країна може краще підготуватися та краще реагувати на потенційні загрози.

2. Інвестувати в кібербезпеку: підвищувати обізнаність персоналу, регулярно перевіряти системи безпеки, впроваджувати інтегрований підхід до забезпечення кібербезпеки, який вимагає значних капітальних витрат, але насправді сприяє серйозним кібератакам і запобігає наслідкам.

3. Співпраця з міжнародними партнерами: Завдяки активній співпраці з міжнародними партнерами щодо обміну досвідом та інформацією щодо захисту критичної інфраструктури можна виявляти загрози та швидко на них реагувати.

4. Навчання персоналу: персонал, відповідальний за безпеку критичної інфраструктури, повинен проходити систематичне підвищення кваліфікації та безперервне навчання для набуття знань і навичок у визначенні та реагуванні на небезпеки та надзвичайні ситуації.

5. Співпраця державного та приватного секторів необхідна для створення якісних систем захисту об’єктів критичної інфраструктури, оскільки досвід зарубіжних країн показує, що реагування на кіберзломи та кібератаки є ефективними лише за умови спільних зусиль. ця партія працює.

Захист критичної інфраструктури в Україні – завдання, яке потребує серйозної уваги та ресурсів. Лише за комплексного підходу та взаємодії на різних рівнях влади, бізнесу, громадян та міжнародних партнерів Україна зможе забезпечити надійний захист критичної інфраструктури та національну безпеку.

2.2 Розробка рекомендацій щодо підвищення стійкості об'єктів критичної інфраструктури

Серед факторів, що впливають на формування державної політики у сфері безпеки автоматизованих систем управління критичною інфраструктурою, слід звернути увагу на такі [40]:

- інтеграція критичних об’єктів та іншої інформації, яка використовується в управлінні, в окремих суб’єктах автоматизованих систем управління;

- виробнича та транспортна інфраструктура, адміністрація та фінанси;

- постійна складність програмного забезпечення та обладнання, що використовується в автоматизованих системах управління критичними об'єктами;

- практика іноземних компаній з обслуговування та дистанційного керування системами автоматичного керування важливими об'єктами або їх частинами, а також телекомунікаційним обладнанням у важливих інформаційних інфраструктурах;

- прагнення організацій, що розробляють програмне забезпечення для систем автоматичного управління критичними об'єктами, знизити витрати і, як наслідок, використовувати стандартні рішення та запозичене програмне забезпечення;

- суттєве вдосконалення способів і способів використання інформаційно-комунікаційних технологій на шкоду Україні, а також спроби їх використання в протиправних і конкурентних цілях, які в майбутньому будуть поширеними;

- підвищення ризику тероризму, зростання незаконної діяльності з використанням інформаційно-комунікаційних технологій;

- сформована серед операторів та власників інформаційних систем тенденція до приховування зусиль або фактів щодо порушення нормального функціонування АСУ критичних об'єктів;

- недостатня підготовка та професійна підготовка персоналу, що обслуговує АСУ важливих питань, зниження технічної культури виробництва;

- відсутність належних нормативно-правових положень щодо процесів, спрямованих на забезпечення безпеки автоматизованих систем управління критичними об'єктами, у тому числі визначення їх реального рівня безпеки;

- примусова участь у створенні автоматизованих систем управління значної частини іноземних компаній – виробників і постачальників програмно-апаратних засобів обробки, зберігання та обміну даними, а також використання іноземних програмно-апаратних рішень, що створює умови для технічне вдосконалення та незалежність від іноземних держав [16].

При цьому в основу державної політики щодо безпеки автоматизованих систем управління важливими питаннями мають бути покладені такі принципи:

- дотримання всіма вимог законодавства України та міжнародних договорів в Україні. учасники створення та використання автоматизованих систем управління важливими справами;

- поєднання інтересів і взаємної відповідальності держави, громадян і організацій, які беруть участь у розробці, створенні та використанні автоматизованих систем управління важливими питаннями;

- персональна відповідальність посадових осіб, операторів, службовців та інших осіб, залучених до розробки, створення, впровадження, використання та модернізації автоматизованої системи управління важливими об'єктами;

- забезпечення комплексного захисту критичної інформаційної інфраструктури в цілому, включаючи створення єдиної державної системи виявлення та запобігання комп’ютерним атакам на критичну інформаційну інфраструктуру та оцінки ефективного захисту її частин;

- забезпечення роботи затвердженого типу у сфері забезпечення безпеки автоматизованих систем управління критичним майном із застосуванням системи ліцензування та сертифікації;

- розподіляти завдання між Центральним виконавчим комітетом держави у сфері безпеки важливих об'єктів та інших частин важливої інформаційної інфраструктури та іншими виконавчими органами держави, які виконують завдання у сфері безпеки; важливих частин та інших частин важливої інформаційної інфраструктури та між державним контролем, який здійснює нагляд за роботою важливих частин та інших частин важливої інформаційної

інфраструктури, та регуляторними органами, що посилює координацію їх діяльності;

- встановити правила щодо прав та обов'язків власників автоматизованих систем з управління важливими частинами та іншими частинами важливої інформаційної інфраструктури, а також організацій, які їх обслуговують;

- запобігання технічній чи іншій залежності від іноземних держав при здійсненні діяльності у сфері безпеки автоматизованих систем, призначених для контролю критичних об'єктів [14].

У визначеному контексті засад державної політики забезпечення безпеки автоматизованих систем контролю важливих об’єктів визначено основні завдання щодо реформування нормативно-правової бази у сфері забезпечення безпеки автоматизованих систем контролю важливих об’єктів. Цілі повинні включати наступне:

- визначити та обмежити повноваження:

а) головного органу виконавчої влади держави у сфері забезпечення важливих цілей та інших ланок важливої інформаційної інфраструктури;

б) інші органи виконавчої влади, що здійснюють діяльність у сфері забезпечення безпеки важливих об'єктів та інших частин важливої інформаційної інфраструктури;

в) органи державного регулювання та регуляторні органи здійснюють управління функціонуванням критичних об’єктів та інших частин критичної інформаційної інфраструктури;

- законодавче визначення та закріплення прав і обов'язків власників та експлуатаційних організацій автоматизованих систем управління критичними об'єктами та інших об'єктів критичної інформаційної інфраструктури у сфері безпеки систем безпеки, автоматизованого управління критичною інфраструктурою;

- визначити послідовність:

а) розробки, впровадження, використання та модернізації автоматизованих систем управління критичними об’єктами та іншими елементами критичної інформаційної інфраструктури;

б) отримати реалізаційну здатність державної організації щодо забезпечення безпеки критичної інфраструктури від системи автоматичного управління критичними об’єктами та іншими частинами критичної інформації критичної інфраструктури;

в) застосовувати сили і методи для виявлення та запобігання комп’ютерним атакам на критичну інформаційну інфраструктуру;

г) застосування сили і методів для усунення наслідків комп'ютерних збоїв щодо критичної інформаційної інфраструктури;

д) дії посадових осіб, службовців та власників автоматизованих систем управління критичними об'єктами та іншими частинами критичної інформаційної інфраструктури при виявленні спроб або фактів порушення нормативів використання цих об'єктів у разі виходу з ладу ЕОМ [12];

- створити законодавчу базу та визначити порядок проведення обов'язкових заходів щодо обміну інформацією з об'єктами інформації, джерелами комп'ютерних атак до їх повної ліквідації;

- нормативно-правове забезпечення впровадження єдиної державної системи виявлення комп'ютерних атак на об'єкти критичної інформаційної інфраструктури та моніторингу їх фактичного рівня безпеки;

- покласти відповідальність за послідовність розробки, впровадження, використання та модернізації автоматизованих систем управління критичними об'єктами та іншими ланками критичної інформаційної інфраструктури;

- посилення відповідальності за створення або використання комп'ютерних атак на критичну інфраструктуру;

- удосконалення законодавства України в частині ліцензійних процедур, пов’язаних з розробкою, виробництвом, використанням та супроводом автоматизованих систем управління критичними об’єктами [24].

При цьому основними завданнями комісії із забезпечення безпеки АСУ є:

- розвиток системи управління та контролю комісії та посилення координації заходів безпеки критичної інформаційної інфраструктури;

- виділити (залучити) обсяги та джерела фінансування (бюджетні та позабюджетні), необхідні для реалізації планів і планів заходів, спрямованих на забезпечення безпеки автоматизованої системи управління критично важливих об'єктів та критичної інформаційної інфраструктури;

- створення єдиної державної системи виявлення та запобігання комп'ютерним атакам на критичну інформаційну інфраструктуру та оцінки безпеки її елементів;

- забезпечення стабільного функціонування національної частини єдиної міжнародної інформаційно-телекомунікаційної мережі в умовах сильного деструктивного впливу інформації, що надходить з територій за межами юрисдикції України;

- створити умови для розвитку в Україні комунікаційного обладнання, стійкого до комп'ютерних атак;

- створювати та підтримувати постійну готовність сил і засобів для ліквідації наслідків виходу з ладу ІТ критичних інформаційних інфраструктур;

- розвивати міжнародне співробітництво, зокрема шляхом вдосконалення міжнародного співробітництва у сфері інформаційної безпеки;

- особливо щодо змісту, заохочуються дослідження, які проводяться приватними організаціями та окремими особами з метою виявлення вразливостей програмного забезпечення та обладнання, що використовується в системах автоматичного керування критично важливими об'єктами та іншими частинами критичної інформаційної інфраструктури, з наданням результатів до державного органу. орган виконавчої влади у сфері безпеки критичної інфраструктури [21].

Крім того, найважливішими завданнями удосконалення виробничої та науково-технічної політики у сфері забезпечення безпеки АСУ критичних об'єктів мають бути:

- реалізація різноманітних заходів щодо оцінки системи, способів і методів технічного розвитку фактичного рівня безпеки автоматичних систем управління критичними частинами установок та критичної інформаційної інфраструктури в цілому;

- створення єдиного реєстру програмно-технічних засобів, що використовуються в автоматизованих системах управління критичними будівлями;

- створення баз даних, що стосуються надійності системи автоматичного управління критичними установками, ситуації з їхньою безпекою, технічного стану обладнання та оцінки ефективності заходів безпеки, що діють і впроваджуються в критичних установках;

- здійснювати комплекс організаційно-технічних заходів для запобігання обміну інформацією між автоматизованими системами управління значущих об'єктів, розташованих на території іноземних держав, а якщо таке виключення є технічно неможливим – створювати захисні заходи та впроваджувати їх для уникнення негативних наслідків внаслідок процеси, контрольовані автоматизованими системами управління, важливою частиною, якщо нормальна робота цього каналу зв'язку переривається;

- розробити заходи щодо створення та впровадження телекомунікаційного обладнання, стійкого до комп'ютерних атак;

- створення репозиторію еталонного програмного забезпечення, що використовується в автоматизованих системах управління критичними об'єктами та іншими ланками критичної інформаційної інфраструктури;

- розвиток науково-виробничої бази (з урахуванням готовності до введення в дію), забезпечення випуску системи (методів) забезпечення безпеки АСУ критичних об'єктів та інших частин критичної інформаційної інфраструктури;

- розробка та впровадження імпортозаміщувальних технологій, матеріалів, комплектуючих та інших видів продукції в системах автоматичного управління критичними об'єктами [22].

Основні завдання в галузі фундаментальних і прикладних наук, розробка технологій і методів забезпечення безпеки автоматизованих систем, призначених для контролю критичної інфраструктури та критичної інформаційної інфраструктури:

- розробка методів і засобів для швидкого виявлення загроз і оцінки ризиків, їх автоматизовані аварійні системи, системи управління критичною інфраструктурою та інші елементи критичної інформаційної інфраструктури;

- розробка та впровадження спеціалізованих систем аналізу інформації, розробка досліджень математичних моделей процесу забезпечення безпеки автоматизованих систем, призначених для контролю критичної інфраструктури та інших частин критичної інформаційної інфраструктури, з метою розвитку ймовірних ситуацій та підтримки управлінські рішення;

- розробити та впровадити комплексні системи захисту та безпеки для систем автоматичного керування критичною інфраструктурою та іншими частинами критичної інформаційної інфраструктури, які відповідають сучасному рівню розвитку IT та мінімізують залучення обслуговуючого персоналу до встановлення та використання програмно-апаратних засобів та супутніх товарів;

- розробити автоматизовані системи управління критичною IT-інфраструктурою, що виключають або мінімізують обмін інформацією на технічному рівні та підлягають обов'язковому захисту [7].

Основними завданнями, пов’язаними з освітою, підготовкою та навчанням персоналу, є забезпечення безпеки важливих автоматизованих систем управління інфраструктурою та підвищення загальної культури інформаційної безпеки громадян:

- Система підготовки, перепідготовки та атестації персоналу (включно з менеджерами) покращити.

д) у сфері безпеки забезпечити автоматизовану систему на базі навчальних закладів, що спеціалізуються на управлінні критичною інфраструктурою та критичною інформаційною інфраструктурою;

- загальне підвищення культури інформаційної безпеки громадян, у тому числі підвищення обізнаності громадськості щодо критичної інформаційної інфраструктури, загроз інформаційній безпеці та способів захисту від цих загроз;

- нетерпимість у загальній свідомості до людей, які використовують інформаційні технології для здійснення незаконної діяльності, пов'язаної з критичною інфраструктурою.

Реалізація цих основних шляхів забезпечується шляхом об’єднання зусиль державних інститутів та організацій громадянського суспільства для захисту інтересів України із застосуванням комплексних заходів правового, організаційного, технічного, соціально-економічного, спеціального та іншого забезпечення. Державна служба України з надзвичайних ситуацій координує діяльність державних органів з виконавчою владою щодо реалізації цих основних методів [19].

2.3 Оцінка ефективності запропонованих заходів щодо підвищення стійкості об'єктів критичної інфраструктури

Наведемо основні засоби та етапи реалізації державної політики, спрямованої на забезпечення безпеки системи управління критичною інфраструктурою.

На першому етапі буде необхідно [4]:

- розробити план дій для впровадження цих основних модальностей;

- регулювання та обмеження повноважень і відповідальності органів державної виконавчої влади, які здійснюють діяльність у сфері безпеки, інших органів державної виконавчої влади, які виконують завдання, пов’язані з регіональною безпекою, контрольно-регулюючих органів держави, які здійснюють нагляд за діяльністю важливих структур та інформаційної інфраструктури важливі об'єкти;

- рішення щодо порядку застосування збройних сил та способу виявлення та запобігання комп'ютерним атакам на критичні інформаційні інфраструктури;

- розробка концепції застосування сил і методів для ліквідації наслідків збоїв у роботі ІТ, спрямованих на критичні інформаційні інфраструктури;

- визначити обсяги та джерела коштів (бюджетних та позабюджетних), необхідних для реалізації планів і планів заходів у сфері забезпечення безпеки АСУ важливих об’єктів та всієї значущої інформаційної інфраструктури протягом відповідного періоду;

- підготувати пропозиції щодо внесення змін до затверджених національних планів та адаптувати пропозиції до національних планів захисту важливої інфраструктури [22].

На другому етапі необхідно:

- підготувати нормативно-правові акти, які визначають:

а) порядок набуття повноважень державної виконавчої влади у сфері безпеки критичної інфраструктури надання інформації щодо систем автоматичного керування критичними об'єктами та іншими ланками критичної інформаційної інфраструктури;

б) права та обов'язки власників автоматизованих систем управління критичними частинами та іншими частинами критичної інформаційної інфраструктури, а також організацій, що працюють у сфері безпеки;

в) методику розробки, впровадження, експлуатації та модернізації автоматизованих систем, призначених для управління критичними об'єктами;

г) нормативно-правові акти щодо функціонування єдиної державної системи виявлення та запобігання комп’ютерним атакам на критичну інформаційну інфраструктуру та оцінки безпеки її складових;

е) процедури усунення наслідків збою ІТ, що впливає на критичну інформаційну інфраструктуру;

д) дії посадових осіб, працівників і власників автоматизованих систем управління критичними об'єктами та іншими об'єктами критичної інформаційної інфраструктури при виявленні несанкціонованого доступу до інформації, що оброблюється, та інших ІТ-подій;

ж) відповідальність за порушення встановленого порядку у зв'язку з розробкою, впровадженням, використанням і модернізацією автоматизованих систем, призначених для управління критичними об'єктами та іншими складовими інфраструктури критичної інформації;

є) правові підстави та правовий порядок вжиття заходів щодо примусової зміни інформаційного обміну з об’єктами інформаційного обміну, які є джерелом комп’ютерних атак, до повного їх вимкнення:

- сертифікація автоматизованих систем управління критичними активами;

- розробити систему грантів для окремих осіб та установ, метою якої є заохочення досліджень для виявлення слабких місць у програмному забезпеченні та обладнанні системи автоматичного керування значущих сайтів та інших частин інфраструктури важливої інформації;

- розробка комплексних систем захисту та безпеки для автоматичного управління критичними та іншими частинами критичної інформаційної інфраструктури, що відповідають сучасному рівню розвитку інформаційно-комунікаційних технологій, і мінімізують участь обслуговуючого персоналу в установці та використанні апаратного забезпечення і програмне забезпечення, що входить до їх конфігурації;

- визначення обсягів і джерел ресурсів (бюджетних і зовнішніх), необхідних для реалізації планів і планів заходів, пов'язаних з безпекою автоматизованих систем, призначених для управління критичними об'єктами та інформаційною інфраструктурою, критика перших кроків інших у роботі;

- впровадження цих ключових стратегій у цілому;

- реалізувати першу чергу урядового центру з виявлення та запобігання комп’ютерним атакам на критичну інформаційну інфраструктуру та оцінки фактичного рівня безпеки її елементів;

- створення сил і методів ліквідації наслідків комп’ютерних збоїв у критичних інформаційних інфраструктурах [23].

На третьому етапі необхідно реалізувати наступне:

- впровадження комплексних систем захисту та безпеки для автоматичних систем, призначених для управління критичними частинами та іншими частинами критичної інформаційної інфраструктури, що відповідають сучасному рівню розвитку інформації та технології та звести до мінімуму участь обслуговуючого персоналу в установці та використанні програмного та апаратного забезпечення;

- впровадження першої черги колекції еталонного програмного забезпечення, що використовується в автоматизованих системах управління критичними об'єктами та іншими важливими частинами інформаційної інфраструктури;

- створити систему підтримки для окремих осіб та установ для сприяння дослідженням у сфері аналізу вразливостей у програмному забезпеченні та обладнанні автоматизованих систем керування критичною інформацією в критичних місцях та інших об’єктах інфраструктури;

- впровадження Системного ситуаційного центру для виявлення та попередження комп’ютерних атак на критичну інформаційну інфраструктуру України, а також оцінки фактичного рівня безпеки її елементів та ситуаційних центрів на регіональному та відомчому рівнях;

- створити автоматизовані системи управління важливими об'єктами, а також економічно вигідну спеціалізовану інформаційну технологію, яка на технічному рівні виключає або скорочує обмін інформацією, що підлягає обов'язковому захисту;

- реалізація загально єдиної державної системи виявлення та попередження комп’ютерних атак на критичну інформаційну інфраструктуру та оцінки реального рівня безпеки її елементів [13].

Після третього періоду має бути здійснено низку заходів для підтримки організаційної, фінансової, науково-технічної та технологічної готовності України до запобігання загрозам безпеці її критичної інформаційної інфраструктури.

Шляхом створення центру для моніторингу та управління збоями інформаційної безпеки критичних компонентів інфраструктури рекомендується:

- впровадження (особливо постачання програмних та апаратних рішень) та розробка системи для виявлення та моніторингу подій безпеки, в тому числі розробити правила відповідності:

а) сукупні джерела інцидентів, включаючи джерела, які зазвичай не підтримуються;

б) розробляти технічні, практичні та організаційні документи щодо системної звітності;

- доставка, інтеграція та впровадження інструментів для державних регуляторних органів;

- розробляти та впроваджувати процеси та правила щодо роботи центру моніторингу та управління інцидентами критичної інфраструктури, включаючи правила спілкування з державними регуляторними органами;

- підготувати персонал, відповідальний за інформаційну безпеку та IT-сервіси, у тому числі організувати навчання онлайн [17].

Створення єдиної інформаційної платформи для інтеграції інформації про об’єкти критичної інфраструктури, інформацію про методи захисту даних та системи об’єктів критичної інфраструктури, включаючи інформацію про системи захисту безпеки та їх сумісність із чинною законодавчою базою України, а також України. та міжнародних стандартів у сфері захисту даних, значне підвищення рівня державного контролю критичної інфраструктури в цілому [19].

Таким чином, створення єдиної системи захисту значних частин критичної інформаційної інфраструктури дозволяє:

- забезпечити дотримання вимог законодавства, вжити необхідних заходів для встановлення зв'язку з державною системою з метою виявлення, блокування та попередження наслідки комп’ютерних атак на українські інформаційні ресурси;

- мінімізувати ризик штрафів і перевірок з боку контролюючих органів, а також адміністративної та кримінальної відповідальності співробітників організації, що виникають при виявленні порушень законодавчих умов;

- управління процесами захисту даних компонентів критичної інфраструктури та процесів реагування на збої в інформаційній безпеці, коригування відповідальності у сфері обробки даних та захисту компонентів критичної інфраструктури;

- підвищення обізнаності працівників сектору IT-безпеки про важливі інфраструктури;

- підвищити ефективність системи інформаційної безпеки шляхом модернізації застарілих засобів інформаційної безпеки та створення центру моніторингу та управління порушеннями інформаційної безпеки щодо критичних компонентів інфраструктури;

- оптимізація витрат для забезпечення відповідності вимогам законодавства та підтримки рівня безпеки інформаційних інфраструктур, що є одним із найважливіших, шляхом створення засобів моніторингу та управління безпекою для кожної фази життєвого циклу критичної інфраструктури;

– зменшити технічні, репутаційні, фінансові та соціальні ризики, пов’язані з безпекою критичних компонентів інфраструктури.

ВИСНОВКИ

Критичні інфраструктури є основою рухомих суспільств. Однак ми все більше залежимо від функціонуючих послуг, навіть якщо кліматичні ризики та глобальні потрясіння виявляють уразливість наших систем. Останніми роками руйнівні землетруси, урагани і навіть глобальна пандемія показали, що без належного захисту нашої інфраструктури наслідки катастроф загострюються, погіршуючи страждання людей і навколишнього середовища. Визнання ключової ролі, яку відіграють інфраструктури в нашому повсякденному житті, і вжиття заходів для мінімізації ризиків для них ніколи не було настільки важливим.

Дослідження UNU-EHS показує, що функціонуюча інфраструктура — це більше, ніж просто наявність технологій та обладнання. Йдеться також про людей, які керують інфраструктурою, а також про їхні потужності та доступ до робочих місць у разі катастрофи. Критична інфраструктура стикається з новими загрозами, які можуть зруйнувати її роботу та створити загрозу громадській безпеці та економічній стабільності. Параметри оцінки критичності мають різний тип і описують вплив кризової ситуації на об’єкт КІ (її наслідки) з різних точок зору. Вони можуть бути представлені в якісній або кількісній формі. Для визначення параметрів оцінки на критичному рівні використовуються фактори і характеристики, зазначені в Зеленій книзі, яка використовується в більшості країнах.

На сьогодні, у процесі є реформування сектору безпеки необхідно проаналізувати пріоритетні напрями уточнення функцій та повноважень державних органів сектору безпеки виходячи із сучасних концепцій забезпечення національної стійкості. Концепція захисту критичної інфраструктури в системі забезпечення національної стійкості. Слід відзначити, що «вимушеність» реформування сектору безпеки в Україні внаслідок неготовності до гібридної війни не є унікальним недоліком країни. Концепція захисту критичної інфраструктури держави дає можливість сформувати

необхідну базу для функціонування спеціального правоохоронного органу держави відповідно до сучасних теоретичних засад та кращої світової практики. Та перш ніж перейти до детальнішого аналізу пріоритетів удосконалення нормативно-правової бази діяльності сектору безпеки з питань забезпечення ЗКІ слід поглянути на роль КІ для забезпечення національної безпеки, а також місце та роль сектору безпеки у забезпеченні стійкості функціонування суспільства та держави з системних позицій. Системний підхід до визначення предмету діяльності сектору безпеки у сфері захист критичної інфраструктури.

Враховуючи сучасні виклики та загрози, які можуть виникнути внаслідок стихійних лих, кібератак, терористичних загроз чи геополітичних конфліктів, захист критичної інфраструктури є важливим завданням для забезпечення національної безпеки країни. Аспекти захисту об'єктів критичної інфраструктури в умовах надзвичайного, надзвичайного та воєнного стану, особливого часу регулюються Законами України «Про правову систему про надзвичайні ситуації», «Про правову систему про надзвичайні ситуації», «Про правову систему надзвичайних ситуацій», «Функціонування єдиної транспортної системи України в особливий час» та «Про оборону України «Спеціальний закон про забезпечення кіберзахисту та кібербезпеки критичної інфраструктури». Глобальні тенденції до посилення природних та техногенних загроз, зростання терористичних загроз, зростання кількості та складності кібератак, а також пошкодження інфраструктури на сході та півдні України, а також наслідки збройного нападу російської федерації призвела до руйнування систем, засобів, необхідних для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки та реального захисту ресурсів. Організації у сфері захисту критичної інфраструктури бізнесу здійснюють класифікацію компонентів критичної інфраструктури відповідно до спеціалізацій, галузевих законодавчих вимог і чотирьох визначених категорій важливості та критичності компонентів. В Україні охорона об'єктів, віднесених до «критичної інфраструктури» згідно з міжнародними угодами, регулюється

численними нормативно-правовими актами, які мають переважно внутрішньовідомчий характер.

Серед факторів, що впливають на формування державної політики у сфері безпеки автоматизованих систем управління критичною інфраструктурою, слід звернути увагу на такі: інтеграція критичних об’єктів та іншої інформації, яка використовується в управлінні, в окремих суб’єктах автоматизованих систем управління; виробнича та транспортна інфраструктура, адміністрація та фінанси; постійна складність програмного забезпечення та обладнання, що використовується в автоматизованих системах управління критичними об'єктами; практика іноземних компаній з обслуговування та дистанційного керування системами автоматичного керування важливими об'єктами або їх частинами, а також телекомунікаційним обладнанням у важливих інформаційних інфраструктурах; прагнення організацій, що розробляють програмне забезпечення для систем автоматичного управління критичними об'єктами, знизити витрати і, як наслідок, використовувати стандартні рішення та запозичене програмне забезпечення; суттєве вдосконалення способів і способів використання інформаційно-комунікаційних технологій на шкоду Україні, а також спроби їх використання в протиправних і конкурентних цілях, які в майбутньому будуть поширеними; підвищення ризику тероризму, зростання незаконної діяльності з використанням інформаційно-комунікаційних технологій; сформована серед операторів та власників інформаційних систем тенденція до приховування зусиль або фактів щодо порушення нормального функціонування АСУ критичних об'єктів; недостатня підготовка та професійна підготовка персоналу, що обслуговує АСУ важливих питань, зниження технічної культури виробництва; відсутність належних нормативно-правових положень щодо процесів, спрямованих на забезпечення безпеки автоматизованих систем управління критичними об'єктами, у тому числі визначення їх реального рівня безпеки; примусова участь у створенні автоматизованих систем управління значної частини іноземних компаній - виробників і постачальників програмно-апаратних засобів обробки, зберігання та обміну даними, а також використання

іноземних програмно-апаратних рішень, що створює умови для технічне вдосконалення та незалежність від іноземних держав.

СПИСОК РЕФЕРОВАНОЇ ЛІТЕРАТУРИ

1. Болвановська Т. В. Аналіз об’єктів критичної інфраструктури. *Дніпровський національний університет залізничного транспорту. Матеріали*. 2020. 79. С. 151-152.

2. Борсук Ю. Критична інфраструктура західного регіону україни в умовах війни: суспільно-географічне дослідження. *Реалії, проблеми та перспективи розвитку географії, екології, туризму та сфери*. 2023. С. 52. https://geography.lnu.edu.ua/wp-content/uploads/2023/10/Zbirnyk_studkonf_2023.pdf#page=52

3. Ботнаренко І. А. Критична інфраструктура в україні та її складові: поняття, зміст та законодавче визначення. *Редакційна колегія*. 2024. С. 17.

4. Галіахметов І. А. Правовий режим об’єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану. 2022. https://ir.kneu.edu.ua/bitstream/handle/2010/39024/Psvic_22-2.pdf?sequence=1

5. Гора І. В. Окремі питання захисту об’єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії*. 2021. С. 132-139.

6. Горбачук В. Теоретико-ігрові та оптимізаційні моделі і методи підвищення безпеки кіберінфраструктур. 2022. https://ekmair.ukma.edu.ua/items/e5378262-0574-4f65-8b48-83b1c82ebd00

7. Громовенко К. В. Захист критично важливих об'єктів інфраструктури в контексті міжнародного миру та безпеки. 2021. http://lsej.org.ua/9_2021/9_2021.pdf#page=329

8. Жукова І. Сутність поняття механізм державного регулювання розвитку критичної інфраструктури. *Věda a perspektivy*. 2023. 6 (25). С. 45-47.

9. Зюзюн В. І. До розробки моделей управління регіональними програмами безпеки об’єктів критичної інфраструктури транспорту. *Вісник Національного транспортного університету*. 2019. 2. С. 81-89.

10. Іваненко О. І. Підхід до національної оцінки ризиків для критичної інфраструктури. *Вестник Херсонского национального технического университета*. 2020. 2 (73). С. 9-22.

11. Кідалова Н. О. Правові проблеми захисту критичних об’єктів інфраструктури стратегічного значення в України. 2019. https://dglib.nubip.edu.ua/bitstream/123456789/8429/1/124_Kidalova.pdf

12. Ковалів М. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. *Traektoriâ Nauki= Path of Science*. 2021. 7.4. С. 2011-2018.

13. Корченко О. Метод оцінювання рівня підвищення стану кіберзахисту об’єктів критичної інфраструктури держави. *Наукоємні технології.* 2024. 61.1. С. 3-20.

14. Крилова І. І. Забезпечення стійкості та безпеки систем водопостачання та водовідведення в рамках державного регулювання критичної інфраструктури. *Вчені записки*. 2019. 19. С. 32-40.

15. Крилова І. І. Стратегічні цілі сфери водопостачання та водовідведення в рамках створення національної системи захисту критичної інфраструктури. *Фінанси, бухгалтерський облік та підприємництво: національні особливості та світові тенденції.* 2019. С. 27-30.

16. Кузьменко Ю. В. Захист об’єктів критичної інфраструктури: адміністративно-правове забезпечення. 2021. https://dspace.oduvs.edu.ua/handle/123456789/2873

17. Кулик В. В. Моделювання міжгалузевої економіки як критичної інфраструктури: розроблення сценаріїв розвитку економіки україни в умовах війни та післявоєнного відновлення. *Cybernetics & Systems Analysis/Kibernetiki i Sistemnyj Analiz*. 2023. 6. https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=10195262&AN=173637337&h=PIEtkzkoyVSTFsOr8fioZJWMVYt2REV3GdsMPZIIhXp9qCsDksWaaPq9D8S8nQcIDvETyHyQqlO5TJc3jN9RDw%3D%3D&crl=c

18. Кучма О. Критична інфраструктура та кіберзагрози: досягнення стратегічних цілей державного аудиту щодо кіберзахисту критичної інфраструктури. *Наукові перспективи*. 2023. 10 (40).

19. Леонов Б. Д. Розвиток методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури (на прикладі США). *Інформація і право*. 2020. 3 (34). С. 88-95.

20. Лойко В. Економіко-правові засади забезпечення захисту критичної інфраструктури. *Financial and credit activity: problems of theory and practice*. 2020. 4.35. С. 426-438.

21. Мальцева І. Аналіз методик оцінки кіберстійкості критичної інфраструктури. *Електронне фахове наукове видання Кібербезпека: освіта, наука, техніка*. 2021. 4.12. С. 29-35.

22. Оксенчук Д. Міжнародне регулювання безпеки об'єктів критичної інфраструктури. *Національний авіаційний університет*, 2022. https://dspace.nau.edu.ua/handle/NAU/55069

23. Осіпчук І.І. Адміністративна діяльність Служби безпеки України як основа забезпечення критичної інфраструктури. *Law and Safety*. 2020. 78.3. С. 32-37.

24. Потетюєва М.В. Залізничний транспорт у структурі критичної інфраструктури іноземних держав. *The XV International Scientific and Practical Conference Innovative technologies in the field of human services*. 2022. 15-17. С. 122-124.

25. Пядишев В.Г. Кібербезпека критичних інфраструктур: закордонний досвід та українські реалії. 2022. https://dspace.oduvs.edu.ua/handle/123456789/4525

26. Солопова І. В. Правові умови захисту об'єктів критичної інфраструктури в Україні: проблеми та перспективи. *Південноукраїнський правничий часопис*. 2021. 2. С. 119-125.

27. Стащук А.А. Організація безпеки та захисту об’єктів критичної інфраструктури України. *Актуальні проблеми забезпечення державної безпеки: матеріали*. 2023. С. 241.

28. Таран О. В. Проблеми кримінальної відповідальності за посягання на об’єкти критичної інфраструктури в ядерній енергетиці. *Ядерна та радіаційна безпека*. 2019. 3. С. 58-67.

29. Трушкіна Н. В. Розвиток критичної інформаційної інфраструктури з позицій кібербезпеки: теоретичні аспекти. *Українська інженерно-педагогічна академія.* 2023. 5. С. 206. http://repo.uipa.edu.ua/jspui/bitstream/123456789/7218/1/pdf.pdf#page=206

30. Трушкіна Н.В. Ключові проблеми розвитку критичної інфраструктури в україні у воєнний період. *Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку*. 2020. 3. С. 45. http://perspectives.pp.ua/public/site/conferency/conf-30.pdf#page=346

31. Трушкіна Н.В. Економічне забезпечення організації і функціонування критичної інфраструктури. *Успіхи і досягнення у науці*. 2024. 1 (1). С. 34-36.

32. Трушкіна, НВ. Сутність методології ідентифікації об’єктів критичної інфраструктури: досвід франції та великобританії. *Програмний комітет*. 2023. С. 46. https://msu.edu.ua/wp-content/uploads/2023/05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA-%D1%82%D0%B5%D0%B7-%D0%9C%D0%9D%D0%9F%D0%9A_%D0%9C%D0%A3%D0%95%D0%9F.pdf#page=46

33. Хрутьба В.О. Формування методів управління проектами та програмами безпеки об’єктів критичної інфраструктури. 2019. https://repositary.knuba.edu.ua/bitstream/987654321/3147/1/11.pdf

34. Хрутьба В.О. Огляд науково-теоретичних аспектів безпеки об’єктів критичної інфраструктури транспорту. *Вісник Національного технічного*

університету ХПІ. Серія: Стратегічне управління, управління портфелями, програмами та проектами. 2019. 2. С. 60-65.

35. Хулак Г. Методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури об’єктів ядерної енергетики. *Електронне фахове наукове видання Кібербезпека: освіта, наука, техніка*. 2021. 4.12. С. 172-186.

36. Швець А.В. Нормативно-правове забезпечення захисту критичної інфраструктури, пов’язаної з небезпечними матеріалами, в Україні. *Редакційна колегія*. 2020. С. 389.

37. Шиповський В. Система показників оцінювання кіберстійкості інформаційних систем об’єктів критичної інфраструктури. *Ukrainian Information Security Research Journal*. 2023. 25.1. С. 37-45.

38. Шпатакова О. Перспективи відновлення критичної інфраструктури на деокупованих територіях України. *Економіка та суспільство*. 40. 2022.

39. Ярута В. Теоретичні засади функціонування об’єктів критичної інфраструктури. *Наука про цивільний захист як шлях становлення молодих вчених*. 2020. https://chipb.dsns.gov.ua/upload/1/8/0/4/2/6/8/2-fomic.pdf#page=104

40. Ящук В. І. Принципи проектування автоматизованих інформаційних систем управління об’єктами критичної інфраструктур. 2021. https://sci.ldubgd.edu.ua/bitstream