Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)
Кафедра Безпеки інформаційних технологій
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Комплекс моніторингу (контролю) акустичного простору на об'єкті кіберзахисту

(тема)

Виконав: Тютюник В.В.
(прізвище, ініціали)
студент 2 курсу, групи БІКСзм-19-1
Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Безпека інформаційних і комунікаційних систем»
(повна назва освітньої програми)
Керівник професор Заболотний В.І.
(посада. прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет_____Комп'ютерної інженерії та управління_____
(повна назва)
Кафедра_____Безпеки інформаційних технологій_____
(повна назва)
Рівень вищої освіти_____другий (магістерський)_____

Спеціальність _____125 Кібербезпека_____
(код і повна назва)
Тип програми _____освітньо-професійна_____
(освітньо-професійна, або освітньо-наукова)
Освітня програма___«Безпека інформаційних і комунікаційних систем»____
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові____Тютюнику Вадиму Володимировичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи __Комплекс моніторингу (контролю) акустичного простору на об'єкті кіберзахисту_____
затверджена наказом по університету від _23_ __жовтня_____20_20 р. № _166 Стз_____
2. Термін подання студентом роботи до екзаменаційної комісії ____ _____ 20__ р.
3. Вихідні дані до роботи __*функціональна схема комплексу оперативного моніторингу (контролю) акустичної простору на об'єктах кіберзахисту*_____
4. Перелік питань, що потрібно опрацювати в роботі _____
*__1. Аналіз особливостей формування державної політики забезпечення кібернетичної безпеки*_____
*__2. Дослідження умов функціонування комплексної системи кібербезпеки в зоні контролю навколо об'єктів кіберзахисту*_____
*__3. Оцінка вразливості об'єктів кіберзахисту на основі ризико-орієнтованого підходу та оцінювання ефективності функціонування системи інформаційної безпеки*_____
*__4. Дослідження амплітудно-частотних спектрів акустичних сигналів від терористичних дій на об'єкті кіберзахисту*_____
*__5. Розробка функціональної схеми комплексу оперативного моніторингу (контролю) акустичної простору на об'єктах кіберзахисту*__
5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5. включається до завдання за рішенням випускової кафедри)
*_Презентаційний матеріал у вигляді слайдів_*_____

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Пошук літератури та аналіз особливостей формування державної політики забезпечення кібернетичної безпеки*	01.11.2020– 07.11.2020	
2	*Дослідження умов функціонування комплексної системи кібербезпеки в зоні контролю навколо об'єктів кіберзахисту та оцінка вразливості об'єктів кіберзахисту на основі ризико-орієнтованого підходу та оцінювання ефективності функціонування системи інформаційної безпеки*	08.11.2020– 14.11.2020	
3	*Дослідження амплітудно-частотних спектрів акустичних сигналів від терористичних дій на об'єкті кіберзахисту та аналіз отриманих результатів*	15.11.2020– 21.11.2020	
4	*Розробка функціональної схеми комплексу оперативного моніторингу (контролю) акустичної простору на об'єктах кіберзахисту*	22.11.2020– 30.11.2020	
5	*Оформлення пояснювальної записки*	01.12.2020– 07.12.2020	
6	*Подання атестаційної роботи керівникові та її попередній захист*	08.12.2020– 09.12.2020	
7	*Подання атестаційної роботи на рецензування*	10.12.2020– 11.12.2020	

Дата видачі завдання _23_ __жовня___2020 р.

Студент _____
(підпис)

Керівник роботи _____ _____професор Заболотний В.І._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до магістерської атестаційної роботі містить 129 с., 1 табл., 38 рис., 142 джерела.

У роботі проведено аналіз особливостей формування державної політики забезпечення кібернетичної безпеки. Проведені дослідження умов функціонування комплексної системи кібербезпеки в зоні контролю навколо об’єктів кіберзахисту. Здійснено оцінка вразливості об’єктів кіберзахисту на основі ризико-орієнтованого підходу та оцінювання ефективності функціонування системи інформаційної безпеки. За результатами досліджень амплітудно-частотних спектрів акустичних сигналів від терористичних дій на об’єктах кіберзахисту розроблено функціональну схему комплексу оперативного моніторингу (контролю) акустичного простору на об’єктах кіберзахисту.

ОБ’ЄКТ КІБЕРЗАХИСТУ, ЗОНА НАВКОЛО ОБ’ЄКТУ КІБЕРЗАХИСТУ, ОЦІНКА ВРАЗЛИВОСТІ, РИЗИКО-ОРІЄНТОВАНИЙ ПІДХІД, АКУСТИЧНІ СПЕКТРИ, АВТОМАТИЗОВАНІ ПРИСТРОЇ КОНТРОЛЮ АКУСТИЧНОГО ПРОСТОРУ, СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

РЕФЕРАТ

Пояснительная записка к магистерской аттестационной работе содержит 129 с., 1 табл., 38 рис., 142 источника.

В работе проведен анализ особенностей формирования государственной политики обеспечения кибернетической безопасности. Проведены исследования условий функционирования комплексной системы кибернетической безопасности в зоне контроля вокруг объектов кибернетической защиты. Осуществлена оценка уязвимости объектов кибернетической защиты на основе риск-ориентированого подхода и оценка эффективности функционирования системы информационной безопасности. По результатам исследования амплитудно-частотных спектров акустических сигналов от террористических действий на объектах кибернетической защиты разработано функциональную схему комплекса оперативного мониторинга (контроля) акустического пространства на объектах кибернетической защиты.

ОБЪЕКТ КИБЕРНЕТИЧЕСКОЙ ЗАЩИТЫ, ЗОНА ВОКРУГ ОБЪЕКТА КИБЕРНЕТИЧЕСКОЙ ЗАЩИТЫ, ОЦЕНКА УЯЗВИМОСТИ, РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД, АКУСТИЧЕСКИЕ СПЕКТРЫ, АВТОМАТИЗИРОВАННОЕ УСТРОЙСТВО КОНТРОЛЯ АКУСТИЧЕСКОГО ПРОСТРАНСТВА, СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

THE ABSTRACT

The magister’s attestation work contain 129 p., 1 tabl., 38 pic., 142 sources.

The paper analyzes the features of the formation of the state policy of ensuring cyber security. Research has been carried out on the conditions for the functioning of an integrated cyber security system in the control zone around objects of cyber defense. An assessment of the vulnerability of objects of cyber defense based on a risk-oriented approach and an assessment of the effectiveness of the functioning of the information security system has been carried out. Based on the results of the study of the amplitude-frequency spectra of acoustic signals from terrorist actions at cyber defense facilities, a functional diagram of a complex for operational monitoring (control) of the acoustic space at cyber defense facilities has been developed.

OBJECT OF CYBERNETIC PROTECTION, AREA AROUND THE OBJECT OF CYBERNETIC PROTECTION, VULNERABILITY ASSESSMENT, RISK-BASED APPROACH, ACOUSTIC SPECTRA, AUTOMATED SYSTEM OF ACOUSTICITY CONTROL.

ЗМІСТ

ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ

АЕ – акустична емісія;

АК – автомат М.Т. Калашникова;

АПС – акустичний пожежний сповіщувач;

АСВП – автоматична система виявлення пожежі;

АСГП – автоматична система гасіння пожежі

АЧЕ – акустичний чутливий елемент (мікрофон);

БПЛА – безпілотний літальний апарат;

ДССЗЗІ – Державна служба спеціального зв'язку та захисту інформації України;

ДТЗС – допоміжні технічні засоби та системи;

ЄДСЦЗ – Єдина державна система цивільного захисту;

КМУ – Кабінет міністрів України;

МВС України – Міністерство внутрішніх справ України;

НС – надзвичайна ситуація;

ОКЗ – об’єкт кіберзахисту;

ОПР – особа, що приймає рішення;

ОТЗС – основні технічні засоби та системи;

ПП – пороговий пристрій;

ПМ – пістолет М.Ф. Макарова;

РНБО – Рада національної безпеки і оборони України;

СБУ – Служба безпеки України;

СЦ – ситуаційний центр;

ТЗІ – технічний захист інформації.

ВСТУП

Стрімкий розвиток інформаційно-комунікаційних технологій сприяв формуванню кібернетичного простору, який здійснює значний вплив на соціально-економічне становище України та її національну безпеку, а також вказує на необхідність розробки ефективних заходів виявлення та ліквідації терористичних дій навколо об’єктів кіберзахисту.

Перспективним напрямом розробки таких заходів є створення комплексу оперативного моніторингу акустичної інформації від джерел терористичних небезпек на об’єктах кіберзахисту, з метою розробки та реалізації ефективних антикризових рішень щодо мінімізації наслідків від небезпеки.

Мета магістерської роботи – розробка комплексу оперативного моніторингу акустичної інформації від джерел терористичних небезпек на об’єктах кіберзахисту.

Об’єктом дослідження є комплекс оперативного моніторингу (контролю) акустичного простору на об’єктах кіберзахисту.

Предмет дослідження – параметри амплітудно-частотних спектрів акустичних сигналів від терористичних дій на об’єктах кіберзахисту.

У роботі проведено аналіз особливостей формування державної політики забезпечення кібернетичної безпеки. Проведені дослідження умов функціонування комплексної системи кібербезпеки в зоні контролю навколо об’єктів кіберзахисту. Здійснено оцінка вразливості об’єктів кіберзахисту на основі ризико-орієнтованого підходу та оцінювання ефективності функціонування системи інформаційної безпеки. За результатами досліджень амплітудно-частотних спектрів акустичних сигналів від терористичних дій на об’єктах кіберзахисту розроблено функціональну схему комплексу оперативного моніторингу (контролю) акустичного простору на об’єктах кіберзахисту.

РОЗДІЛ 1
АНАЛІЗ ОСОБЛИВОСТЕЙ ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

1.1 Сутність кібербезпеки в системі забезпечення національної безпеки України

Процеси глобалізації, які характерні для сучасного суспільства, зростання кількості загроз і викликів, актуалізували проблеми національної безпеки для більшості країн світу, в тому числі і для України. За таких умов постає необхідність адекватного реагування на існуючі виклики та загрози, тобто запровадження дієвої політики національної безпеки задля забезпечення національних інтересів держави. Її зміст, складові, методи та інструменти значною мірою залежать від сприйняття та розуміння сутності національної безпеки суб'єктами прийняття державних управлінських рішень.

Зазначимо, що сьогодні в колах науковців та практиків приділяється значна увага тлумаченню терміна «національна безпека», що передбачає використання різних підходів для визначення його сутності.

Так, в Законі «Про національну безпеку України» це поняття трактується як «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [1].

В роботі [2] національна безпека визначається як сукупність офіційно прийнятих поглядів на цілі і державну стратегію в області забезпечення безпеки особистості, суспільства і держави від зовнішніх і внутрішніх загроз політичного, економічного, соціального, військового, техногенного, екологічного, інформаційного та іншого характеру з урахуванням наявних ресурсів і можливостей.

В роботі [3] акцентується увага на «здатності нації задовольняти потреби, необхідні для її самозбереження, самовідтворення і самовдосконалення з

мінімальним ризиком збитку для базових цінностей її нинішнього стану».

Аналіз теоретичних напрацювань та практичного досвіду функціонування системи забезпечення національної безпеки країни [4–10] дозволив виокремити основні її елементи, які, формують певні підсистеми (рис.1.1).

Рисунок 1.1 – Структура системи забезпечення національної безпеки України

Зазначимо, що кожна з підсистем забезпечення національної безпеки спрямована на виконання поставлених завдань, що здійснюються на основі реалізації відповідного комплексу заходів відповідно до компетенцій та функцій, які здатен виконувати кожен із суб'єктів, із врахуванням актуальних викликів і загроз, використовуючи сучасні вітчизняні напрацювання у цій сфері та передовий закордонний досвід задля розвитку національних інтересів держави, добробуту її населення і ефективного функціонування системи національної безпеки в цілому.

Однак, сьогодні набувають значущості економічні, політичні та інші несилові елементи забезпечення національної безпеки, які виділено в структурі системи.

Зазначимо, що основи теорії розвитку інформаційного суспільстват закладено у працях Д. Белла [11], Б. Гейтса [12], М. Кастельса [13], Е. Тоффлера [14], в яких сформульовано певні теорії, що дозволяють оцінити наслідки впливу революції в інформаційних технологіях на розвиток країн світу та які складають теоретичний базис для подальшого формування відповідної державної політики.

Стрімкий розвиток інформаційно-комунікаційних технологій сприяв зростанню світового показника кількості користувачів мережі Інтернет до 4,021 мільярда осіб (55,6 %) від усього населення Землі та формуванню інформаційного суспільства. Найбільший рівень проникнення Інтернет – у країнах Європи (81,4 %) та Північній Америці (94,3 %). Найменший – у країнах Африки (35,2 %) [15–18].

Враховуючи кількість населення, найбільший відсоток Інтернет-користувачів в масштабах планети – у країнах Азії (50,1%), найменший – в Австралії (0,7%) (рис. 1.2).

Результати аналізу даних рис. 1.2 дозволили констатувати наряду зі зростанням кількості користувачів Інтернету по всьому світу, активізацію використання соціальних медіа, яке підвищилось за останні 12 місяців на 13%, досягнувши позначки в 3,196 мільярда користувачів. До цього ж використання соціальних медіа через мобільні пристрої виросло за рік на 14% (до 2,958 мільярда користувачів), при цьому 93 % користувачів соціальних медіа знаходять з мобільних пристроїв.

Слід вказати на той факт, що завдяки процесам розвитку комунікаційних технологій та інформаційно-телекомунікаційних систем сформувались та розвиваються інформаційний і кібернетичний простори, які здійснюють значний вплив на соціально-економічний розвиток країн світу.

Ґрунтуючись на визначенні, яке наведено в міжнародних стандартах, зазначимо, що кіберпростір – являє собою середовище існування, що створено в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за

допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі [19].

Рисунок 1.2 – Питома вага Інтернет-користувачів в світі

Зростання рівня проникнення, використання інтернету та соціальних медіа приватними особами і компаніями по всьому світу, в свою чергу, сприяє розвитку інтернет-бізнесу, що підтверджується рядом досліджень.

Так, у 2019 році загальна сума витрат на покупки товарів через електронні платформи склала 1,474 трлн. доларів, що на 16% більше, ніж в 2018 році. Така динаміка назавжди змінила поведінку користувачів, так як прості громадяни і професіонали в області бізнесу все частіше проводять дослідження, приймають рішення про покупки, шукають підтримку і рекомендують бренди в режимі онлайн.

Необхідно констатувати, що найближчим часом місяці в цифровій сфері очікуються найважливіші зміни: аудіовізуальний контент почне переважати над текстом. Соціальні відносини і онлайн-суспільства будуть розвиватися таким чином, щоб взяти на озброєння ці нові способи взаємодії людей між собою.

Американські дослідники звертають увагу на той факт, що цифрові інновації можуть створити цінний взаємозв'язок між бізнес моделями, досвідом клієнтів та операційною діяльністю [20].

Але тісніший взаємозв'язок призводить до посилення вразливості в комп'ютерних мережах та підвищення ризику для інформаційної безпеки та виникнення кібернетичних втручань, кіберінцидентів, які несуть загрози особистим, корпоративним та/або національним інтересам.

При цьому, серед основних загроз інформаційній безпеці слід віднести наступні:

- прагнення ряду країн до домінування у світовому інформаційному просторі;
- витиснення України із зовнішнього та внутрішнього інформаційного ринку;
- розроблення рядом держав концепцій інформаційних війн, які передбачають створення засобів небезпечною впливу на інформаційні сфери інших країн;
- порушення нормального функціонування інформаційних та телекомунікаційних систем, а також збереження інформаційних ресурсів, отримання несанкціонованого доступу до них;
- монополізація інформаційної сфери.

Слід вказати на той факт, що сьогодні не існує єдиного трактування поняття «кібербезпека», що спричиняє певні дискусії з цієї теми.

Так, науковці, використовуючи соціально-економічний підхід, зазначають, що кібербезпека являє собою «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційнотелекомунікаційних систем». Однак, акцент на функціонуванні інформаційнотелекомунікаційних систем «сталості розвитку» у даному визначенні та відсутність конкретизації такого впливу, робить це трактування досить широким, зміщуючи його в бік поняття «інформаційна безпека» [21].

Трактування у надто широкому сенсі з використанням соціального підходу представлено у роботі [22], де надається поняття кібербезпеці як «стану здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації.

На розгляді кібербезпеки як «стану захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж» наголошується у роботі [23], визначаючи серед основних факторів небезпеки «негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації».

На переконання деяких науковців, запропоноване у роботі [24] визначення поняття "кібербезпека" багато в чому є надмірно "конкретизованим", що потенційно може створити перешкоди пов'язані з його використанням у практичній діяльності держави. Крім того, вважаємо доцільним звернути увагу на розгляд автором поняття «кібербезпека» через призму технічного підходу.

Такий же підход використовується у роботах [25, 26], акцентуючись на безпеці об'єктів, пов'язаних з комп'ютерними технологіями (цифровими мережами) від небажаного або несанкціонованого доступу.

Згідно з затвердженим на законодавчому рівні трактуванням, кібербезпека являє собою «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [27, 28].

Звертаючи увагу на особливості та різні підходи до трактування поняття «кібербезпека» в ряді національних стратегій слід зазначити, що кожна держава самостійно встановлює основні елементи, об'єкти і суб'єкти кібернетичної безпеки, перелік її забезпечення, виходячи зі тих стратегічних цілей і завдань, які стоять перед державою на національному та міжнародному рівнях, та її практичних можливостей реалізації національних інтересів. спільним для них є забезпечення,

формування сукупності заходів (зусиль), спрямованих на запобігання, протидію, мінімізацію ризиків у кіберпросторі [28, 29].

Узагальнення підходів щодо визначення поняття «кібербезпека» дозволило сформувати її структуру та виокремити певні складові (рис. 1.3), на основні визначення яких вважаємо доцільним звернути увагу.

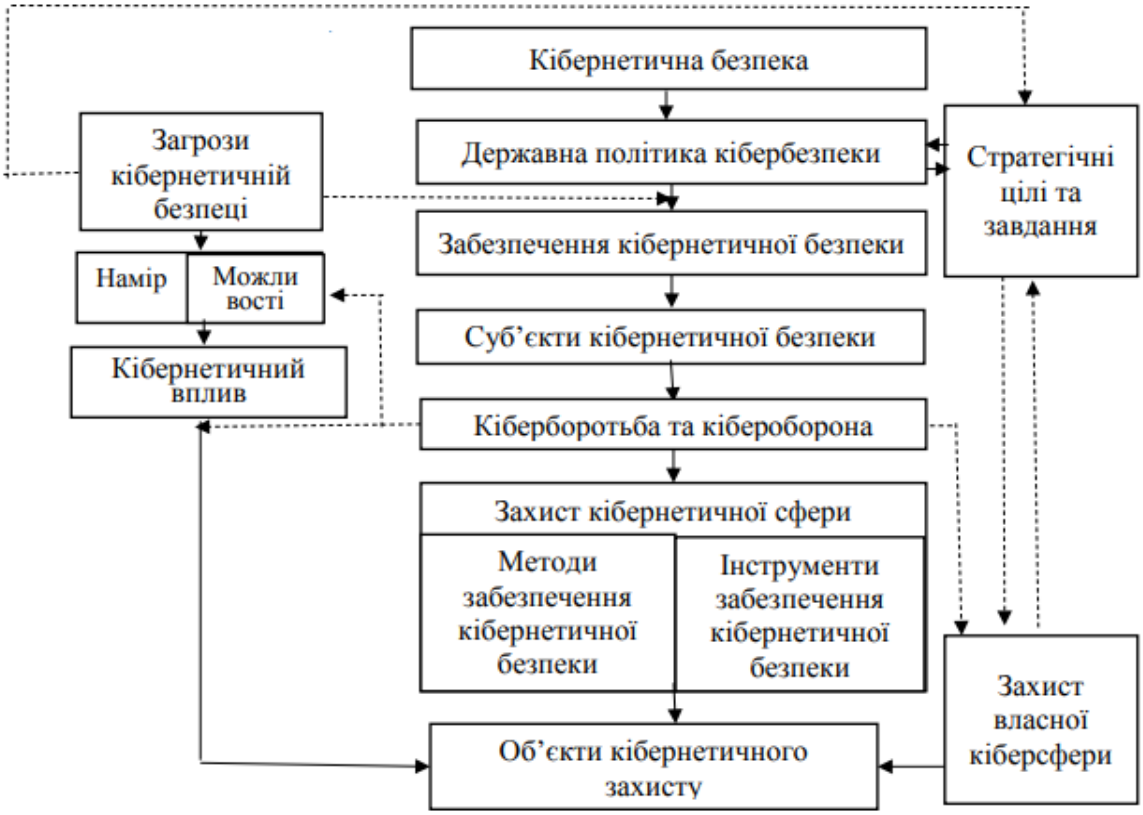

Рисунок 1.3 – Структурна модель кібербезпеки

Зазначимо, що кібернетичні впливи створюють відповідні загрози для об'єктів кібербезпеки, що потребує формування державної політики, яка базується на дієвих методах та інструментах.

На законодавчому рівні визначено, шо кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

Науковці, визначаючи термін «кіберзагроза», в свою чергу, справедливо роблять акценти не лише на безпеці держави, але звертають увагу на неї, як

«протиправні, карані дії суб'єктів інформаційних правовідносин, які створюють небезпеку життєво важливим інтересам людини, суспільства та держави в цілому»; загрозу «застосування деструктивних інформаційнопсихологічних впливів на свідомість та психічний стан населення» [27–31].

Запровадження у роботу державних структур, підприємств та організацій, життя українського суспільства сучасних інформаційно-телекомунікаційних технологій, призводить до трансформації злочинів, появи їх нових видів.

Аналогічні наголоси на «наявних та потенційно можливих явищах і чинниках, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в кібернетичній сфері» було розставлено і у відповідних Проектах Стратегії забезпечення кібернетичної безпеки України.

Тому, спираючись на законодавчу базу [32] необхідно зазначити, що кібернетичні загрози можуть виходити від:

- окремих злочинців, які мають відповідну підготовку у сфері інформаційних технологій;
- груп хакерів (в тому числі міжнародних);
- державних органів інших країн;
- фінансово-промислових груп і корпорацій; терористичних угрупованнь та інших.

Класифікація кіберзагроз за даними [33–35] наведена у табл. 1.1.

Таблиця 1.1 – класифікація кіберзагроз

КЛАСИФІКАЦІЙНА ОЗНАКА	ВИДИ КІБЕРНЕТИЧНИХ ЗАГРОЗ
1	2
Сфера спрямування	- державне управління; військова сфера; - економічна; - екологічна; - соціальна; - науково-технічна
Об'єкти спрямування або реалізації загроз	- державні органи; - бізнес структури, підприємства та організації; - об'єкти критичної інфраструктури - приватні особи.

Продовження таблиці 1.1

1	2
Суб'єкт чи носій загрози	- іноземна держава; - вітчизняні й іноземні організації, групи осіб, хакерсью угруповання; - окремі особи; - самоорганізовані технічні системи, окремі дії або цілковите функціонування яких здійснює негативний вплив на об'єкт
Середовище поширення	- інформаційне; - комунікаційне; - комп'ютерні мережі; - соціотехнічне: програмно-технічні загрози; економічні (зломи платіжних аккаунтів, фішинг-атаки); - контентні (поширення матеріалів, що порушують законодавство: терористична і екстремістська інформація; злочини проти персональних даних, честі та гідності особи;наркопропаганда тощо)
Періодичність	- повторювані (періодичні, неперіодичні); - разові
Ступень прихованості	- відкриті; - приховані
Джерело виникнення	- внутрішні (Укрнет, вітчизняний сегмент глобальної інформаційно-комунікаційної мережі); - зовнішні (здійснюються з територій інших держав); - інтегровані - одночасно відносяться до внутрішніх і зовнішніх джерел (наприклад, хакерські атаки, кібертероризм, пропаганда національної, релігійної чи будь якої іншої дискримінації)
Причини виникнення та характер спрямування	- нормативно-правові (низький рівень та дієвість запроваджених нормативно-правових актів, їх неадекватність сучасним викликам; прогалини у комплексній державній політиці забезпечення кібербезпеки); - організаційний-низький рівень підготовки фахівців та комп'ютерної грамотності населення; - інженерно-технічний - рівень захищеності інформаційно-телекомунікаційних систем від несанкціонованого доступу (захищеність програмного забезпечення; вразливість обладнання, людський фактор (забезпечення збереження та запобігання витоку секретних кодів доступу та іншої інформації)

Продовження таблиці 1.1

1	2
Відповідність основним категоріям інформації	- доступність; - цілісність; - конфіденційність
Рівень ієрархії інфраструктури	- фізичний рівень; - мережевий; - операційні системи; - системи управління базами даних; - рівень технологічних взаємовідносин і сервісів
Мета та спосіб реалізації загроз	- кібервійна; - кібертероризм; - кіберзлочинність; - кібершпигунство

Враховуючи важливість критерію мети та способу реалізації загроз, представимо їх більш докладно на рис. 1.4, визначивши серед основних такі: кібервійна, кібертероризм, кіберзлочинність та кібершпигунство.

Слід вказати на той факт, що означена сукупність ознак чи частина з них дозволяє охарактеризувати ту чи іншу загрозу, охарактеризувати її зміст, сформувати цілісну уяву, що є важливим кроком для формування складових політики кібербезпеки в частині своєчасного виявлення кіберзагроз та запровадження заходів для запобігання їм (за умов, коли загроза поки не здійснена), або стримування та протидії (якщо об'єкт зазнав кібервпливу). Запропонований перелік є відкритим задля своєчасного доповнення та коригування в залежності від змін кіберзагроз та викликів [30].

Необхідно акцентувати увагу на тому, що на протидію реальним та потенціальним сучасним кібернетичним загрозам необхідно формування відповідної сукупності заходів кіберборотьби, яка передбачає «здійснення управлінського і/або деструктивного впливу на автоматизовані ІТ-системи протиборчої сторони», запровадження комплексу кібернетичного захисту, здійснення спеціалізованих навчань [35].

В цьому контексті представляється слушною думка вітчизняних науковців, які розглядають кібербезпеку у вигляді системи, яка складається з таких підсистем: кібервпливу, кіберрозвідки та кіберзахисту.

Слід погодитись з авторами дослідження [36], які визначають цілеспрямованість цього процесу та звертають увагу на використання при кібервпливі «усього наявного комплексу засобів та заходів на визначені елементи кіберпростору з метою порушення процесів управління в кібернетичних системах протиборчої сторони шляхом зміни нормальних режимів їх функціонування з подальшим, або співвимірним у часі впливу взяттям їх під власне управління та контроль».

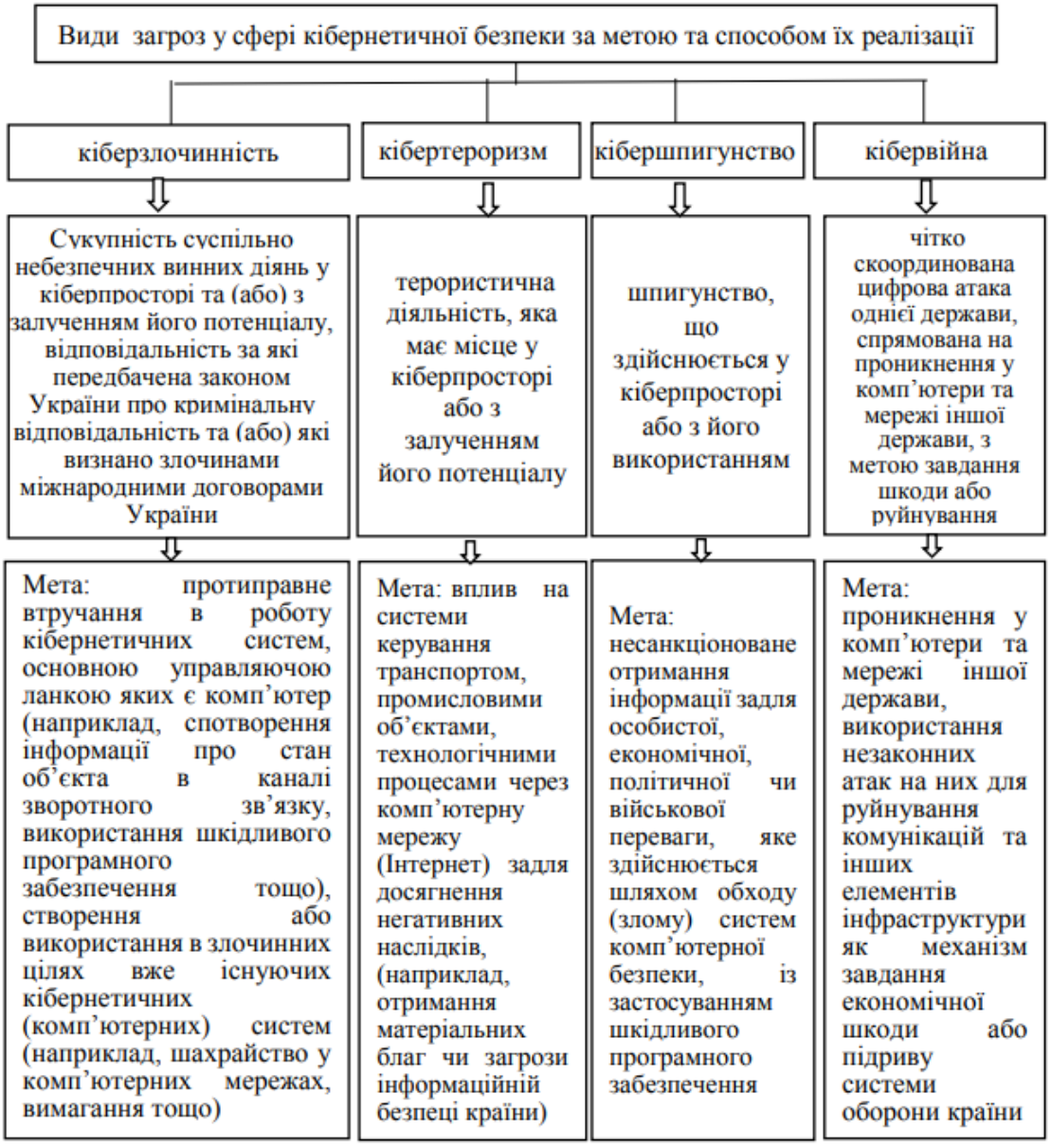

Рисунок 1.4 – Основні види загроз у сфері кібернетичної безпеки за метою та способом їх реалізації

Необхідно звернути увагу, що об'єктами такого впливу у кіберпросторі виступають технічні системи, соціотехнічні системи (наприклад, з використанням засобів масової інформації та мережі Інтернет), соціум (вплив на свідомість індивідів чи груп осіб), які зазнають фізичний, інформаційний та психологічний вплив.

Як свідчать результати досліджень, на практиці часто виникають суперечки та дискусії стосовно визначення об'єктів впливу для кібер та інформаційної безпеки в частині технічних систем. Тому, в контексті вищезазначеного вважаємо доцільним визначитись з їх розмежуванням (рис. 1.5).

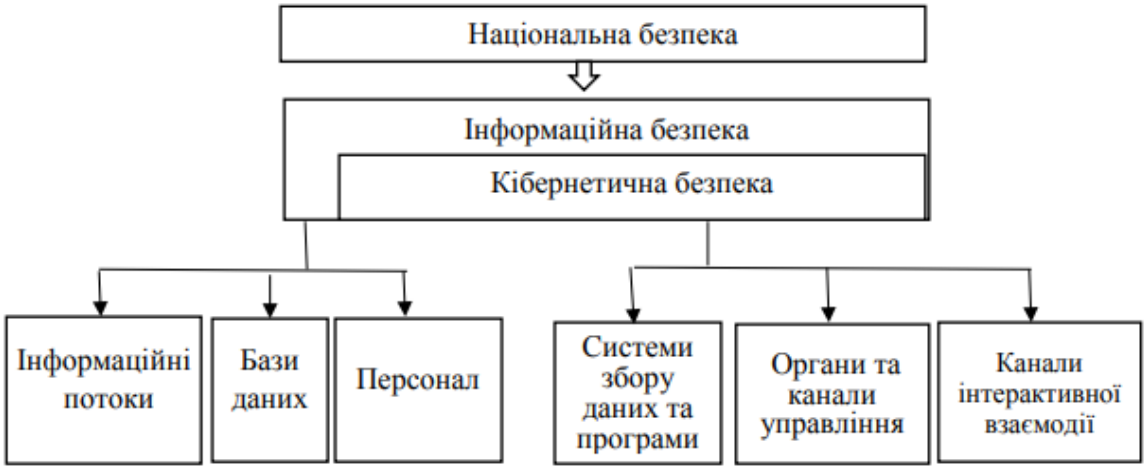

Рисунок 1.5 – Об'єкти впливу інформаційної та кібербезпеки (технічні системи)

Звертаючи увагу на підсистему кіберрозвідки слід зазначити, що вітчизняне законодавство трактує це поняття як «діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням» [27].

Зазначимо, що саме в процесі кіберрозвідки здійснюється отримання, накопичення та узагальнення даних, прогнозування потенціальних кібернетичних загроз з метою подальшого формування та реалізації комплексу заходів, спрямованих на кіберзахист об'єктів та кібервплив.

Слід вказати, що формування адекватного кіберзахисту являє собою «сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [27].

Основні об'єкти кібербезпеки та кіберзахисту, які визначено на законодавчому рівні, наведено на рис. 1.6.

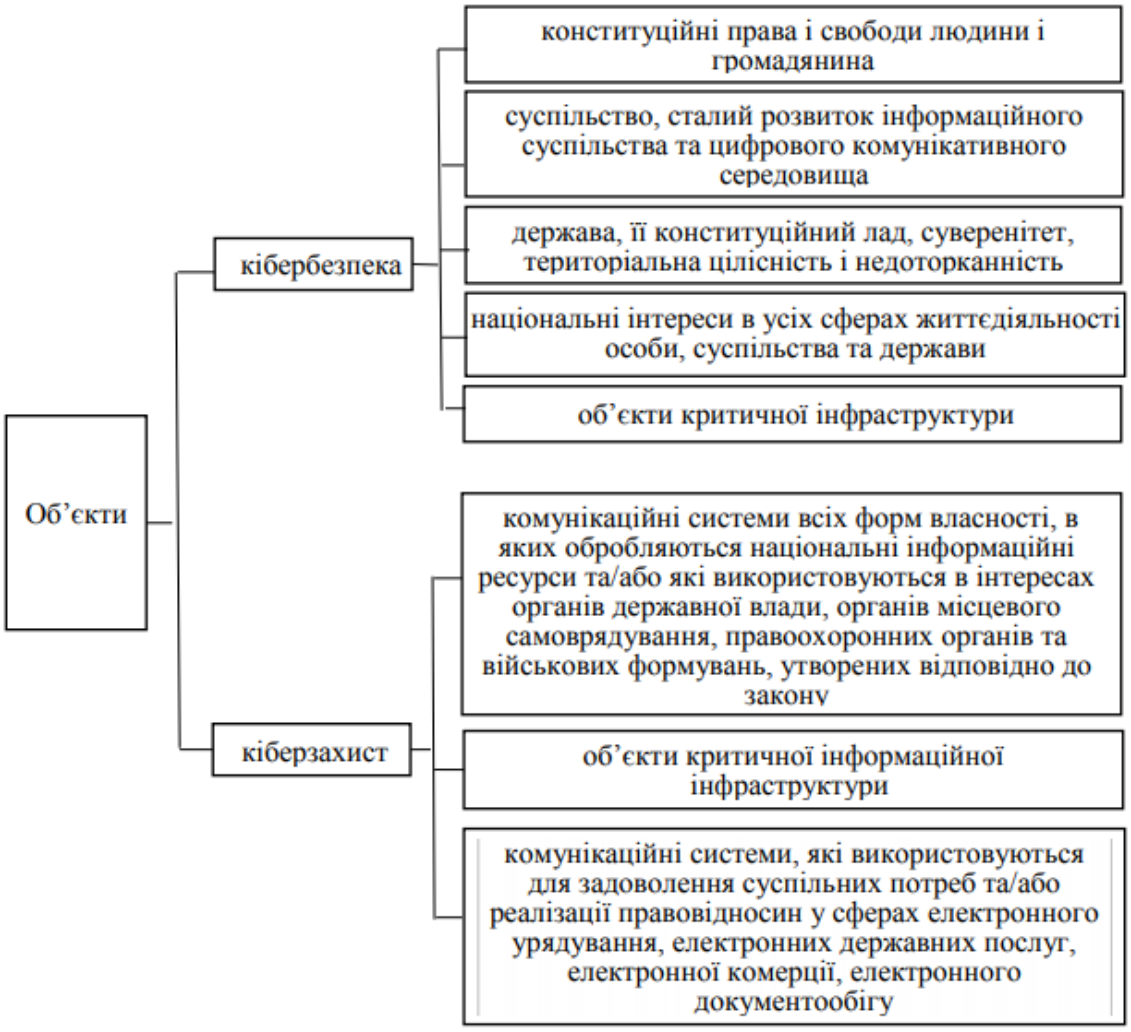

Рисунок 1.6. – Основні об'єкти кібербезпеки та кіберзахисту

Згідно з Законом України «Про основні засади забезпечення кібербезпеки України» до об'єктів критичної інфраструктури відносяться підприємства, установи

та організації, які діють в «галузях енергетики, хімічної промисловості, транспорту, інформаційно- комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах, надають послуги у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; комунальні, аварійні та рятувальні служби, служби екстреної допомоги населенню, включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави, є об'єктами потенційно небезпечних технологій і виробництв» [27].

Тому, в контексті даної магістерської роботи акцентуємо увагу на тому, що серед об'єктів з критичною інформаційною інфраструктурою, які потенційно можуть підвергатися кібернетичним впливам, слід відзначити такі:

- державні електронні інформаційні ресурси;
- спеціалізовані телекомунікаційні системи та ті, що створено для загального користування;
- автоматизовані системи управління, в тому числі виробничими процесами, що мають місце на підприємствах (незалежно від форми власності), які є стратегічними для національної економіки або безпеки держави;
- електронні інформаційні ресурси, на яких зберігається або обробляється інформація, яка входить до сфери забезпечення національних інтересів держави;
- електронні інформаційні ресурси та автоматизовані системи управління у військовій сфері тощо.

Тому, захист критичної інфраструктури має ґрунтуватись на наступних засадах:

- визнання необхідності забезпечення безперервності та стійкості функціонування критичної інфраструктури;
- визначення законодавчих вимог до її захисту;

- створення умов, спрямованих на мінімізацію реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів;
- створення умов швидкого відновлення функціонування критичної інфраструктури у випадку реалізованих загроз, кризових ситуацій; створення системи виявлення загроз;
- запровадження взаємодії держави, суб'єктів господарювання, експертного середовища та населення з питань забезпечення захисту та стійкості критичної інфраструктури;
- забезпечення міжнародного співробітництва у сфері захисту критичної інфраструктури.

1.2. Основні аспекти державної політики забезпечення кібербезпеки України

Формування основних аспектів забезпечення кібербезпеки України здійснюється на основі відповідної державної політики, яка є самостійним напрямом політики національної безпеки.

Визначаючи основи державної політики забезпечення кібербезпеки, необхідно розглянути відповідну дефініцію.

Аналіз визначення поняття «державна політика» дозволив дійти висновку стосовно різноманітності підходів до його трактування різними науковцями.

Зазначимо, що у широкому сенсі вітчизняні дослідники пропонують розглядати державну політику як: «основні принципи, норми та діяльність зі здійснення державної влади»; «діяльність, результати якої набувають статусу офіційних; «сукупність цілей і завдань, що практично реалізується державою»; «стратегічну лінію поведінки держави в тих чи інших сферах суспільного життя»; «сукупність ціннісних цілей, державно-управлінських заходів, рішень і дій, порядок реалізації державно-політичних рішень»; «набір цінностей, цілей та знарядь, пов'язаних із визначенням суспільних проблем» [37, 38].

Аналогічний широкий підхід до трактування терміну «державна політика» використовують і деякі закордонні науковці, визначаючи її як: «складні взаємозв'язки форм влади, типи проблем та організації держав в особливих підсистемах суспільства; «заплановану програму цілей, цінностей і дій».

Ряд науковців трактує поняття «державна політика» у вузькому сенсі, з більшою конкретизацією цілей, процесів та результатів, визначаючи дефініцію, як [39]:

- пропонований курс діяльності уряду для задоволення потреб чи використання можливостей, сформульований із зазначенням очікуваних результатів та їх впливу на наявний стан справ і конкретне розв'язання проблем;
- дії системи органів державної влади згідно з визначеними цілями, напрямами, принципами для розв'язання проблем у певній сфері суспільної діяльності;
- сукупність організаційних, правових та економічних заходів, які здійснюються державними органами в усіх сферах суспільного життя та реалізуються у напрямах залежно від стратегічних завдань, поставлених перед державою;
- безперервний циклічний процес, що складається із сукупності послідовних дій, взаємодії елементів інститутів з певними функціями, засобів, які спрямовані на досягнення певного наслідку;
- ухвалене на конституційних засадах із залученням громадськості стратегічне рішення з чітким визначенням результатів, яке є засобом забезпечення суспільних потреб у тій чи іншій сфері і реалізується органами державного управління.

Таким чином, під державною політикою в сфері кібербезпеки слід розуміти засновану на чинних нормативно-правових актах, узгоджену за цілями систему державно-управлінських заходів з боку органів державної влади, спрямовану на реалізацію функцій держави стосовно забезпечення безпечності кіберпростору,

мінімізації наслідків будь-яких кібератак, кіберінцидентів та кіберзагроз, нейтралізацію потенційно шкідливих наслідків як на рівні держави, так і приватних користувачів Інтернету, недопущення посягань на об'єкти національної критичної інформаційної інфраструктури з метою своєчасного запровадження дієвих заходів, адекватних характеру і масштабам реальних та потенційних кіберзагроз, спрямованих на захист інтересів людини, суспільства та держави у кіберпросторі.

Вважаємо доцільним, визначаючи основи державної політики забезпечення кібернетичної безпеки, звернути увагу на структуру відносин в цій сфері і визначити її суб'єкт і об'єкт.

Це обумовлено тим, що саме суб'єкт та об'єкт державної політики, вступаючи в певні взаємозв'язки між собою та зовнішнім середовищем, утворюють систему державного управління, яка спрямована на забезпечення кібернетичного захисту.

На державному рівні визначено, що суб'єкти забезпечення кібербезпеки у межах своєї компетенції:

- здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;
- здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;
- здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз; розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;
- забезпечують проведення аудиту інформаційної безпеки та інші заходи.

Визначаючи суб'єктів державної політики забезпечення кібернетичної безпеки, слід погодитись з думкою І. Діордіци, який звертає увагу на необхідність їх розподілу на дві групи: загальні та спеціалізовані (уповноважені здійснювати боротьбу з кіберзлочинністю та захист об'єктів національної критичної інфраструктури).

Вважаємо, що такий підхід є раціональним з точки зору виокремлення функцій та повноважень при формуванні та реалізації державної політики. Основні суб'єкти забезпечення кібернетичної безпеки наведено на рис. 1.7 [27, 28].

Розглянемо більш детально специфіку діяльності визначених спеціалізованих суб'єктів, які складають основу національної системи кібербезпеки з точки зору організаційного виміру.

На законодавчому рівні на Міністерство оборони та Генштаб Збройних сил України покладена зобов'язаність забезпечувати кібероборону військових об'єктів, кіберзахист об'єктів критичної інфраструктури під час війни і надзвичайного стану, а також відбивати військову агресію в кіберпросторі.

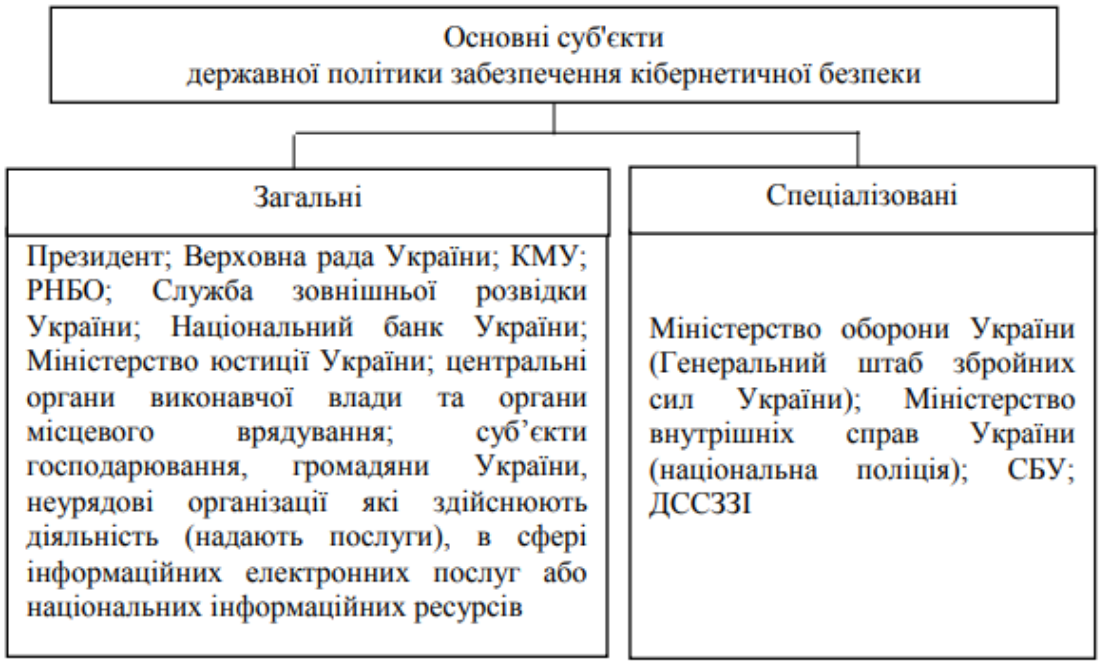

Рисунок 1.7. – Основні суб'єкти державної політики забезпечення кібернетичної безпеки

Серед підрозділів, які відповідальні за забезпечення кібернетичної безпеки країни, слід виокремити війська радіоелектронної боротьби і фахівців Головного управління розвідки. До задачі перших відноситься захист систем управління військами та зброєю від навмисних радіоелектронних перешкод противника, а також порушення роботи інформаційних систем управління противника.

Фахівці Головного управління розвідки беруть участь у здійсненні спеціальних заходів щодо забезпечення національних інтересів в інформаційній сфері (розвідувальні заходи, інформаційне шпигунство, розшукові заходи). Слід підкреслити, що робота Головного управління розвідки в сфері кібернетичної безпеки країни є секретною.

У структурі МВС України діє спеціальний підрозділ – Департамент кіберполіції, який є міжрегіональним територіальним органом Національної поліції України, входить до структури кримінальної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність.

Серед основних його завдань слід виокремити такі: участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку; завчасне інформування населення про появу нових кіберзлочинців; впровадження програмних засобів для систематизації кіберінцидентів; реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної Цілодобової мережі контактних пунктів

СБУ в межах своїх повноважень зобов'язана попереджати, виявляти, припиняти та розкривати злочини проти миру та безпеки людства в кібер- просторі, боротися з кібертероризмом і кібершпигунством, проводити таємні перевірки об'єктів критичної інфраструктури.

Зазначимо, що у складі Центрального управління СБУ створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, який сприятиме концентрації сил і засобів, оптимізації управлінської діяльності у вирішенні завдань із захисту законних інтересів держави та прав громадян в інформаційній сфері від розвідувально-підривної діяльності іноземних спецслужб, протиправних посягань організацій, груп і осіб. Робота Департаменту засекречена,

проте судити про результати можна за кількістю повідомлень про знешкодження хакерських груп і «телефонних терористів».

ДССЗЗІ є поки єдиною структурою в Україні, яка цілеспрямовано займається питаннями кібернетичної безпеки. Вона створена відповідно до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», становить основу національної системи кібербезпеки і приймає участь у формуванні та реалізації державної політики в сфері захисту державних інформаційних ресурсів, криптографічного і технічного захисту інформації. На ДССЗІ (разом з СБУ) покладене одне з основних завдань - взаємодія з Міністерством оборони у забезпеченні кіберзахисту інформаційної інфраструктури. Її робота спрямована на захист державної інфраструктури. В контексті дослідження на особливу увагу заслуговують такі підрозділи служби:

Computer Emergency Response Team of Ukraine (CERT-UA). Серед основних його завдань слід виокремити такі: запобігання, виявлення і усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно- телекомунікаційних системах; консультаційна та методична допомога в питаннях захисту державних інформаційних ресурсів; взаємодія з міжнародними організаціями реагування на несанкціоновані дії (наприклад, з Форумом команд реагування на інциденти безпеки – FIRST). На жаль, ресурсів CERT-UA бракує для того, щоб забезпечувати захист не тільки державних інформаційних ресурсів, але й приватних компаній і користувачів;

Центр антивірусного захисту інформації (ЦАЗІ). Його мета –забезпечення єдиної системи антивірусного захисту державних інформаційних ресурсів. Однак, в Україні досі не існує державного проекту зі створення національного антивірусу, що є серйозним упущенням враховуючи той факт, що в країні вже існують компанії, які володіють антивірусними продуктами високої якості і ефективності.

Дослідження теоретичного підгрунтя та державотворчих процесів у сфері кіберзахисту створили базу для пропозиції авторського бачення моделі державного управління кібернетичною безпекою, яка включає управлінську, організаційно-

забезпечуючу, результативну складові та комплекс інструментів управлінського впливу та є основою для формування державної політики забезпечення кібернетичної безпеки, спрямованої на формування безпечного кібернетичного простору (рис. 1.8).

Слід вказати, що до процесів формування і реалізації державної політики забезпечення кібербезпеки можуть залучатись підприємства, організації різних форм власності, неурядові (волонтерські) організації.

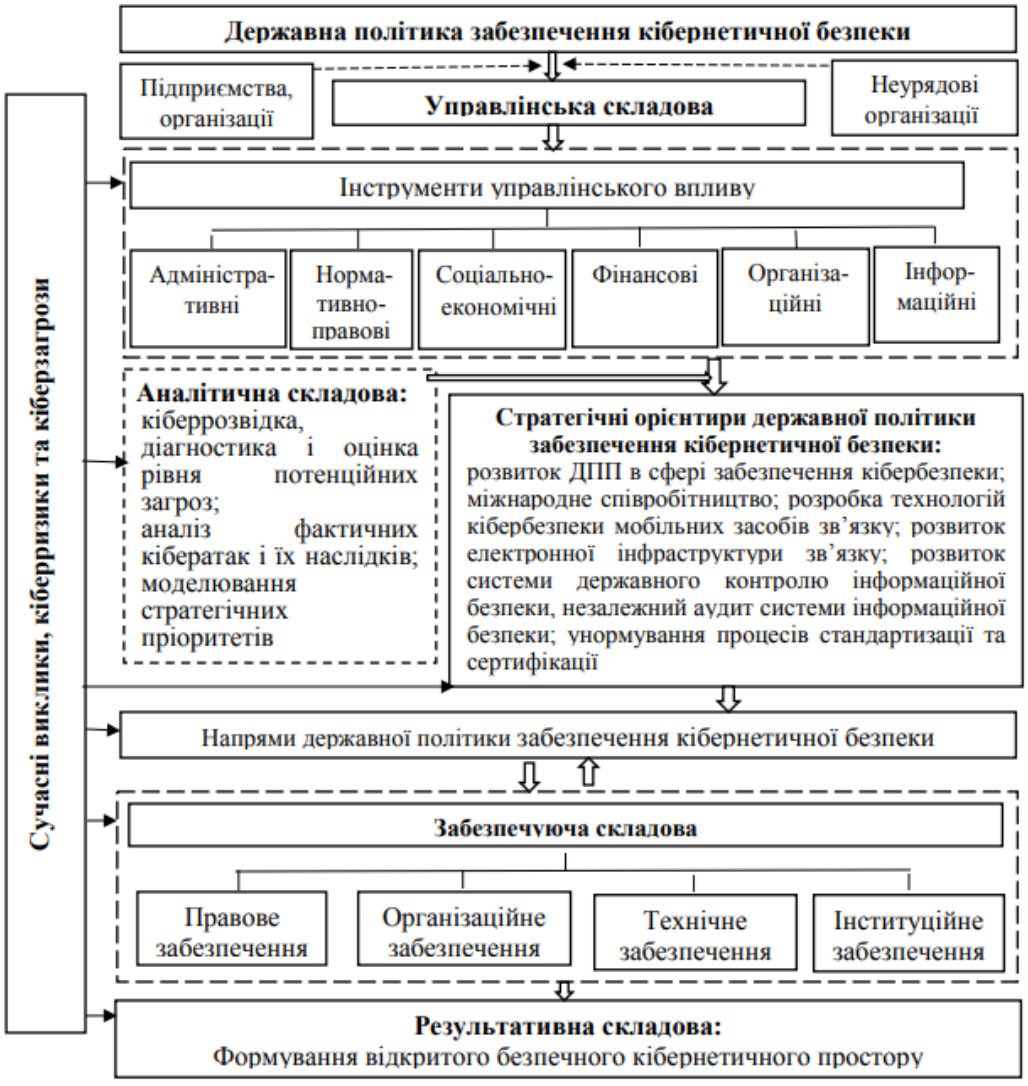

Рисунок 1.8 – Модель державного управління кібернетичною безпекою

Зазначимо, що для досягнення результату - формування безпечного кібернетичного простору - є необхідним належне правове, організаційне, технічне,

інституційне забезпечення, яке є елементами забезпечуючої складової і формується відповідно до сформульованих на основі визначених управлінських орієнтирів напрямів державної політики забезпечення кібернетичної безпеки.

Обґрунтованість управлінських орієнтирів та напрямів державної політики досягається на основі аналітичної складової, яка передбачає використання методів кіберрозвідки, діагностик і оцінку рівня потенційних загроз; аналіз фактичних кібератак і їх наслідків, моделювання стратегічних пріоритетів забезпечення кібернетичної безпеки.

Необхідно звернути увагу, що формування та реалізація державної політики забезпечення кібербезпеки здійснюється на основі сукупності принципів.

Зазначимо, що основні з них виокремлено на законодавчому рівні. Серед основних з них:

- верховенства права і поваги до прав та свобод людини і громадянина; забезпечення національних інтересів України;
- відкритості, доступності, стабільності та захищеності кіберпростору;
- широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту;
- пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам;
- пріоритетності запобіжних заходів; невідворотності покарання за вчинення кіберзлочинів; пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу; міжнародного співробітництва;
- забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки.

Однак, враховуючи специфіку і масштабність сучасних кіберзагроз, задля розв'язання актуальних питань в сфері кіберзахисту, розробки ефективних, дієвих

державно-управлінських рішень та формування адекватної викликам державної політики в зазначеній сфері, ці принципи потребують уточнення та коригування.

Тому, вважаємо за доцільне звернути увагу додатково на такі принципи формування державної політики забезпечення кібернетичної безпеки [39]:

- системності – актуалізація цілей, визначення методів та інструментів для використання суб'єктами державної політики забезпечення кібербезпеки повинні здійснюватися в системі з іншими сферами діяльності країни, з врахуванням нових потенційних і реальних кібервикликів та загроз;
- координованості – досягнення узгодженості пріоритетів та дій суб'єктів державної політики забезпечення кібербезпеки, які впливають на попередження кібервпливів, нівелювання їх наслідків;
- синергії –- синхронізація основних дій, які здійснюються суб'єктами державної політики забезпечення кібербезпеки і спрямовані на забезпечення відкритого безпечного кібернетичного простору;
- концептуального підходу – розробка та запровадження основоположного документу (концепції), який би започатковував основні напрями відповідної державної політики, створював підґрунтя для формування сучасної, адекватної існуючим викликам політики кібербезпеки і яким би керувалася як держава, так і підприємства, незалежно від форми власності, при визначенні напрямів діяльності, спрямованої на захист у кіберпросторі;
- програмного підходу реалізація державної політики забезпечення кіберзахисту повинна здійснюватися на основі взаємопов'язаних програм в рамках сучасної Стратегії кібернетичної безпеки України.

Зазначимо, що систематизація підходів до розуміння державотворчих процесів в цій сфері дозволяє інтегрувати відповідні наукові знання та надає можливість практикам формувати ефективні, раціонально виважені державно-управлінські рішення, спрямовані на комплексне вирішення проблеми кіберзахисту.

Реальні прояви кібератак здатні призвести до порушень функціонування інформаційно-телекомунікаційних систем, які безпосередньо впливають на стан національної безпеки і оборони.

У зв'язку із цим існуючі загрози вимагають формування та реалізації державної політики забезпечення кібернетичної безпеки, яка має бути спрямована на забезпечення інформаційного суверенітету України у кіберпросторі, створення надійного захисту національного сегменту кіберпростору в умовах антитерористичної операції; зміцнення обороноздатності держави у кіберпросторі; боротьбу з кіберзлочинністю та кібертероризмом; недопущення та запобігання втручанню у внутрішні справи України і припинення посягань на її Інтернет-ресурси з боку інших держав.

Висновки до розділу 1

1. Сьогодні Україна зазнає значного впливу інцидентів та атак в кібернетичній сфері, що обумовлює необхідність своєчасного виявлення, запобігання й нейтралізації реальних і потенційних кібернетичних втручань і загроз особистим, корпоративним та національним інтересам.

2. Державна політика в сфері кібербезпеки заснована на чинних нормативно-правових актах, які спрямовані на реалізацію функцій держави стосовно забезпечення безпечності кіберпростору, мінімізації наслідків будь-яких кібератак, кіберінцидентів та кіберзагроз, нейтралізацію потенційно шкідливих наслідків як на рівні держави, так і приватних користувачів Інтернету, недопущення посягань на об'єкти національної критичної інформаційної інфраструктури з метою своєчасного запровадження дієвих заходів, адекватних характеру і масштабам реальних та потенційних кіберзагроз, спрямованих на захист інтересів людини, суспільства та держави у кіберпросторі.

3. Встановлено, що модель державного управління кібернетичною безпекою повинна містити такі основні складові: управлінську, забезпечуючу, результативну, а також комплекс засобів і інструментів управлінського впливу та є основою для забезпечення кібернетичної безпеки, спрямованої на створення безпечного кібернетичного простору.

РОЗДІЛ 2
ОЦІНКА ВРАЗЛИВОСТІ ОБ'ЄКТІВ КІБЕРЗАХИСТУ НА ОСНОВІ РИЗИКО-ОРІЄНТОВАНОГО ПІДХОДУ

2.1. Умови функціонування комплексної системи кібербезпеки в зоні контролю навколо об'єктів кіберзахисту

Територія України, як система з територіально-часовим розподілом параметрів життєдіяльності – рис. 2.1, у процесі свого функціонування та розвитку створює передумови для виникнення небезпек, які негативно впливають на стан природно-екологічного, економіко-технічного та соціально-політичного балансу на її території [40–49].

У відповідності до рис. 2.1, джерело інтегральної небезпеки в точці $A(x,y,z)$ локальної території (як елементу функціональної поверхні, горизонтальні проекції якої співпадають з конфігурацією локальної території, а її випуклості відповідають рівням небезпеки в містах з конкретними географічними координатами) нелінійно об'єднує джерела природної небезпеки [50–52]: $1'$ – процеси у атмосфері; $2'$ – процеси у біосфері; $3'$ – процеси у літосфері; $4'$ – процеси у гідросфері; джерела техногенної небезпеки [53–56]: $1''$ – аварії на промислових об'єктах і транспорті; $2''$ – вибухи; $3''$ – пожежі; $4''$ – вивільнення інших видів енергії; джерела соціальної небезпеки [57–60]: $1'''$ – психологічні особливості особи й особливості виховання; $2'''$ – несприятливе положення особи; $3'''$ – соціальна несправедливість; $4'''$ – напруженість у міжгрупових, міжконфесійних і міжнаціональних стосунках; $5'''$ – негативні соціальні процеси, що призводять до руйнування етичних засад, соціальної стійкості особи та законослухняності; джерела воєнної небезпеки [61–63]: $1''''$ – наявність гострих суперечностей, розв'язання яких є можливим лише із застосуванням воєнної сили; $2''''$ – наявність у однієї із сторін достатньої кількості військових сил і засобів для розв'язання суперечності на свою користь або здатність держави створити такі сили в перспективі; $3''''$ – наявність у лідерів або урядів

політичної волі та рішучості піти на застосування сили, здатності використовувати збройні сили для вирішення можливого конфлікту; $4''''$ – наявність надійних союзників серед держав, їх коаліцій або інших суб'єктів військово-політичних відносин; $5''''$ – сприятливі геополітичні умови та реальна (або прогнозована) військово-політична обстановка для здійснення військових акцій.

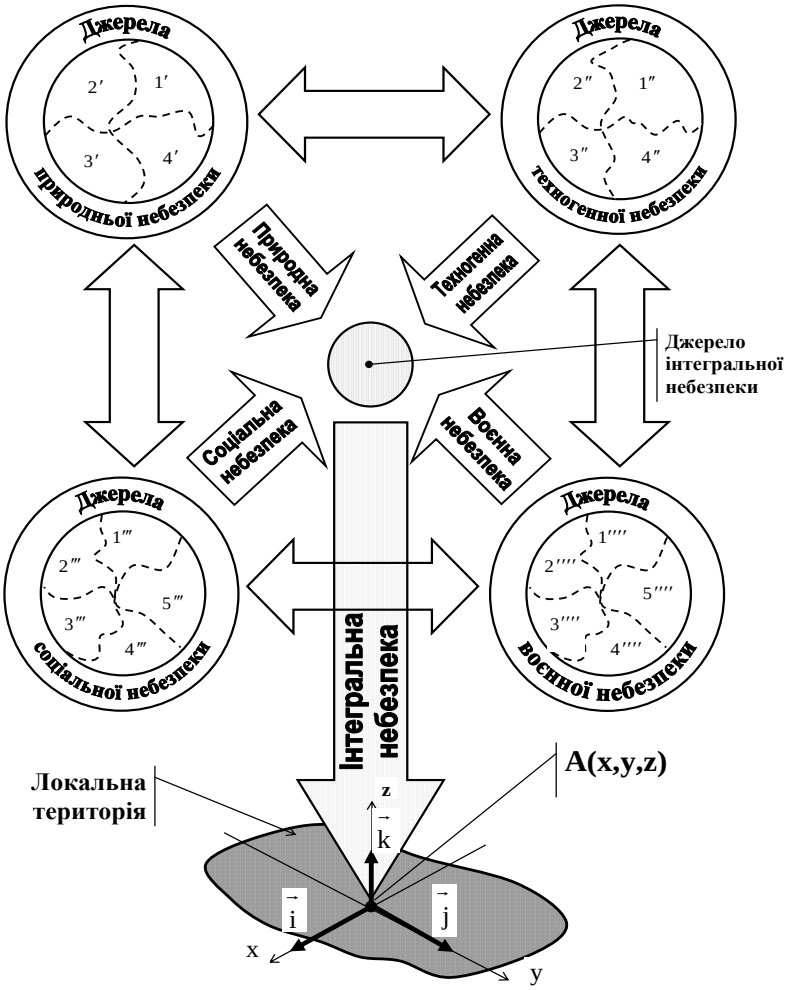

Рисунок 2.1 – Модельне представлення процесів зародження в зоні безпеки навколо об'єктів кіберзахисту джерел небезпек різного походження

В Україні для забезпечення реалізації державної політики у сфері цивільного захисту функціонує Єдина державна система цивільного захисту (ЄДСЦЗ), яка складається з функціональних і територіальних підсистем та спрямована на розв'язання питань забезпечення необхідного рівня безпеки життєдіяльності території держави лише в умовах, коли виникла НС.

При цьому, цілковито відкритими для держави залишаються проблемні питання реалізації, базуючись на уявленнях системного підходу та за даними рис. 2.2, в системі ЄДСЦЗ функції моніторингу та розробки ефективних управлінських рішень всіх локальних підсистем, спрямованих на попередження та локалізацію НС, в умовах зародження джерел небезпек різної природи [64].

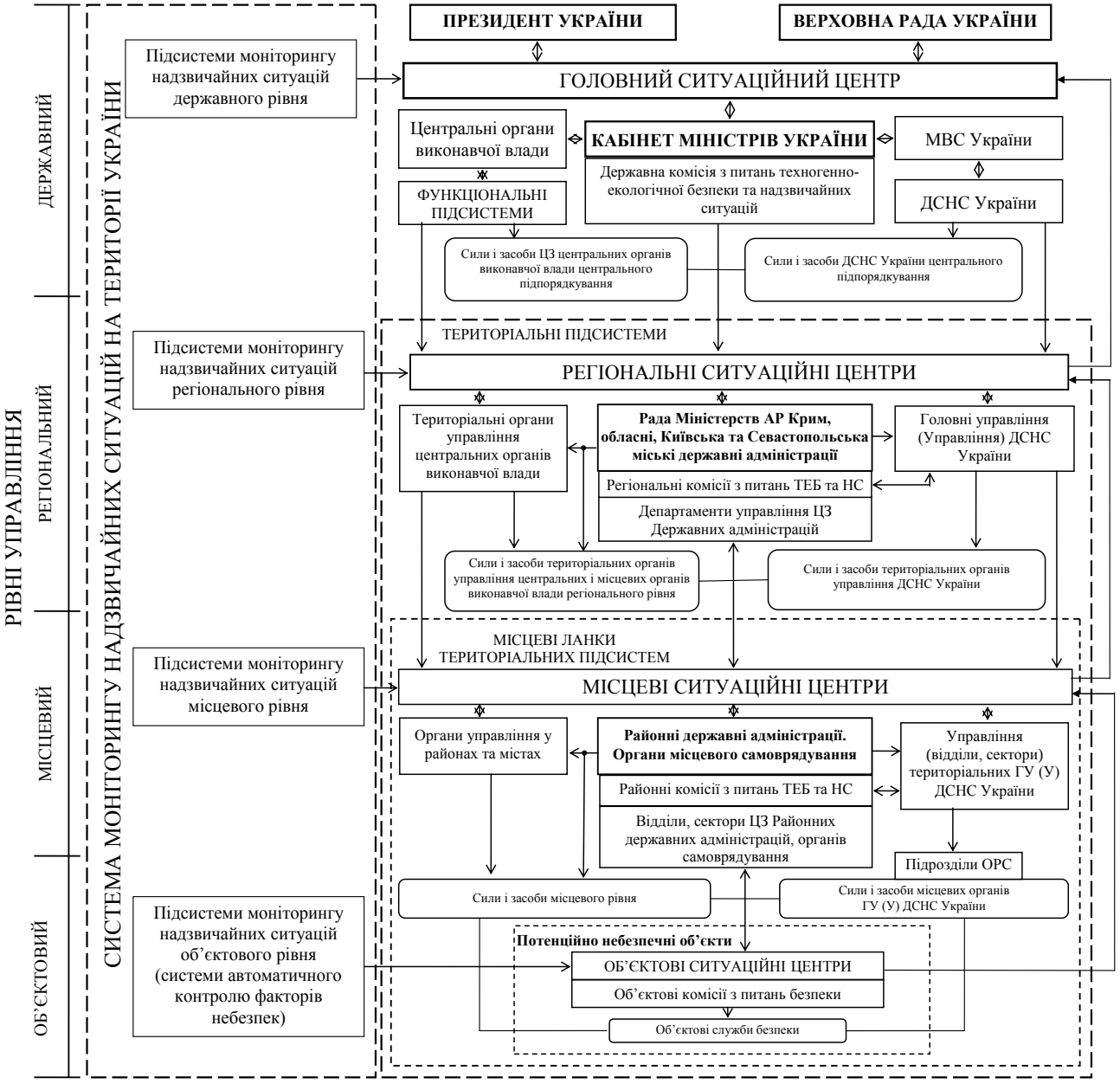

Рисунок 2.2 – Комплексна функціональна схема інформаційно-аналітичної підсистеми управління процесами попередження, локалізації та ліквідації наслідків НС у Єдиній державній системі цивільного захисту

Це вказує на необхідність термінового розв’язання питань включення до складу ЄДСЦЗ інформаційно-аналітичної підсистеми управління процесами попередження й локалізації наслідків НС.

Створення ефективної інформаційно-аналітичної підсистеми управління процесами попередження й локалізації наслідків НС пропонується у відповідності за підходом, який розроблено у роботах та графічно представлено на рис. 2.2. У цьому підході реалізовано комплексне включення в діючу систему ЄДСЦЗ по вертикалі від об’єктового до державного рівнів різних функціональних елементів територіальної підсистеми моніторингу НС та складових підсистеми ситуаційних центрів, які жорстко пов’язані між собою на інформаційному та виконавчому рівнях для прийняття відповідних антикризових рішень для розв’язання різних функціональних задач моніторингу, попередження та ліквідації НС природного, техногенного, соціального та воєнного характеру [65].

Однією з важливих функцій інформаційно-аналітичної підсистеми управління процесами попередження й локалізації наслідків НС Єдиної державної системи цивільного захисту є забезпечення кібербезпеки нормальних умов функціонування об’єктів критичної інфраструктури, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення. Виведення з ладу або порушення функціонування цих об’єктів може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, а також заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей [27–29].

До об’єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які [27, 66]:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і

газу, виробництва продуктів харчування, сільського господарства, охорони здоров’я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об’єктами потенційно небезпечних технологій і виробництв. Ці об’єкти у процесі свого функціонування потребують забезпечення відповідного рівня їх кіберзахисту, шляхом комплексної реалізації організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації.

Об’єктами кіберзахисту (ОКЗ) в державі є [27–29, 66]:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об’єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Середовищем (віртуальним простіром), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних є кіберсередовище.

Особливості функціонування в кіберпросторі рознесених по території України ОКЗ схематично представлені на рис. 2.3, де передача даних між цими об’єктами здійснюється в умовах імовірнісного територіально-часового прояву кібервійни, кібертероризму, кібершпигунства та кіберзлочинності.

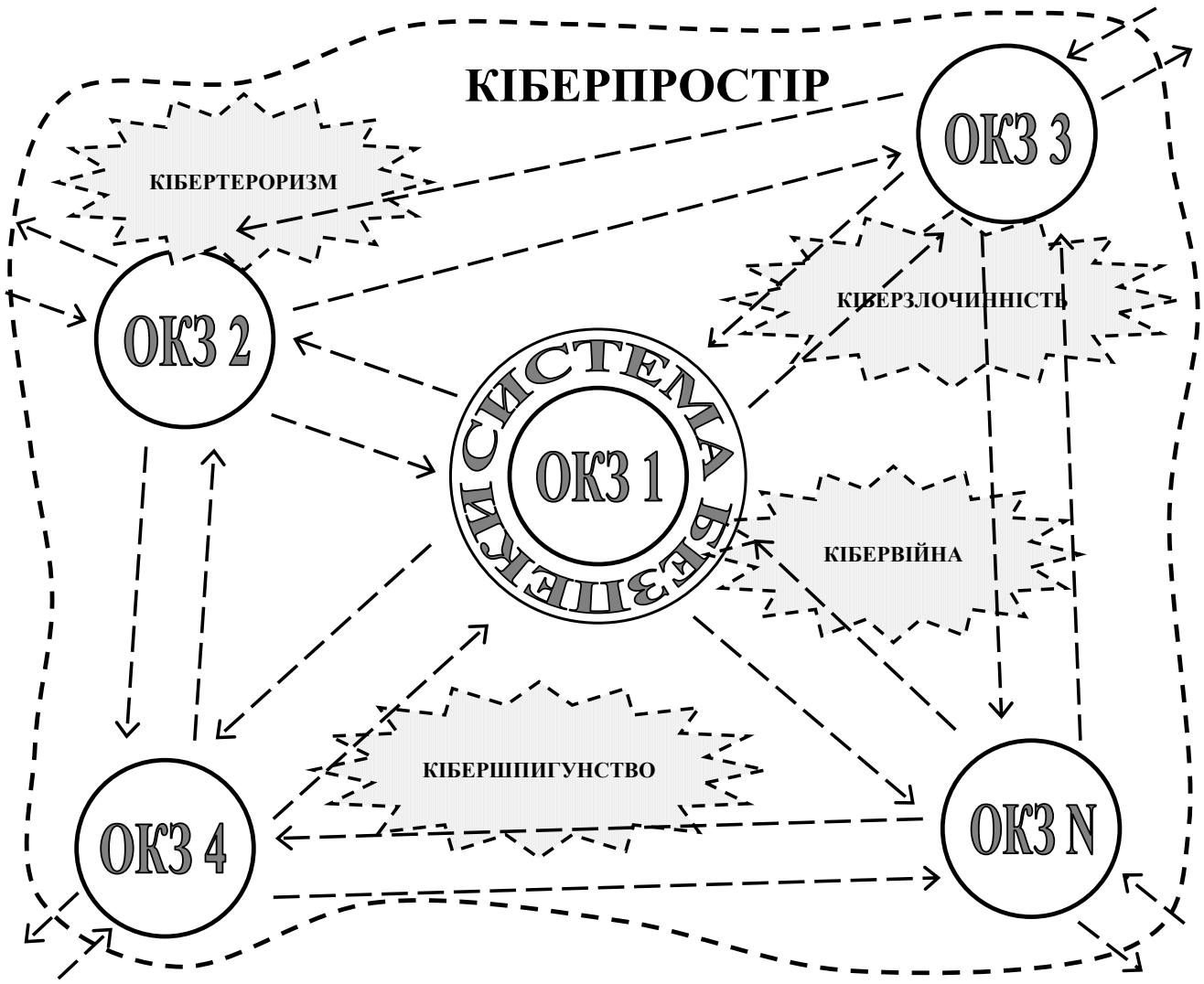

Рисунок 2.3 – Особливості функціонування в кіберпросторі рознесених по території України об’єктів кіберзахисту

Крім того, результати аналізу даних рис. 2.3 вказують на відсутність чітких меж та установлених метричних розмірів кіберпростору для ОКЗ, що ускладнює функціонування відповідної системи безпеки щодо забезпечення відповідного рівня кібербезпеки ОКЗ України.

В той же час, забезпечення безпеки функціонування ОКЗ вимагає використання різних технічних засобів. Це, в першу чергу, інженерно-технічний захист безпосередньо самої інформації і засоби охорони об'єктів, які і є об'єктами охорони – охоронна сигналізація, телевізійні системи відеоспостереження, системи контролю і управління доступом, інженерна укріплених об'єктів. На рис. 2.4 представлена схема організації захисту інформації ОКЗ з використанням технічних засобів.

Організація захисту інформації (рис. 2.4) визначає зміст і порядок дій щодо забезпечення захисту інформації [67–69].

Основні напрямки в організації захисту інформації визначаються системою захисту інформації, заходами щодо захисту інформації та заходами по контролю ефективності захисту інформації.

Пропонована система захисту інформації – це сукупність органів та / або виконавців щодо захисту інформації, що використовується ними техніки захисту безпосередньо самої інформації, а також об'єктів інформатизації, організованих і функціонують з урахуванням вимог відповідних правових, організаційно-розпорядчих та нормативних документів щодо захисту інформації.

Заходи щодо захисту інформації визначають сукупність дій з розробки та / або практичного застосування способів і засобів захисту інформації, а заходи по контролю ефективності захисту інформації – сукупність дій з розробки та / або практичного застосування методів (способів) і засобів контролю ефективності захисту інформації.

Мінімізація витрат на захист інформації вимагає оптимального використання досить дорогих технічних засобів.

В якості одного з напрямків мінімізації витрат може бути побудова системи захисту об'єкта з суміщенням зони R_2 і контрольованої зони об'єкта (рис. 2.5).

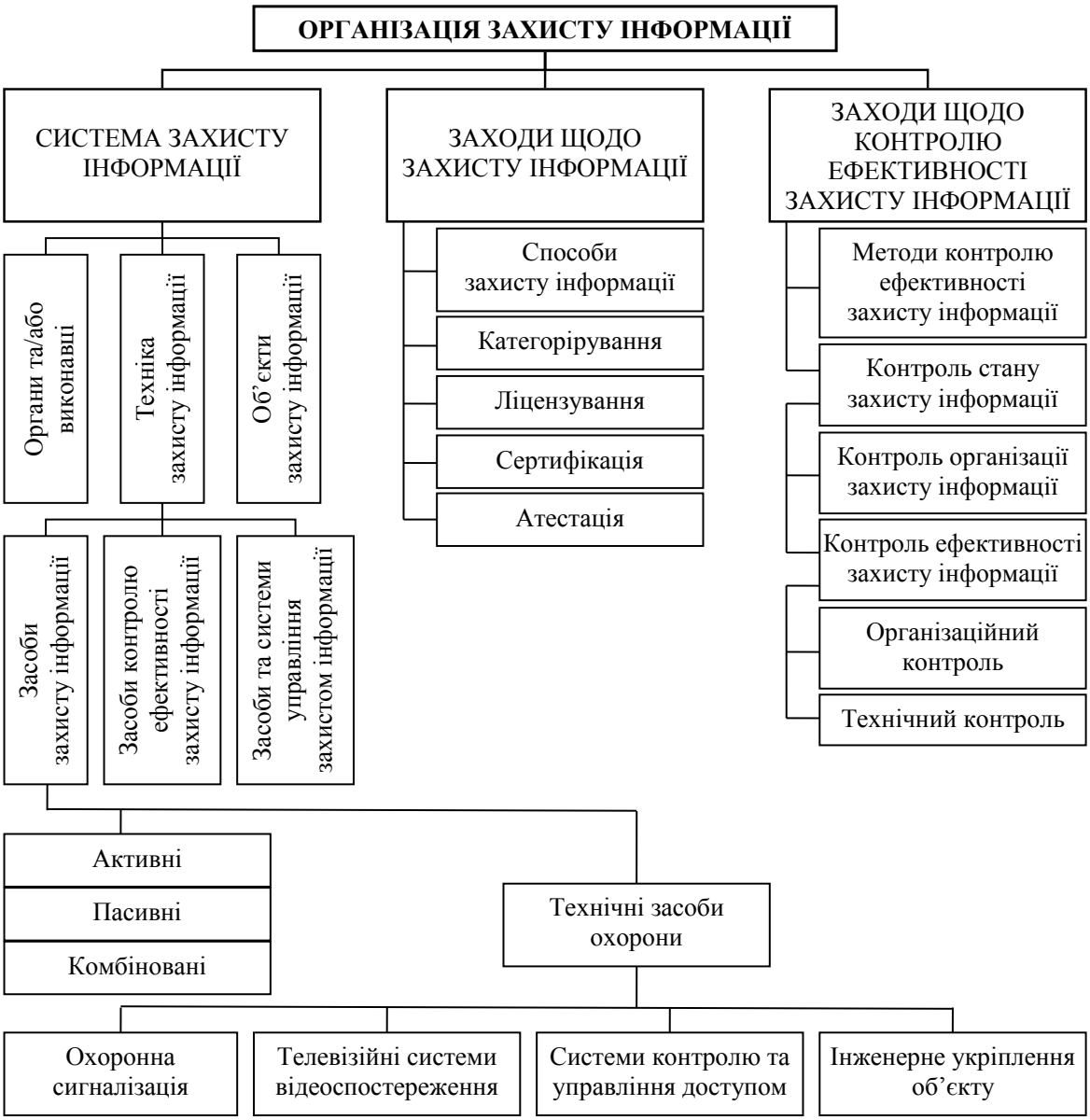

Рисунок 2.4 – Організація захисту інформації з використанням технічних засобів

Особливого значення набуває захист контрольованої зони об'єкту кіберзахисту.

Контрольована зона – територія об'єкта, на якій виключено неконтрольоване перебування осіб, які не мають постійного або разового допуску.

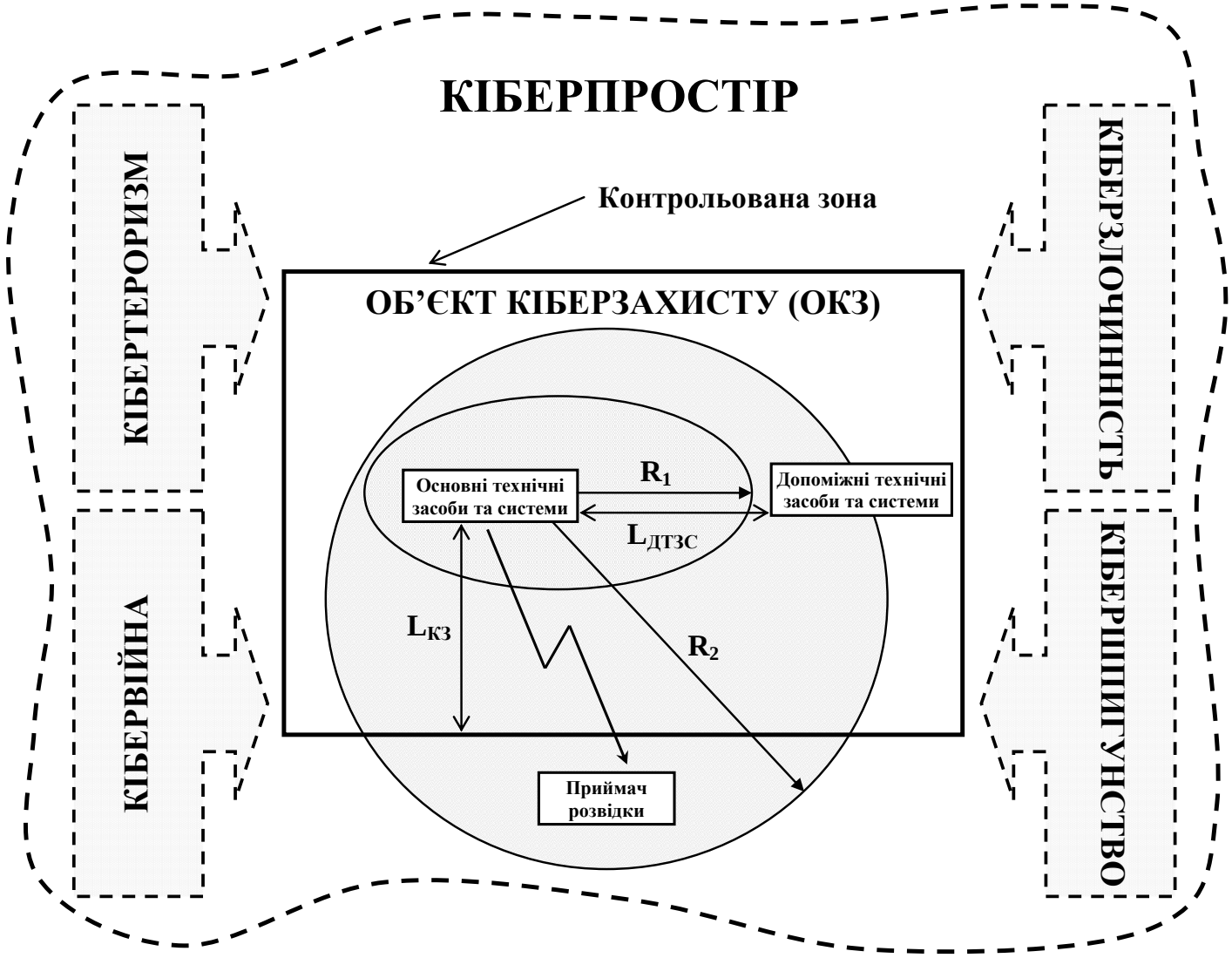

Рисунок 2.5 – Зони безпеки інформації об'єктів кіберзахисту в кіберпросторі

Контрольована зона може обмежуватися:

периметром території об'єкту кіберзахисту;

частиною території об'єкту кіберзахисту, в яких проводяться закриті заходи;

частиною будівлі об'єкту кіберзахисту (кімнати, кабінети, зали засідань, переговорні приміщення, в яких проводяться закриті заходи).

Контрольована зона при необхідності може бути більше, ніж територія, що охороняється, при цьому відповідною службою забезпечується постійний контроль частиною території, що не охороняється.

Бувають постійна і тимчасова контрольовані зони.

Постійна контрольована зона – зона, межа якої встановлюється на тривалий термін. Ця зона встановлюється в разі, якщо конфіденційні заходи всередині неї проводяться регулярно.

Тимчасова контрольована зона – зона, встановлена для проведення конфіденційних заходів разового характеру.

Кожен технічний засіб, призначений для обробки інформації, має свою граничної зоною безпеки, в якій не повинна розташовуватися антена або датчик приймача, використовуваного при відновленні даних. У цьому випадку буде забезпечена конфіденційність інформації, що обробляється даними засобом.

Однак слід ще врахувати, що безпечна зона може бути розширена з урахуванням застосування активних засобів несанкціонованого доступу до конфіденційної інформації.

Контрольована зона тісно пов'язана з небезпечними зонами R_1 і R_2.

Основні технічні засоби та системи (ОТЗС) – технічні засоби, призначені для передачі, обробки та зберігання конфіденційної інформації.

Допоміжні технічні засоби та системи (ДТЗС) – засоби та системи, які не призначені для передачі, обробки та зберігання конфіденційної інформації, на які можуть впливати електричні, магнітні та акустичні небезпечні сигнали.

"Небезпечна" зона 1 (зона R_1) – простір навколо технічного засобу обробки інформації, в межах якого на випадкових антенах наводиться небезпечний сигнал вище допустимого нормованого рівня. У зоні 1 забороняється розміщення

випадкових антен, що мають вихід по струмопровідним комунікаціям за межі контрольованої зони.

Випадкова антена – це електричний ланцюг допоміжного технічного засобу або системи, здатна приймати побічні електромагнітні випромінювання.

"Небезпечна" зона 2 (зона R_2) – простір навколо технічного засобу обробки інформації, в межах якого відношення "небезпечний сигнал / перешкода" для складових напруженості електромагнітного поля перевищує допустиме нормоване значення. Зона 2 повинна бути контрольованою, так як в ній може бути перехоплення побічних електромагнітних випромінювань за допомогою приймача розвідки та подальша розшифровка інформації.

2.2. Оцінка вразливості об’єктів кіберзахисту та оцінювання ефективності функціонування системи інформаційної безпеки

Актуальними при реалізації відповідної системи безпеки ОКЗ є наукові дослідження спрямовані на розвиток науково-технічних основ раннього виявлення загроз та попередження виникнення різного роду небезпек для ОКЗ, які свідчать про необхідність проведення оцінки вразливості ОКЗ та встановлення для цих об’єктів ризику виникнення різного роду загроз.

Для отримання порівняльної оцінки рівня небезпеки для ОКЗ в умовах прояву різної природи загроз слід використовувати наступні методи: статистичний, що базується на аналізі даних статистики виникнення загроз протягом кількох років для визначення показників небезпеки ОКЗ; імовірний, оснований на застосуванні математичних моделей, які пов’язують передумови до виникнення загроз із можливістю їх прояву; експертний, що базується на експертному оцінюванні у поєднанні з теорією нечітких множин.

Перевагою статистичного методу є об’єктивність. Імовірний та експертний методи дозволяють враховувати джерела потенційної небезпеки, які рідко проявляються у формі небезпеки, але наслідки від якої є катастрофічними для нормального функціонування ОКЗ. Однак імовірний метод є надзвичайно

громіздким і трудомістким, вимагає великого числа вихідних даних, що призводить до низької точності одержуваних результатів. За відсутністю апробованих математичних моделей і досить достовірних та формалізованих вихідних даних для них, оцінку впливу на умови нормального функціонування ОКЗ великого числа потужних небезпек доцільно проводити експертним методом.

Використаний у роботах ризико-орієнтований підхід поряд з оцінкою рівня загроз потребує визначення збитків від наслідків небезпек. Він може бути застосованим, насамперед, для наукового обґрунтування прийнятного рівня безпеки функціонування ОКЗ та прийняття рішень щодо розміщення нових ОКЗ і розширення або зміни профілю діючих.

Метою цієї роботи є розробка системи критеріїв оцінювання ефективності функціонування системи інформаційної безпеки ОКЗ шляхом проведення наукових досліджень, спрямованих на розповсюдження ризико-орієнтованого підходу для оцінки вразливості ОКЗ.

Забезпечення належного рівня безпеки функціонування ОКЗ в умовах імовірнісного прояву великої кількості загроз небезпек для інформації, що обертається у процесі функціонування ОКЗ, є перше черговою задачею ефективної системи інформаційної безпеки цього об’єкту, основу створення якої має складати класичний контур управління – рис. 2.6 [70].

Перший рівень – це пристрої реєстрації факторів загроз для інформації, що обертається у процесі функціонування ОКЗ. Вони призначені для контролю поодиноких або відразу декількох параметрів та рознесені у просторі по горизонталі й по вертикалі. При цьому, отримана засобами контролю первинна інформація про фактори загроз для інформації, що обертається у процесі функціонування ОКЗ, по кабелях або радіоканалу транслюється до пристроїв другого рівня, призначених виконувати обробку отриманої інформації та представляти її у вигляді, необхідному для третього рівня.

Обробка отриманої інформації може виконуватися як в одному місці, так і на декількох, залежно від конкретної підсистеми моніторингу системи безпеки ОКЗ та розмірів контрольованого підсистемою моніторингу зони інформаційної безпеки

ОКЗ. Оброблена інформація у відповідному вигляді потрапляє до третього рівня, де виконується аналіз отримуваної інформації та систематизація даних, на основі якої робиться висновок про стан небезпеки для інформації, що обертається у процесі функціонування ОКЗ.

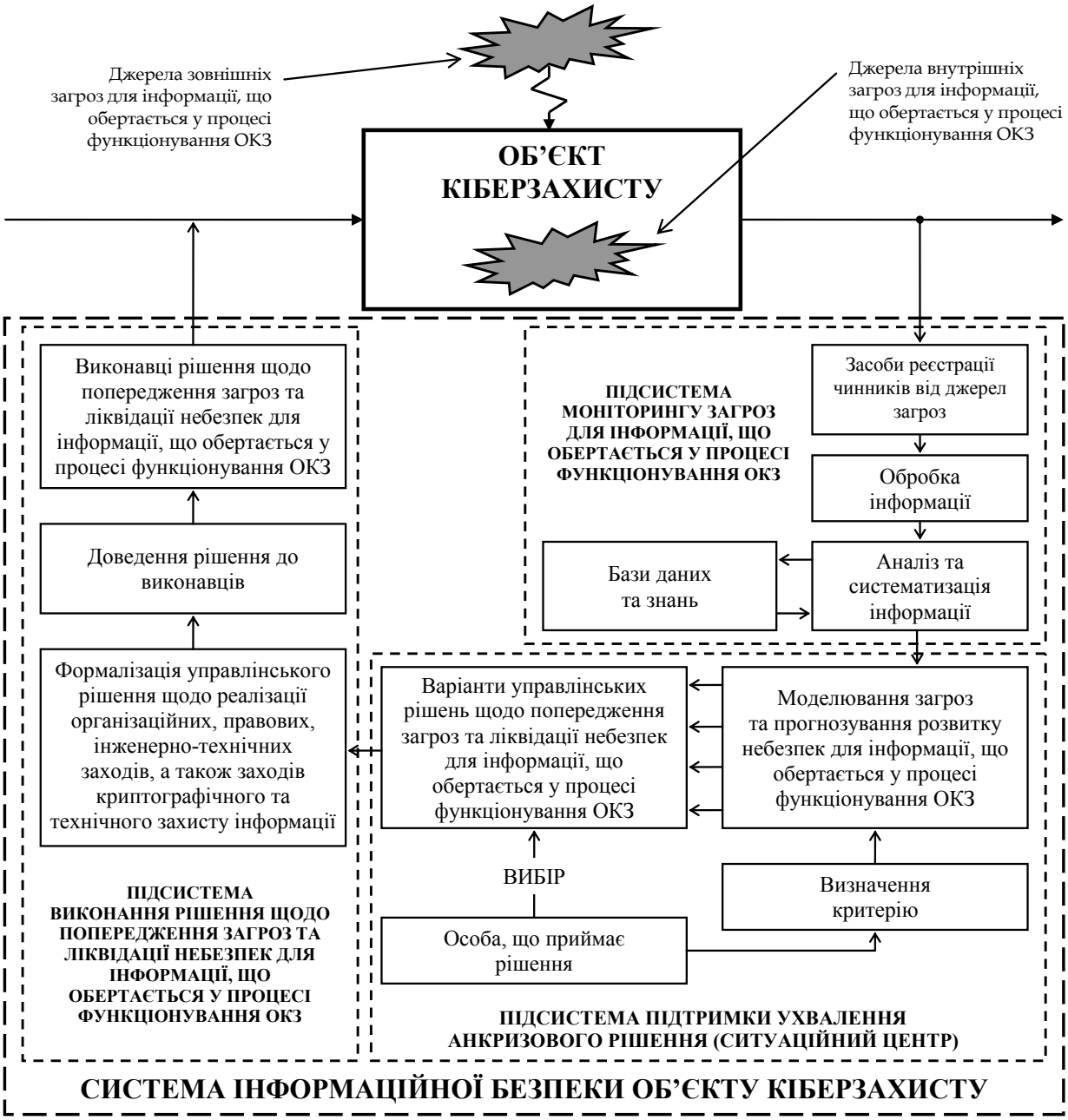

Рисунок 2.6 – Схема структури системи інформаційної безпеки об'єкту кіберзахисту як засобу управління

Використання автоматизованих засобів обробки інформації дозволяє

прискорити процеси на другому та третьому рівнях підсистеми моніторингу системи безпеки ОКЗ, а також створити електронні, доступні в реальному масштабі часу, бази даних та знань.

Розробка спеціального програмного забезпечення та навчання персоналу для цих цілей дозволяє на основі отриманої інформації виконувати моделювання загрози та здійснювати прогнозування її розвитку до рівня небезпеки для інформації, що обертається у процесі нормального функціонування ОКЗ, при цьому графічно (у тому числі у вигляді електронних карт) відображати прогнозовану динаміку небезпечних для ОКЗ подій.

Інша інформаційна система, яка, як показано на рис. 1, є системою підтримки ухвалення антикризового рішення. Тут особа, що приймає рішення, визначає один або декілька критеріїв, відповідно до яких здійснюється прогностичне моделювання розвитку небезпек для інформації, що оберталась у процесі функціонування ОКЗ, та виробляються варіанти управлінських рішень, які обґрунтовані відповідними розрахунками.

Отримавши набір варіантів управлінських антикризових рішень, особа, що приймає рішення, обирає один з них або задає ще додаткові критерії, відповідно до яких виконується моделювання та розробка управлінських рішень, направлених на недопущення розвитку небезпеки до рівня інформаційної катастрофи для ОКЗ, або, якщо катастрофи вже не уникнути, то виконується розробка управлінських рішень, спрямованих на мінімізацію наслідків від неї.

Затверджене вказаною вище особою антикризове рішення потрапляє до системи виконання рішення, де виконується його формалізація та доведення до виконавців, які, у свою чергу, впливають на джерела інформаційної небезпеки, які виникли на ОКЗ. Зміни стану ОКЗ та зміни стану інформаційної небезпеки на ньому викликатимуть зміни у величинах вимірюваних параметрів, що фіксуються пристроями контролю. Надалі ці зміни будуть відпрацьовані, а подальше моделювання покаже ефективність виконання управлінського антикризового рішення – контур управління рівнем інформаційної безпеки функціонування ОКЗ замкнувся.

З метою оцінки ефективності функціонування системи інформаційної безпеки об’єкту кіберзахисту та базуючись на основних постулатах ризико-орієнтованого підходу, показник ризику для інформації, що обертається у процесі функціонування ОКЗ, можливо представити як [71–78]:

$$R_{ОКЗ}^{Інформац\ \cdot} = \sum_{i=1}^{3} R_{ОКЗ_i}^{Інформац\ \cdot}, \tag{2.1}$$

де $R_{ОКЗ_1}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується розголошенням інформації; $R_{ОКЗ_2}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації; $R_{ОКЗ_3}^{Інформац\ \cdot}$ – показник ризику для комп’ютерної інформації, що обертається у процесі функціонування.

Під розголошенням інформації мається на увазі навмисні або випадкові дії співробітників, що призвели до ознайомлення з конфіденційною інформацією осіб, які не мають до неї доступу. Цей вид інформаційної небезпеки реалізується через передачу, надання та пересилання повідомлень каналами їх поширення.

Під витоком інформації мається на увазі безконтрольне виведення конфіденційної інформації за межі організації або кола осіб, яким її було довірено.

Показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації, включає наступні складові:

$$R_{ОКЗ_2}^{Інформац\ \cdot} = \sum_{m=1}^{4} R_{ОКЗ_{2.m}}^{Інформац\ \cdot}, \tag{2.2}$$

де $R_{ОКЗ_{2.1}}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по технічним каналам; $R_{ОКЗ_{2.2}}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі

функціонування ОКЗ, який характеризується витоком інформації по каналам зв'язку; $R_{ОКЗ\ 2.3}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком мовної інформації; $R_{ОКЗ\ 2.4}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації, що відображається.

Показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по технічним каналам, включає наступні складові:

$$R_{ОКЗ\ 2.1}^{Інформац\ \cdot} = \sum_{n=1}^{4} R_{ОКЗ\ 2.1.n}^{Інформац\ \cdot}, \qquad (2.3)$$

де $R_{ОКЗ\ 2.1.1}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електромагнітному каналу; $R_{ОКЗ\ 2.1.2}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу; $R_{ОКЗ\ 2.1.3}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по параметричному каналу (перехоплення інформації шляхом «високочастотного опромінення» технічних засобів прийому, обробки та зберігання інформації); $R_{ОКЗ\ 2.1.4}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по вібраційному каналу (аналіз відповідності між символом, що друкується, і його акустичним образом).

Показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електромагнітному каналу, включає наступні складові:

$$R_{ОКЗ\ 2.1.1}^{Інформац\ \cdot} = \sum_{p=1}^{3} R_{ОКЗ\ 2.1.1.p}^{Інформац\ \cdot}, \quad (2.4)$$

де $R_{ОКЗ\ 2.1.1.1}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електромагнітному каналу за рахунок електромагнітного випромінювання елементів технічних засобів прийому, обробки та зберігання інформації; $R_{ОКЗ\ 2.1.1.2}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електромагнітному каналу за рахунок електромагнітні випромінювання на частотах роботи високочастотних генераторів засобів прийому, обробки та зберігання інформації; $R_{ОКЗ\ 2.1.1.3}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електромагнітному каналу за рахунок випромінювання на частотах самозбудження підсилювачів низької частоти.

Показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу, включає наступні складові:

$$R_{ОКЗ\ 2.1.2}^{Інформац\ \cdot} = \sum_{w=1}^{4} R_{ОКЗ\ 2.1.2.w}^{Інформац\ \cdot}, \quad (2.5)$$

де $R_{ОКЗ\ 2.1.2.1}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу за рахунок наведення електромагнітних випромінювань елементів технічних засобів прийому, обробки та зберігання інформації на сторонні провідники; $R_{ОКЗ\ 2.1.2.2}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу за рахунок просочування інформаційних сигналів в лінії електроживлення;

$R_{ОКЗ\ 2.1.2.3}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу за рахунок просочування інформаційних сигналів у коло заземлення; $R_{ОКЗ\ 2.1.2.4}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу за рахунок знімання інформації з використанням закладних пристроїв.

Показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по каналам зв’язку, включає наступні складові:

$$R_{ОКЗ\ 2.2}^{Інформац\ \cdot} = \sum_{q=1}^{4} R_{ОКЗ\ 2.2.q}^{Інформац\ \cdot}, \qquad (2.6)$$

де $R_{ОКЗ\ 2.2.1}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електромагнітному каналу зв’язку, а саме електромагнітні випромінювання передавачів зв'язку, модульовані інформаційним сигналом (прослуховування радіотелефонів, стільникових телефонів, радіорелейних ліній зв'язку); $R_{ОКЗ\ 2.2.2}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу зв’язку, а саме підключення до ліній зв'язку; $R_{ОКЗ\ 2.2.3}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по індукційному каналу зв’язку, а саме ефект виникнення навколо високочастотного кабелю електромагнітного поля при проходженні інформаційних сигналів; $R_{ОКЗ\ 2.2.4}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації по паразитному каналу зв’язку, а саме паразитні ємнісні, індуктивні і резистивні зв'язку і наведення

близько розташованих один від одного ліній передачі інформації.

Показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком мовної інформації, включає наступні складові:

$$R_{ОКЗ\ 2.3}^{Інформац\ \cdot} = \sum_{d=1}^{5} R_{ОКЗ\ 2.3.d}^{Інформац\ \cdot}, \qquad (2.7)$$

де $R_{ОКЗ\ 2.3.1}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком мовної інформації по акустичному каналу, де середовищем поширення є повітря; $R_{ОКЗ\ 2.3.2}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком мовної інформації по віброакустичному каналу, де середовищем поширення є огороджувальні будівельні конструкції; $R_{ОКЗ\ 2.3.3}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком мовної інформації по параметричному каналу (результат впливу акустичного поля на елементи схем, що призводить до модуляції високочастотного сигналу інформаційним); $R_{ОКЗ\ 2.3.4}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком мовної інформації по акустоелектричному каналу (перетворення акустичних сигналів в електричні); $R_{ОКЗ\ 2.3.5}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком мовної інформації по оптико-електронному (лазерному) каналу (опромінення лазерним променем вібруючих поверхонь).

Показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації, що відображається, включає наступні складові:

$$R_{ОКЗ\ 2.4}^{Інформац\ \cdot} = \sum_{f=1}^{3} R_{ОКЗ\ 2.4.f}^{Інформац\ \cdot}, \quad (2.8)$$

де $R_{ОКЗ\ 2.4.1}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації, що відображається шляхом спостереження за об'єктами (для спостереження днем застосовуються оптичні прилади і телевізійні камери; для спостереження вночі – прилади нічного бачення, тепловізори, телевізійні камери); $R_{ОКЗ\ 2.4.2}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації, що відображається шляхом зйомки об'єктів (для зйомки об'єктів використовуються телевізійні і фотографічні засоби; для зйомки об'єктів в день з близької відстані застосовуються портативні камуфльовані фотоапарати і телекамери, суміщені з пристроями відеозапису); $R_{ОКЗ\ 2.4.3}^{Інформац\ \cdot}$ – показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації, що відображається шляхом зйомки документів (зйомка документів здійснюється з використанням портативних фотоапаратів).

Показник ризику для комп’ютерної інформації, що обертається у процесі функціонування ОКЗ, включає наступні складові:

$$R_{ОКЗ\ 3}^{Інформац\ \cdot} = \sum_{k=1}^{3} R_{ОКЗ\ 3.k}^{Інформац\ \cdot}, \quad (2.9)$$

де $R_{ОКЗ\ 3.1}^{Інформац\ \cdot}$ – показник ризику для комп’ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується втратою інформації; $R_{ОКЗ\ 3.2}^{Інформац\ \cdot}$ – показник ризику для комп’ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується зміною інформації; $R_{ОКЗ\ 3.3}^{Інформац\ \cdot}$ –

показник ризику для комп’ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації.

Найбільш небезпечним з позицій інформаційної безпеки в даний час вважається несанкціонований доступ до комп’ютерної інформації. Показник ризику для комп’ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації, включає наступні складові:

$$R_{ОКЗ\ 3.3}^{Інформац\ \cdot} = \sum_{g=1}^{9} R_{ОКЗ\ 3.3.g}^{Інформац\ \cdot}, \qquad (2.10)$$

де $R_{ОКЗ\ 3.3.1}^{Інформац\ \cdot}$ – показник ризику для комп’ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом перегляду інформації (на екранах комп'ютерів, на друкуючих пристроях тощо); $R_{ОКЗ\ 3.3.2}^{Інформац\ \cdot}$ – показник ризику для комп’ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом копіювання програм і даних (копіювання з інформаційних носіїв і жорстких дисків при слабкому захисті комп'ютерів, при поганій організації зберігання копій і архівів, при читанні даних по лініям зв'язку в мережах, при отриманні інформації за рахунок встановлення спеціальних закладок тощо); $R_{ОКЗ\ 3.3.3}^{Інформац\ \cdot}$ – показник ризику для комп’ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом зміни потоку повідомлень (в тому числі застосування закладок, що змінюють передану інформацію, при тому, що на екрані вона залишається без змін); $R_{ОКЗ\ 3.3.4}^{Інформац\ \cdot}$ – показник ризику для комп’ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом зміни конфігурації комп'ютерних засобів (зміна

прокладки кабелів, зміна комплектації комп'ютерів і периферійних пристроїв під час технічного обслуговування, завантаження сторонньої операційної системи для доступу до інформації, встановлення додаткового порту для зовнішнього пристрою тощо); $R^{Інформац}_{ОКЗ\ 3.3.5}$ – показник ризику для комп'ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом зміни розташування комп'ютерних засобів та/або режиму обслуговування та умов експлуатації. Це – установка додаткових пристроїв поблизу комп'ютерів (систем пожежної та охоронної сигналізації, телефонних мереж, систем електроживлення тощо), зміни розташування комп'ютерів для поліпшення доступу до інформації (візуального спостереження); $R^{Інформац}_{ОКЗ\ 3.3.6}$ – показник ризику для комп'ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом несанкціонованої модифікації контрольних процедур (наприклад, при перевірці аутентичності електронного підпису, якщо він виконується програмними засобами); $R^{Інформац}_{ОКЗ\ 3.3.7}$ – показник ризику для комп'ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом підробки та/або додавання об'єктів, які не є легальними, але володіють основними властивостями легальних об'єктів (наприклад, додавання підроблених записів в файл). Особливо це небезпечно при використанні систем автоматизованого обліку різних об'єктів; $R^{Інформац}_{ОКЗ\ 3.3.8}$ – показник ризику для комп'ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом додавання фальшивих процесів та/або підміна справжніх процесів обробки даних фальшивими. Це відноситься як до роботи операційних систем, так і особливо до роботи пакетів прикладних програм; $R^{Інформац}_{ОКЗ\ 3.3.9}$ – показник ризику для комп'ютерної інформації, що обертається у процесі функціонування ОКЗ, який характеризується отриманням

несанкціонованого доступу до інформації шляхом фізичного руйнування апаратних засобів або переривання функціонування комп'ютерних засобів різними способами з метою часткового або повного знищення інформації, що зберігається.

При цьому складові ризику для інформації, що обертається у процесі функціонування ОКЗ, обчислюють за формулою:

$$R_{ОКЗ\ i.j}^{Інформац\ \cdot} = P_{ОКЗ\ i.j}^{Інформац\ \cdot} \cdot U_{ОКЗ\ i.j}^{Інформац\ \cdot}, \qquad (2.11)$$

де $P_{ОКЗ\ i.j}^{Інформац\ \cdot}$ – оцінка ймовірності перевищення нормативного показника для j-го аспекту і-го процесу небезпеки для інформації, що обертається у процесі функціонування ОКЗ; $U_{ОКЗ\ i.j}^{Інформац\ \cdot}$ – оцінка збитку від перевищення нормативного показника впливи j-го аспекту і-го процесу небезпеки для інформації, що обертається у процесі функціонування ОКЗ.

При одночасному впливі на інформацію, що обертається у процесі функціонування ОКЗ, декількох процесів небезпеки, необхідно враховувати можливість прояву синергетичного ефекту [79, 80]. У цьому випадку імовірність перевищення нормативного показника для двох спільних аспектів небезпеки для інформації, що обертається у процесі функціонування ОКЗ, можна розрахувати як:

$$P_{ОКЗ\ i.j}^{Інформац\ \cdot} = P_{ОКЗ\ i.1}^{Інформац\ \cdot} + P_{ОКЗ\ i.2}^{Інформац\ \cdot} - P_{ОКЗ\ i.1}^{Інформац\ \cdot} \cdot P_{ОКЗ\ i.2}^{Інформац\ \cdot}. \qquad (2.12)$$

Оцінку збитку від перевищення нормативного показника обчислюють як суму збитку вид складових небезпеки для інформації, що обертається у процесі функціонування ОКЗ. Загальний очікуваний збиток $U_{ОКЗ}^{Інформац\ \cdot}$ визначають за формулою:

$$U_{ОКЗ}^{Інформац\ \cdot} = \sum_{i,j} U_{ОКЗ\ i.j}^{Інформац\ \cdot}, \qquad (2.13)$$

де $U_{ОКЗ}^{Інформац\ \cdot}$ – математичне очікування загального економічного збитку ОКЗ від процесів небезпеки для інформації, що обертається у процесі функціонування ОКЗ; $U_{ОКЗ\ i.j}^{Інформац\ \cdot}$ – математичне очікування збитку ОКЗ за ризиком j-го аспекту і-го процесу небезпеки для інформації, що обертається у процесі функціонування ОКЗ.

Виходячи з представленого у вигляді виразів (2.1)–(2.13) матеріалу щодо розповсюдження ризико-орієнтованого підходу для оцінки вразливості ОКЗ та базуючись на основних постулатах теорії систем та синергетики, рівень захищеності ОКЗ в умовах імовірнісного прояву різного роду аспектів процесу інформаційної небезпеки, а також економічної ефективності функціонування системи інформаційної безпеки об’єкту кіберзахисту – $F_{СІБОКЗ}$, можливо представити у вигляді даних рис. 2.7 та записати у вигляді рівняння:

$$Z_{ОКЗ}^{Інформац\ \cdot} = \varphi\left(U_{ОКЗ}^{Інформац\ \cdot}, F_{СІБОКЗ}\right). \qquad (2.14)$$

Вираз (2.14) представлено у вигляді загального функціоналу, вирішення якого можливо при проведенні аудиту щодо стану захищеності в умовах імовірнісного прояву різного роду аспектів процесу інформаційної небезпеки конкретного об’єкту кіберзахисту.

Процес антикризового управління в умовах ризику або загроз для інформації, що обертається у процесі функціонування ОКЗ, ситуаційним центром (який, згідно даних рис. 2.6, є складовою системи інформаційної безпеки ОКЗ) реалізується згідно представленому на рис. 2.8 алгоритму.

Так, діагностика (на базі наведеного у вигляді виразів (2.1)–(2.13) ризико-орієнтованого підходу) кризового стану й загрози для інформації, що обертається у процесі функціонування ОКЗ, може здійснюватися безпосередньо співробітниками служби безпеки ОКЗ чи зовнішніми незалежними експертами. Результати діагностики допомагають установити ступінь небезпеки для інформації та для повсякденного функціонування ОКЗ, а отже — визначити цілі й завдання

антикризового управління щодо запобігання виникнення загроз для інформації, що обертається у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків. Залежно від ступеню небезпеки такими завданнями можуть бути: виведення ОКЗ зі стану існування загроз для інформації; недопущення виникнення небезпеки для інформації; локалізація існуючих загроз для інформації, стабілізація процесу функціонування ОКЗ, запобігання повторенню кризи.

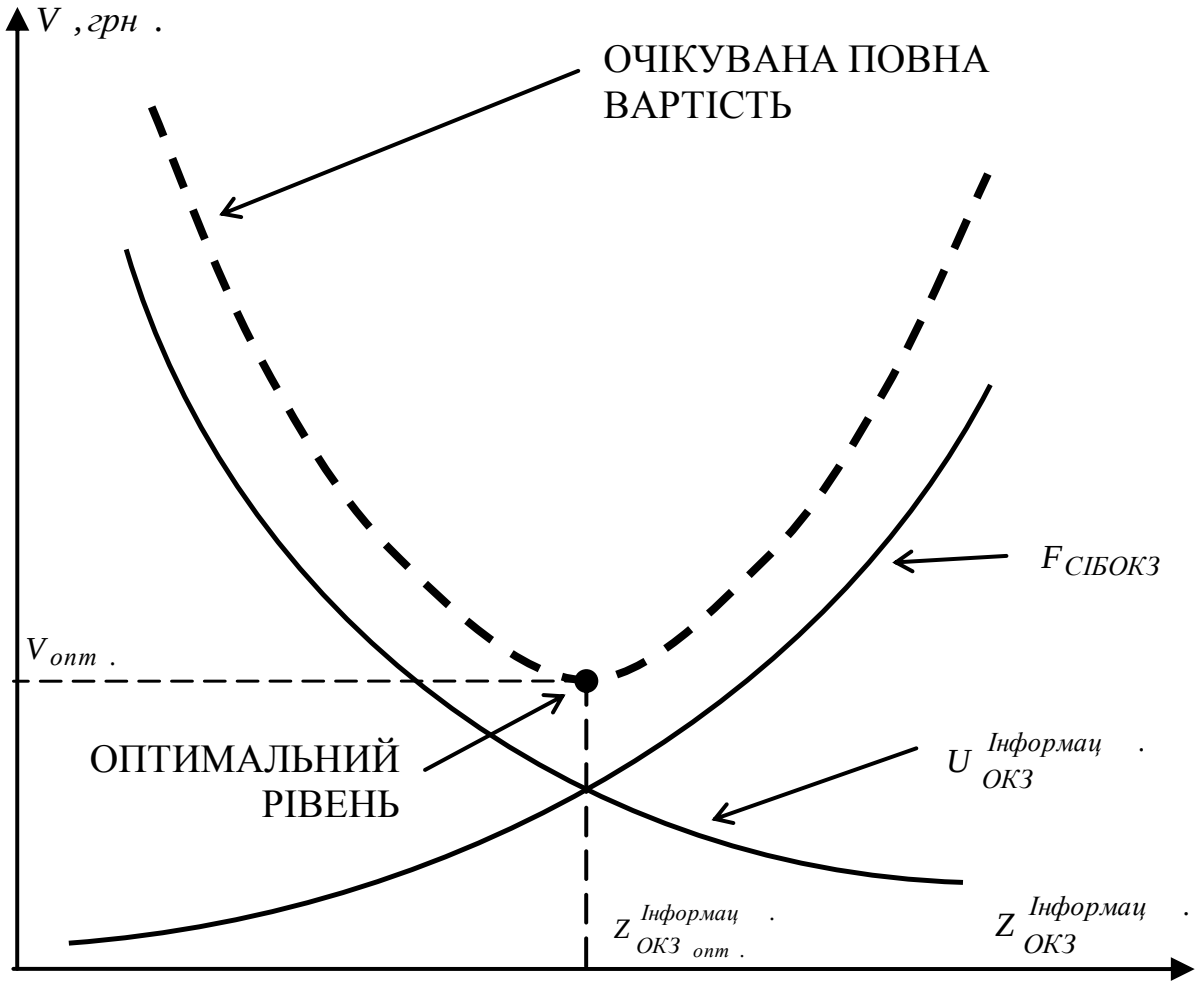

Рисунок 2.7 – Співвідношення між рівнем захищеності ($z_{\text{ОКЗ}}^{\text{Інформац}}$) та вартістю (v) захисту об’єкту кіберзахисту

На етапі визначення суб’єкта антикризової діяльності щодо запобігання виникнення загроз для інформації, що обертається у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків необхідно встановити суб’єкт, який бере

на себе відповідальність за розроблення й реалізацію антикризових процедур, та його повноваження.

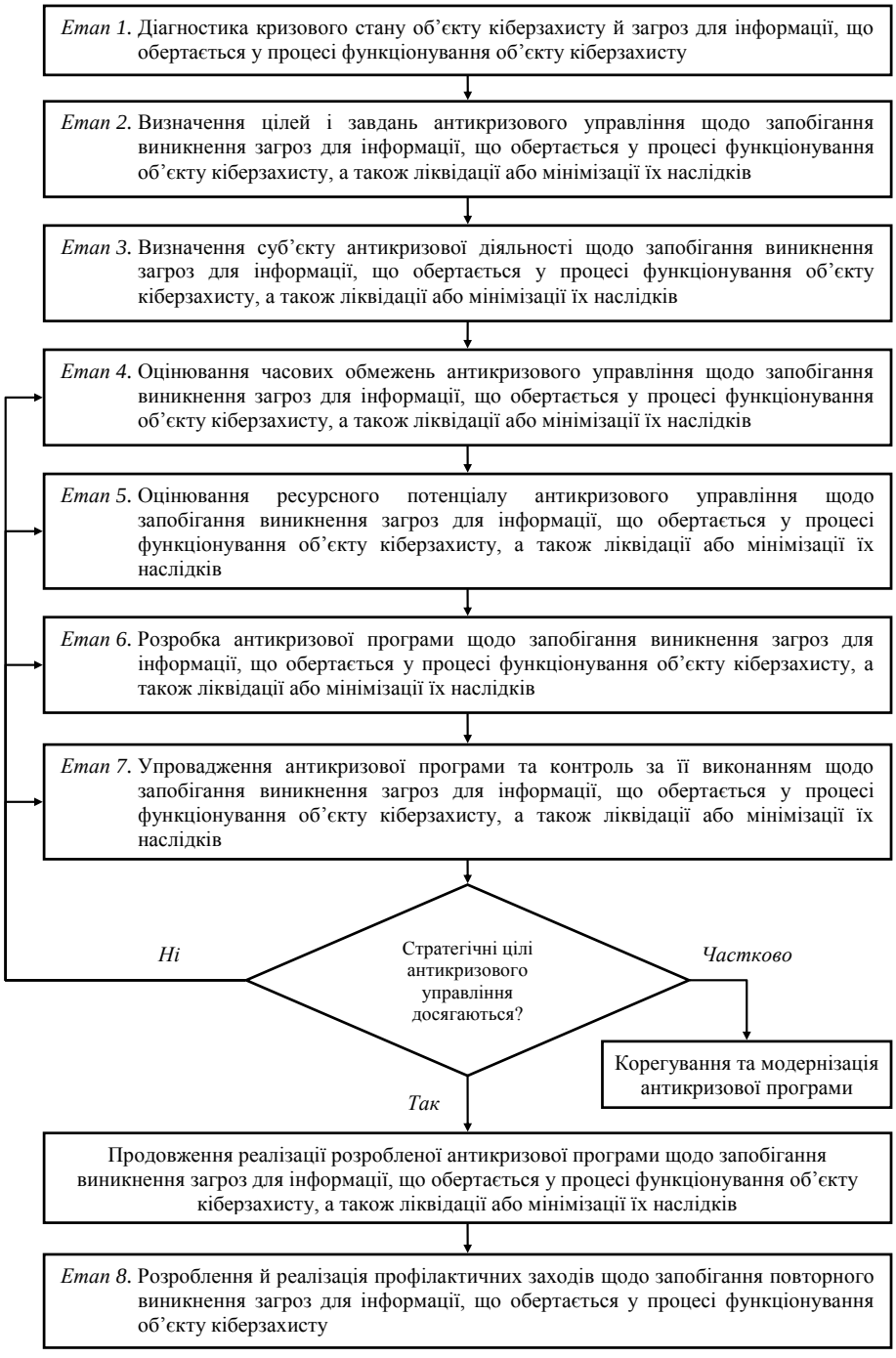

Рисунок 2.8 – Структурно-логічна схема процесу антикризового управління щодо запобігання виникнення загроз для інформації, що обертається у процесі функціонування об'єкту кіберзахисту, а також ліквідації або мінімізації їх наслідків

На етапі оцінювання часових обмежень процесу антикризового управління щодо запобігання виникнення загроз для інформації, що обертається у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків визначається час, наявний у ОКЗ для вжиття запобіжних заходів. Часові обмеження залежать від інтенсивності поширення загроз для інформації. Розуміння цього сприяє недопущенню подальшого поглиблення кризи, оскільки подолання глибшої кризи пов’язане з більшими витратами й труднощами.

У разі реальної загрози для інформації, що обертається у процесі функціонування ОКЗ, стає жорстким обмеженням, набуває центрального значення. Це робить необхідним прогнозування розмірів соціальних, матеріальних та екологічних збитків у наслідок розголошенням та витоку інформації, а також виникнення небезпек для комп’ютерної інформації.

Наступним етапом є оцінювання (на базі наведеного на рис. 2 підходу) ресурсного потенціалу антикризового управління щодо запобігання виникнення загроз для інформації, що обертається у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків. Фахівці в галузі безпеки розглядають ОКЗ як систему ресурсів, що взаємодіють між собою та забезпечують досягнення певних результатів щодо досягнення необхідного рівня інформаційної безпеки. Основними видами ресурсів є технічні, технологічні, кадрові, просторові, ресурси організаційної структури системи управління, інформаційні, фінансові тощо.

Розроблення антикризової програми ОКЗ становить обґрунтовану сукупність заходів, що мають бути вжиті для досягнення визначених цілей та виконання завдань антикризового управління щодо запобігання виникнення загроз для інформації, що обертається у процесі функціонування об’єкту кіберзахисту, а також ліквідації або мінімізації їх наслідків. Зміст програми обумовлюється результатами проведеної діагностики, часовими й ресурсними обмеженнями антикризового процесу. У її складі зазвичай виділяють окремі антикризові політики – сукупність дій, засобів та інструментів досягнення певних результатів.

Після розроблення антикризової програми настає етап безпосереднього впровадження антикризової програми щодо реалізації організаційних, правових,

інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, а також контролю за її виконанням. Найважливішою управлінською функцією на цьому етапі є організація контролю за виконанням антикризової програми для своєчасної модернізації або корегування розробленої політики (процедур, заходів) у зв'язку з не прогнозованими збуреннями у внутрішньому й зовнішньому середовищах функціонування ОКЗ.

Система інформаційної безпеки ОКЗ має забезпечувати: по-перше, відстеження динаміки зовнішніх проявів джерел загроз для інформації, факторів розвитку небезпеки для інформації, інтегральних показників кризового стану; по-друге, оцінювання результатів вжитих антикризових заходів за їх характером, термінами, наслідками реалізації.

Відповідно до ступеня досягнення поставлених цілей щодо забезпечення відповідного рівня інформаційної безпеки ОКЗ можливі такі управлінські дії: 1) продовження реалізації розробленої антикризової програми при досягненні поставлених цілей і завдань, необхідної результативності вжитих заходів; 2) модернізація й корегування антикризової програми в разі недотримання її окремих параметрів (терміни реалізації, досягнутий ефект, необхідні ресурси тощо) або появи несподіваних збурень у зовнішньому середовищі ОКЗ; 3) кардинальний перегляд розробленої програми та внесення відповідних коректив.

Метою етапу розроблення й реалізації профілактичних заходів щодо запобігання повторного виникнення загроз для інформації, що обертається у процесі функціонування ОКЗ, є створення або модернізація основних елементів системи інформаційної безпеки ОКЗ. Для цього мають бути внесені відповідні зміни в основні функціональні стратегії та політики безпеки ОКЗ, які повинні враховувати передові технології, інструменти й засоби управління інформаційною безпекою, забезпечувати відповідний рівень безпеки функціонування ОКЗ.

Висновки до розділу 2

1. Основу системи безпеки в умовах виникнення кіберзагроз становить класичний контур управління, який забезпечує: 1) збір, обробку та аналіз інформації; 2) моделювання розвитку обстановки на об’єкті кіберзахисту та розвитку рівня кіберзагроз на території міста, регіону, держави; 3) розробку та ухвалення управлінських рішень щодо запобігання та ліквідації небезпечних дій в умовах кібервійни, кібертероризму, кіберзлочинності та кібершпигунства, а також мінімізації їх наслідків; 4) виконання рішень щодо запобігання та ліквідації небезпечних дій в умовах кібервійни, кібертероризму, кіберзлочинності та кібершпигунства, а також мінімізації їх наслідків.

2. Створення ефективної інформаційно-аналітичної системи управління процесами попередження й локалізації наслідків небезпечних дій в умовах кібервійни, кібертероризму, кіберзлочинності та кібершпигунства відбувається шляхом комплексного включення в діючу систему безпеки держави по вертикалі від об’єктового до державного рівнів різних функціональних елементів територіальної системи моніторингу НС та складових системи ситуаційних центрів, які жорстко пов’язані між собою на інформаційному та виконавчому рівнях для прийняття відповідних антикризових рішень, для розв’язання різних функціональних задач моніторингу, попередження та ліквідації небезпечних дій.

3. Базуючись на уявленнях про класичний контур управління, в магістерській роботі представлені результати розповсюдження ризико-орієнтованого підходу для оцінки ефективності функціонування системи інформаційної безпеки ОКЗ в умовах розголошення та витоку інформації, а також в умовах виникнення загроз для комп’ютерної інформації. На базі отриманих результатів в роботі розроблено структурно-логічну схему процесу антикризового управління щодо запобігання виникнення загроз для інформації, що обертається у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків.

РОЗДІЛ 3
РОЗРОБКА КОМПЛЕКСУ ОПЕРАТИВНОГО МОНІТОРИНГУ (КОНТРОЛЮ) АКУСТИЧНОГО ПРОСТОРУ НА ОБ'ЄКТАХ КІБЕРЗАХИСТУ

3.1. Розробка пристрою контролю акустичного простору зони терористичних дій навколо об'єктів кіберзахисту

3.1.1. Дослідження амплітудно-частотних спектрів акустичної емісії процесу горіння целлюлозовмісних матеріалів як одних з основних матеріалів, які використовуються для реалізації підпалів та нападів при організації терористичних дій у зоні навколо об'єктів кіберзахисту

Однією із форм впливу терористів на умови нормального функціонування локальної території, як зони навколо об'єктів кіберзахисту, є підпали (див. рис. 3.1), невід'ємною складовою яких є хімічна реакція горіння, яка супроводжується виділенням значної кількості теплоти, диму і газів, а також випромінюванням світла. Процес горіння являє собою швидкий окислювально-відновний процес, при якому горюча речовина з'єднується з окислювачем і виділяється енергія та продукти розкладання [81–91].

Загальним принципом роботи всіх пристроїв виявлення спалаху є своєчасна реєстрація фактора небезпеки і оцінка його фізичної величини.

За результатами проведеного порівняльного аналізу [92–101] різних типів детекторів пожежних сповіщувачів необхідно констатувати наступне.

По-перше, відповідно до встановлених областей функціонування технічно реалізованих, різних типів пожежних сповіщувачів в залежності від часу прояви на кібероб'єкті пріоритетних факторів небезпеки (див. рис. 3.2), як комплексного параметра ефективності функціонування системи раннього виявлення джерел загорянь, можливо виділити два кластера.

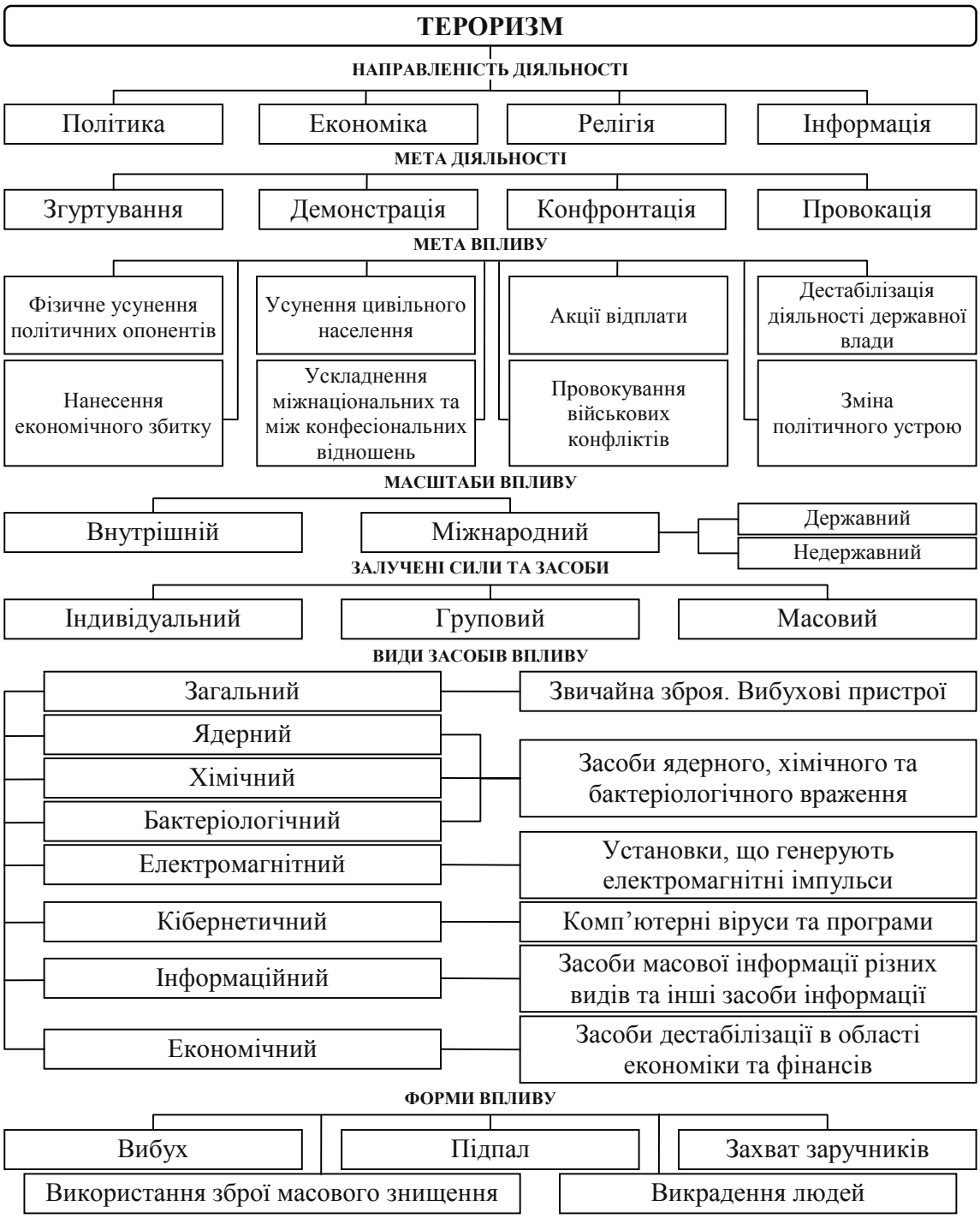

Рисунок 3.1 – Схема класифікації тероризму за видами небезпек

У перший кластер входять пожежні сповіщувачі, призначені для виявлення джерел загорянь, на так званому, етапі можливої появи пожежної небезпеки. Функціонування цих пожежних сповіщувачів засноване на принципах виявлення газоподібних продуктів горіння ($F_{ГПГ}$) і диму ($F_{Д}$).

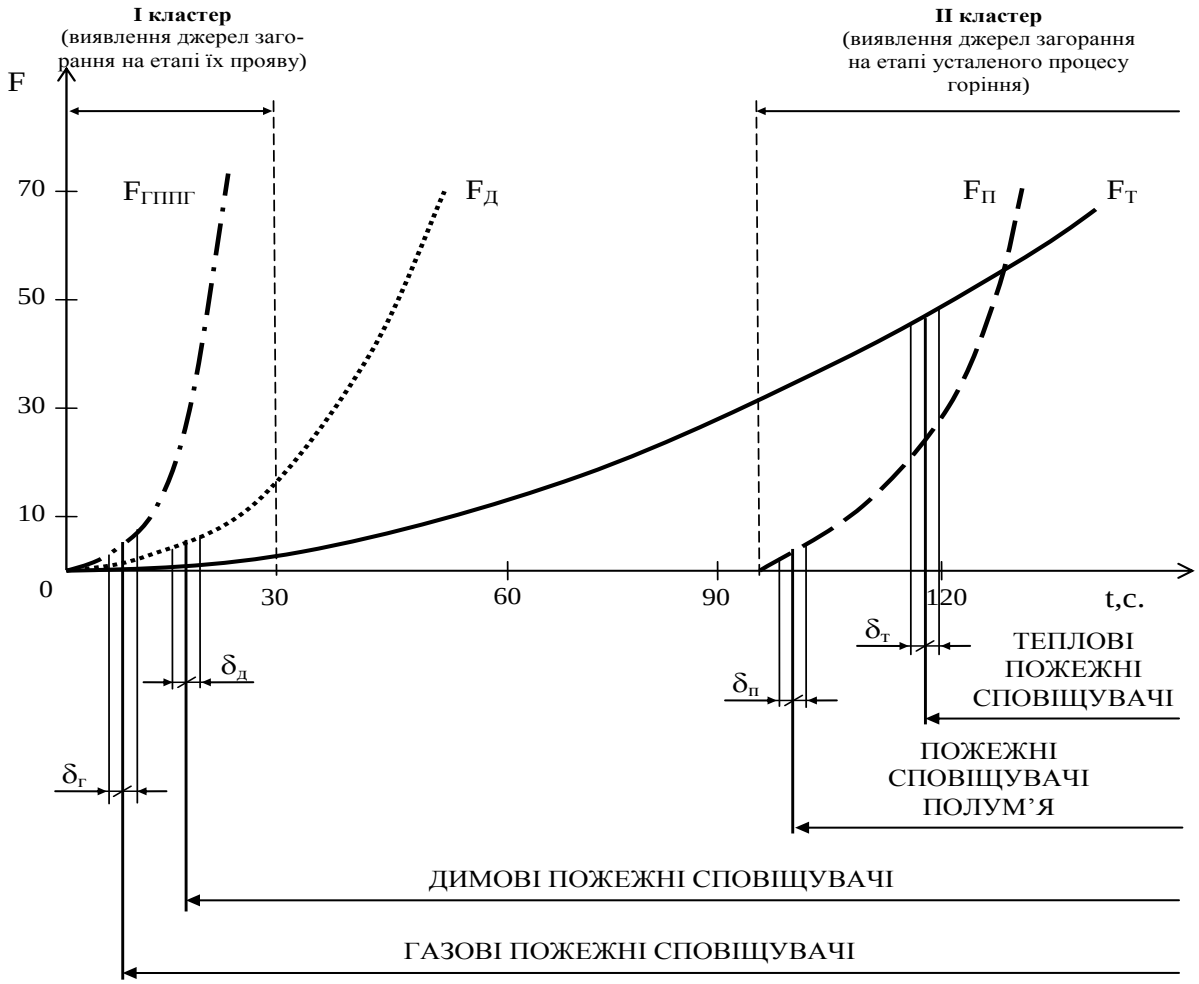

Рисунок 3.2 – Графічне представлення областей функціонування технічно реалізованих, різних типів пожежних сповіщувачів в залежності від часу (t) появу на об'єкті кіберзахисту пріоритетних факторів небезпеки (F) і розмірів зон виявлення (δ) пріоритетних факторів небезпеки (δг – газовий аналіз середовища, δд – виявлення диму, δп – аналіз полум'я, δт – контроль температури середовища), в залежності від тактико-технічних характеристик чутливих елементів засобів виявлення

Розміри і розташування на осі часу графічної залежності рис. 3.2 зон виявлення δг і δд факторів $F_{ГПІГ}$ і $F_Д$ визначаються тактико-технічними характеристиками існуючих газових і димових пожежних сповіщувачів. Зміна параметрів цих зон в сторону підвищення ефективності раннього виявлення джерел загорянь обмежена метрологічними можливостями фізико-хімічних методів аналізу

середовища загоряння, закладених в роботу чутливих елементів розглянутих пожежних сповіщувачів.

У другій кластер входять пожежні сповіщувачі для виявлення джерел загорянь на, так званому, етапі сталого (стаціонарного) процесу горіння. Функціонування цих пожежних сповіщувачів засноване на принципах аналізу (контролю) зростаючої температури ($F_Т$) і факелу горіння ($F_П$).

Розміри і розташування на осі часу графічної залежності рис. 3.3 зон виявлення δт і δп факторів $F_Т$ і $F_П$ визначаються тактико-технічними характеристиками існуючих теплових пожежних сповіщувачів та пожежних сповіщувачів полум'я. Зміна параметрів цих зон для підвищення ефективності раннього виявлення джерел загорянь також обмежена характеристиками фізико-хімічних принципів аналізу середовища загоряння, закладених в роботу чутливих елементів розглянутих пожежних сповіщувачів.

По-друге, сучасний етап розвитку проектування та будівництва об'єкті кіберзахисту спрямований на збільшення зони контролю цих об'єктів у кіберпросторі. У зв'язку з цим, виникають додаткові вимоги до тактико-технічними характеристиками пожежних сповіщувачів при реалізації режиму раннього виявлення джерел загоряння, обумовлених обмеженням швидкості поширення в контрольованій зоні до датчиків системи контролю газоподібних продуктів піролізу і частинок диму в процесі зародження пожежонебезпечної обстановки.

Зазначені обставини свідчать про необхідність технічної реалізації нових фізико-технічних методів аналізу властивостей середовища загоряння, спрямованих на практично миттєвий однозначний контроль хвильових факторів пожежної небезпеки на етапі зародження і прояву джерел загорянь, що і визначило мету наших досліджень.

Загальними закономірностями пожеж, відповідно до даних рис. 3.3, є: 1) горіння з виділенням тепла і продуктів повного та неповного згоряння; 2) массообмен, що виникає внаслідок утворення на пожежі конвекційних газових потоків, які забезпечують надходження свіжого повітря в зону горіння та відведення продуктів горіння з неї; 3) тепло, що виділяється в зоні горіння, передається в

навколишнє середовище і частково витрачається на нагрів горючих речовин, будівельних конструкцій тощо і таким чином робить можливим самостійне розповсюдження процесу горіння [102–109].

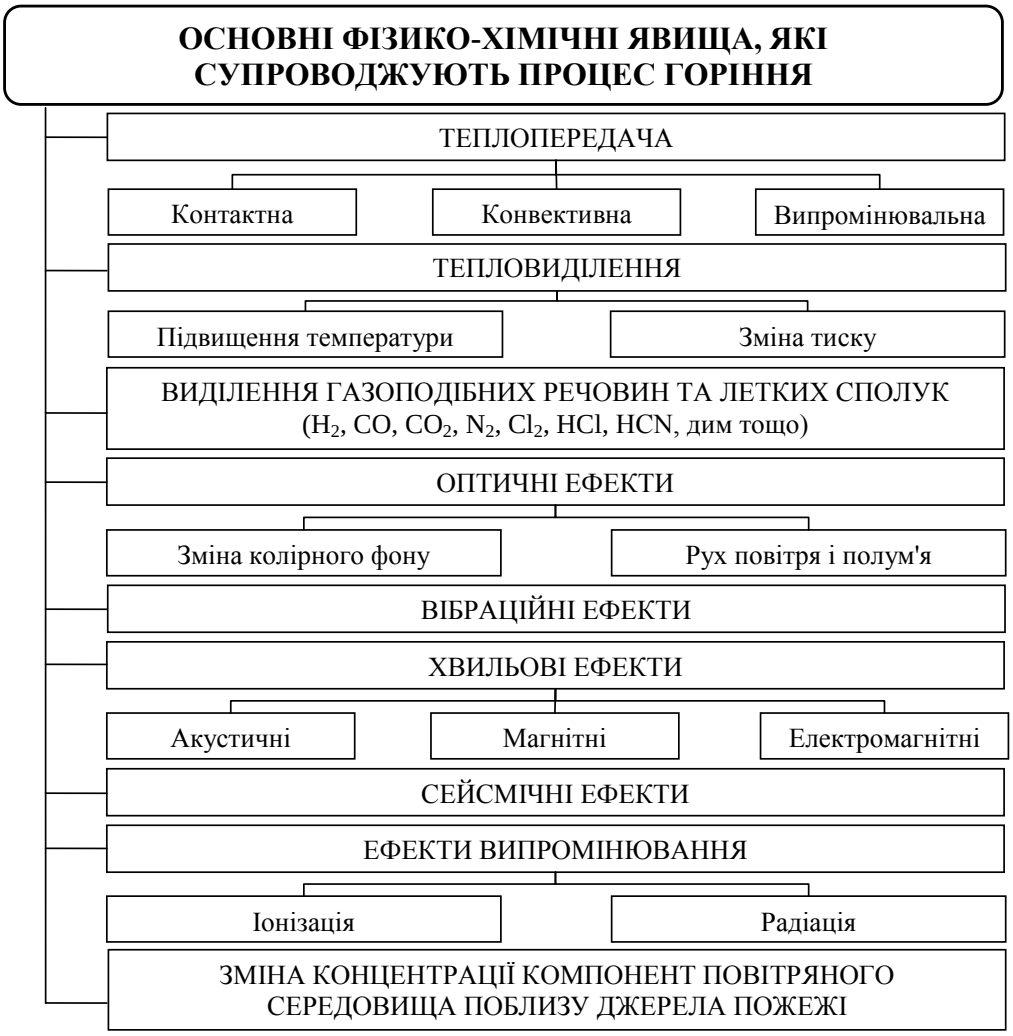

Рисунок 3.3 – Класифікація основних фізико-хімічних явищ, які супроводжують процес горіння

Реалізація режиму раннього виявлення джерел загоряння для ефективної боротьби з терористичними діями свідчить про необхідність технічної реалізації нових фізико-технічних методів аналізу властивостей середовища загоряння, спрямованих на практично миттєвий контроль хвильових факторів небезпеки на етапі зародження та прояву джерел загорянь.

Практична значимість методу контролю хвильових факторів підтверджується

тим, що вже відомі спроби ефективної технічної реалізації методу контролю пружних хвиль, які були викликані локальною динамічною перебудовою внутрішньої структури речовини (так званий процес акустичної емісії) для раннього розпізнавання тріщин в металах і сплавах, для виявлення прихованих дефектів на стадії їх зародження, для дослідження корозії металів під напругою, вивчення кінетики розвитку тріщин в зварних швах, а також для дослідження акустичних властивостей середовища загоряння [110–117].

На підтвердження цих уявлень необхідно особливо відзначити, що в літературних джерелах [118–122] описані позитивні результати про розширення областей використання методу акустичної емісії, наведені експериментальні спроби виявити можливості цього методу для дослідження хімічних реакцій та фізико-хімічних процесів. Так, для встановлення акустичної емісії, що супроводжує процеси в гомогенних середовищах, були обрані і досліджені процеси розчинення сірчаної кислоти та етилового спирту у воді. В результаті розчинення рідини в рідині були зафіксовані характерні акустичні сигнали та відзначено два принципових моменти, які при сущі явищу виникнення акустичної емісії в фізико-хімічних процесах: а) явище носить універсальний характер; б) імпульсний характер акустичної емісії при хімічних реакціях та фізико-хімічних процесах свідчать про те, що реакція відбувається в невеликому об’ємі і когерентно в часі в окремих ділянках системи, тому має місце колективна взаємодія субстратів.

Отримані результати дозволяють нам зробити припущення про перспективи створення пристрою акустичного контролю терористичних дій, в основу функціонування якого закладений принцип аналізу властивостей акустичних коливань, які випромінюються джерелом загоряння в результаті прояву ефекту акустичної емісії, як хвильового чинника на етапах прояву і розвитку пожежної небезпеки на локальній території у результаті підпалів, які скоюють терористи.

Фізико-хімічна суть прояву акустичної емісії при підпалі полягає в тому, що в процесі протікання окислювально-відновної реакції виникає спектр коливань, пов'язаних з виникненням і руйнуванням на молекулярному рівні напружень в кристалічній решітці матеріалу. При горінні же рідкої фази відбувається

переміщення мас реагентів і продуктів та утворення бульбашок газу, що призводять до коливань навколишнього середовища об'єкта загоряння (кавітаційні явища). Чим більше молекул речовини задіяні в процесі протікання реакції, тим інтенсивніше горіння та могутніше випромінюється звукове коливання. Ефект акустичної емісії має місце на всіх стадіях горіння, поки є деструкція матеріалу і температурний градієнт всередині вогнища горіння. При появі відкритого полум'я, коли реакція горіння переходить в стійку стадію, інтенсивність звукових коливань різко зростає. Це обумовлено при горінні твердих тіл посиленням ефектів деструкції і деформації матеріалу. Збільшення інтенсивності звукових коливань при горінні рідинно фазних матеріалів пов'язано з переходом в стадію кипіння поверхневого шару на границі полум'я. При цьому необхідно відзначити, що і саме полум'я викликає значні коливання повітря за рахунок нерівномірності течії реакції горіння. Крім того, виділення газових складових при горінні як твердих, так і рідких речовин, також призводить до локальних коливань повітря в місці виходу газу із зони горіння.

Функціональна схема система раннього виявлення (сформована нами на основі аналізу ефекту акустичної емісії при протіканні процесу горіння джерел загоряння) і попередження виникнення пожежної небезпеки від терористичних дій в контрольованій зоні навколо об’єктів кіберзахисту в кіберпросторі, включає акустичний пожежний сповіщувач (АПС), а також автоматичні системи виявлення (АСВП) і гасіння (АСГП) пожежі. Блок АПС включає акустичний чутливий елемент (АЧЕ) і пороговий пристрій (ПП) або кілька чутливих елементів і порогових пристроїв.

Принцип функціонування такої системи пожежної автоматики розкритий в графічному вигляді на рис. 3.4.

Відповідно до даних рис. 3.4, акустичні коливання, які випромінює джерело загоряння в результаті прояву ефекту акустичної емісії на первинних етапах появу та розвитку пожежної небезпеки, є демаскирующим хвильовим фактором, що запускає функціонування системи раннього виявлення та попередження виникнення пожежної небезпеки. Даний фактор має енергетично-частотну характеристику, в вигляді енергетичного показника, в залежності від частоти (F) і часу (t)

акустичного спектру, що виромінюється ($W^{\text{Акуст}}_{\text{Горіння}} \cdot (F, t)$).

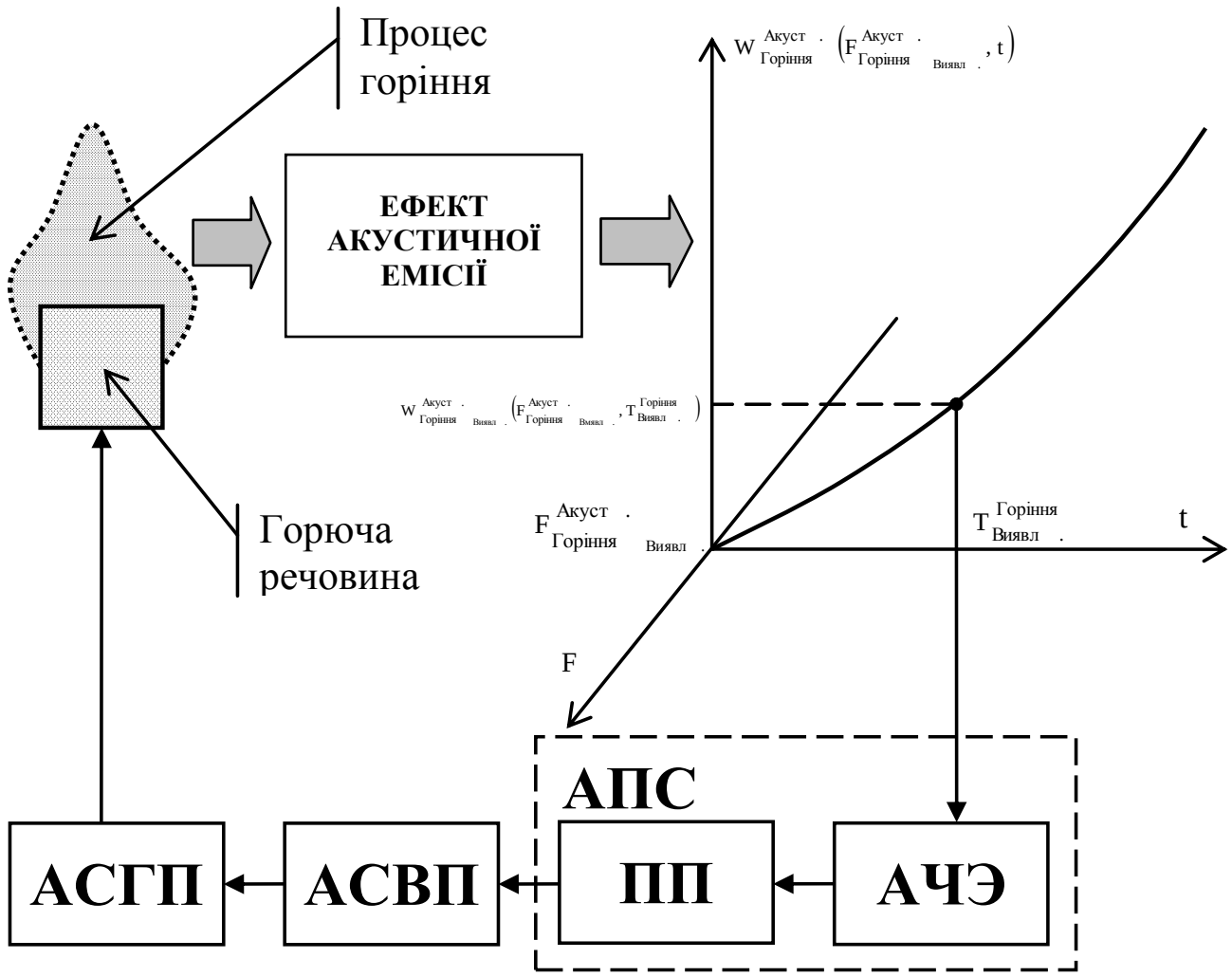

Рисунок 3.4 – Схема функціонування системи раннього виявлення, на основі аналізу ефекту акустичної емісії при протіканні процесу горіння, і попередження виникнення пожежної небезпеки від терористичних дій в контрольованій зоні навколо об’єктів кіберзахисту в кіберпросторі: АПС – акустичний пожежний сповіщувач; АЧЕ – акустичний чутливий елемент (мікрофон); ПП – пороговий пристрій; АСВП – автоматична система виявлення пожежі; АСГП – автоматична система гасіння пожежі

Цей ефект генерації акустичних коливань в процесі прояву й розвитку

пожежної небезпеки (як і при протіканні інших фізико-хімічних процесів) випливає з аналізу об'єднаного рівняння першого і другого законів термодинаміки:

$$dG = pdV - TdS + \sum \mu_i dn_i + \varphi dq + \sigma ds + \ldots, \quad (3.1)$$

де G – енергія Гіббса; S – ентропія; T – температура; V – об’єм; p – тиск; σ – поверхнева напруга (поверхнева напруга для твердих тіл); s – площа поверхні; μ_i – хімічний потенціал і-го компоненту; n_i – кількість молей і-го компоненту; φ – електричний потенціал; q – електричний заряд.

За аналогією з відомими процесами перетворення хімічної енергії в електричну (φdq), теплову (TdS) та електромагнітну, має відбуватися безпосереднє перетворення її в механічну (pdV). Оскільки, у всій системі одинична зміна обсягу у вигляді єдиного імпульсу не може статися в силу фізичних властивостей, то в системі будуть порушуватися акустичні коливання.

У зв'язку з тим, що імпульсний характер акустичної емісії характеризується імпульсами тривалістю $10^{-8} - 10^{-4}$ с (час елементарного акту передачі $\bar{e}$ в хімічній реакції), а енергія окремого імпульсу – від 10^{-9} до 10^{-5} Дж, то частотний спектр акустичної емісії лежить в широких межах від області інфразвуку і частот чутного звуку до десятків і сотень МГц, інтенсивність імпульсів акустичної емісії залежить від обсягу зони, в якій речовина піддається деструкції, а також від зміни обсягу продуктів реакції.

Значення амплітуди механічних коливань (звукові хвилі) в твердих тілах при хімічних реакціях, згідно, знаходяться в межах від $1 \cdot 10^{-4}$ до 5 мм.

Характерний частотний діапазон хімічних реакцій, відповідно до даних рис. 3.5, виходить за області частотних діапазонів, які характерні основним видам життєдіяльності території України. Отже, можливо виділити характеристичний для джерела загоряння спектр випромінюваних звукових хвиль на фоні загального звукового випромінювання [123–125].

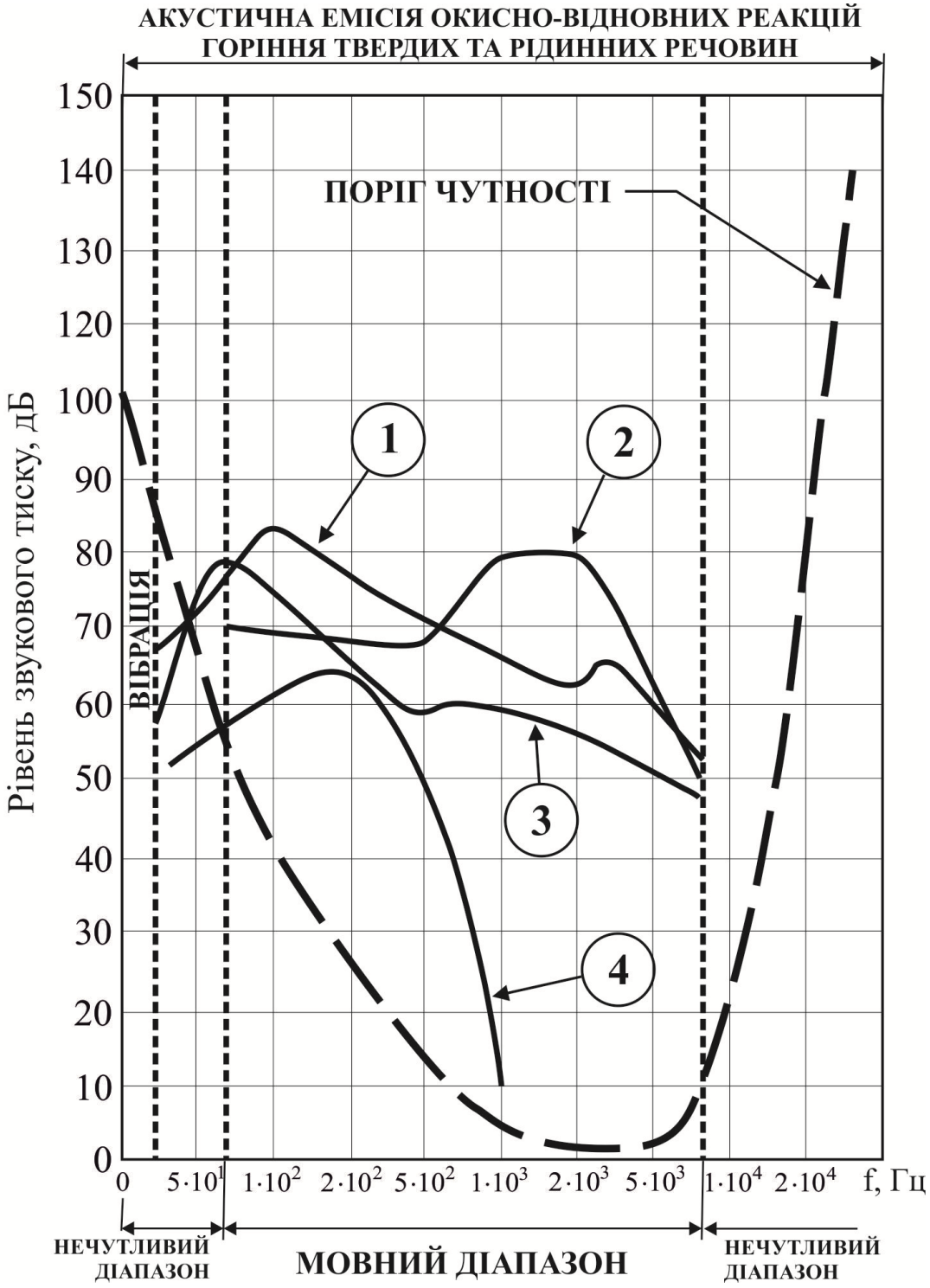

Рисунок 3.5 – Спектральні характеристики основних перешкод для функціонування автоматизованих пристроїв контролю акустичного простору у зоні терористичних дій, які виникають у процесі життєдіяльності локальної території: 1 – транспортні потоки (на відстані 7,5 м) при інтенсивності руху 250 автомобілів за годину; 2 – потяг (на відстані 25 м) при швидкості руху 160 км/год; 3 – місто; 4 – гелікоптер (на відстані 150 м) при швидкості 190 км/год

Дослідження, які були проведені у роботах [126–128], лягли в основу подальших науково-технічних досліджень спектральних характеристик горіння різного роду матеріалів в умовах реалізації підпалів при організації терористичних дій у вигляді порушень правопорядку на локальній території, з метою розробки автоматизованих пристроїв контролю акустичного простору, як складових системи оперативного моніторингу за зоною терористичних дій, рівнем небезпеки в ній та прогнозування виникнення нових ризиків.

Згідно з даними рис. 3.6, ефект акустичної емісії має місце на всіх стадіях горіння. Так, акустичні хвилі будуть випромінюватися протягом усіх стадій горіння, поки є деструкція матеріалу та температурний градієнт всередині джерела горіння. Стадії горіння целюлозовмісних або полімерних матеріалів можливо описати у вигляді наступних рівнянь хімічної реакції:

а) недостаток O_2 (піроліз):

$$nC_6H_{10}O_{5(т)} + nO_{2(г)} \xrightarrow{t} 4nC_{(т)} \downarrow + 2nCO_{(г)} \uparrow + 5nH_2O_{(г)} \uparrow \qquad (3.2)$$

б) надлишок O_2:

$$nC_6H_{10}O_{5(т)} + 3nO_{2(г)} \xrightarrow{t} 6nCO_{(г)} \uparrow + 5nH_2O_{(г)} \uparrow \qquad (3.3)$$

$$nC_6H_{10}O_{5(т)} + 4{,}5nO_{2(г)} \xrightarrow{t} 3nCO_{(г)} \uparrow + 3nCO_{2(г)} \uparrow + 5nH_2O_{(г)} \uparrow \qquad (3.4)$$

$$nC_6H_{10}O_{5(т)} + 6nO_{2(г)} \xrightarrow{t} 6nCO_{2(г)} \uparrow + 5nH_2O_{(г)} \uparrow \qquad (3.5)$$

в) у випадку утворення CO можливе подальше його горіння в умовах контакту у об'ємі полум'я з киснем:

$$CO \uparrow + O_2 \uparrow \xrightarrow{t} CO_2 \uparrow \qquad (3.6)$$

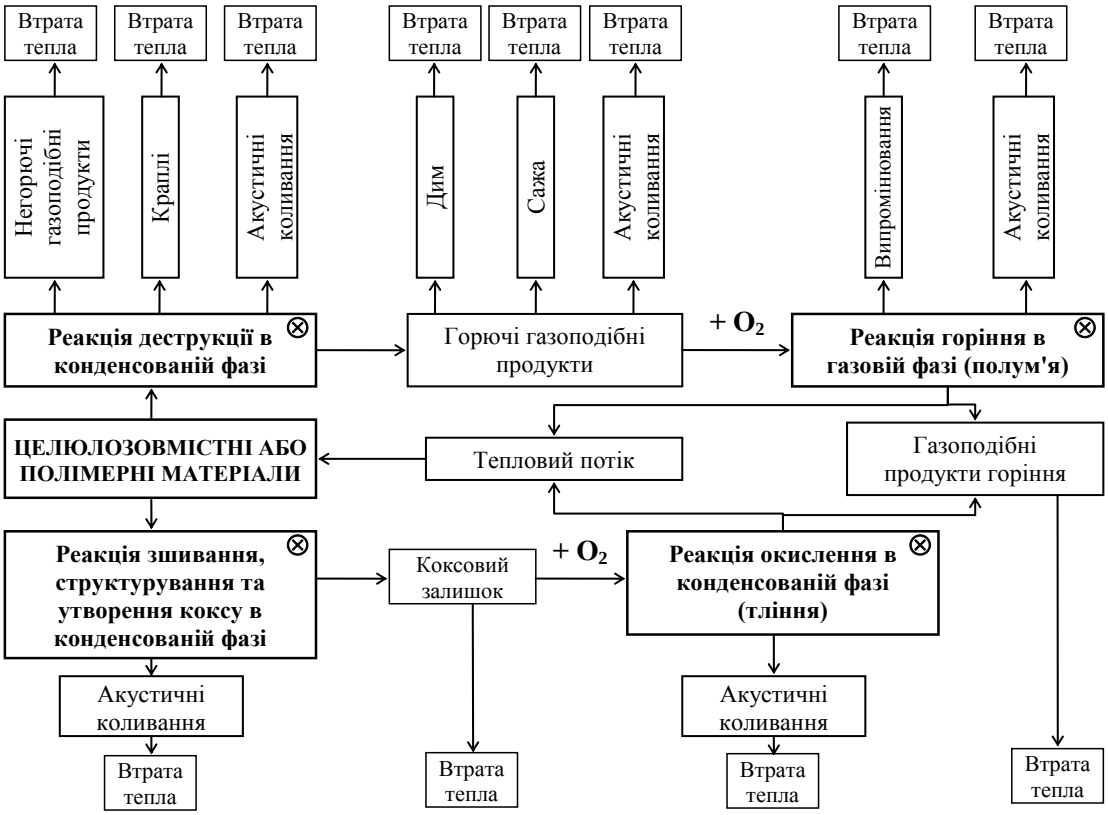

Рисунок 3.6 – Схема горіння целюлозовмісних або полімерних матеріалів та прояву ефекту акустичної емісії на стадіях горіння. ⊗ – найхарактерніші стадії акустичної емісії при фізико-хімічних перетвореннях

Для проведення лабораторних досліджень використано лабораторну установку, структурну схему та фото якої представлено на рис. 3.7 та 3.8.

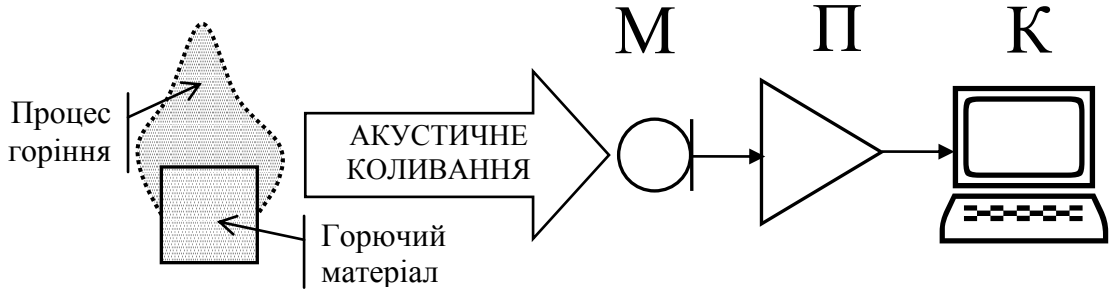

Рисунок 3.7 – Схема лабораторної установки для дослідження умов прояву ефекту акустичної емісії на стадіях горіння різних горючих матеріалів: М – мікрофон; П – підсилювач; К – комп'ютер

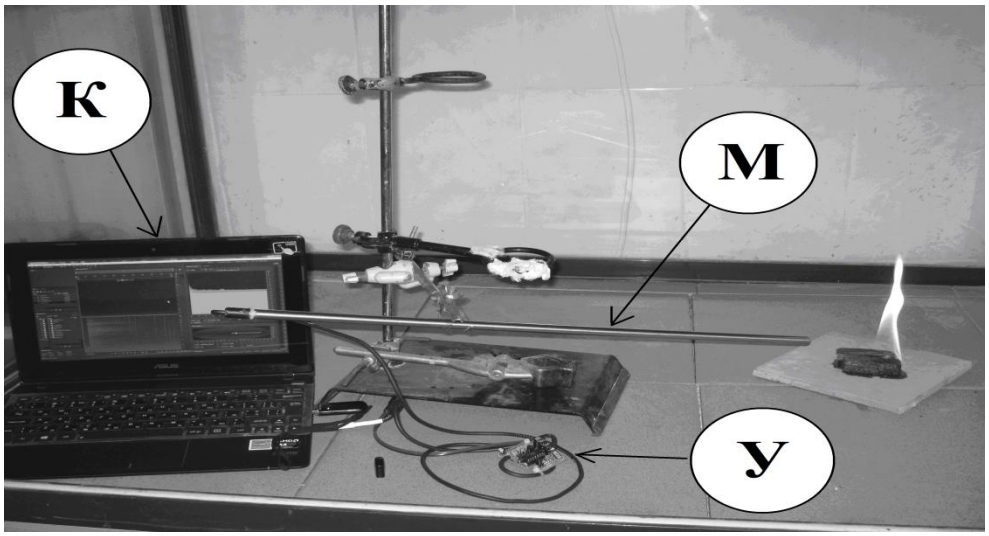

Рисунок 3.8 – Фото лабораторної установки для дослідження умов прояву ефекту акустичної емісії на стадіях горіння різних горючих матеріалів

Результати експериментів представлені на рис. 3.9–3.13 в вигляді амплітудно-частотних акустичних спектрів для деревини (сосна) та інших целлюлозовмісних матеріалів (бинт, картон, папір, вата).

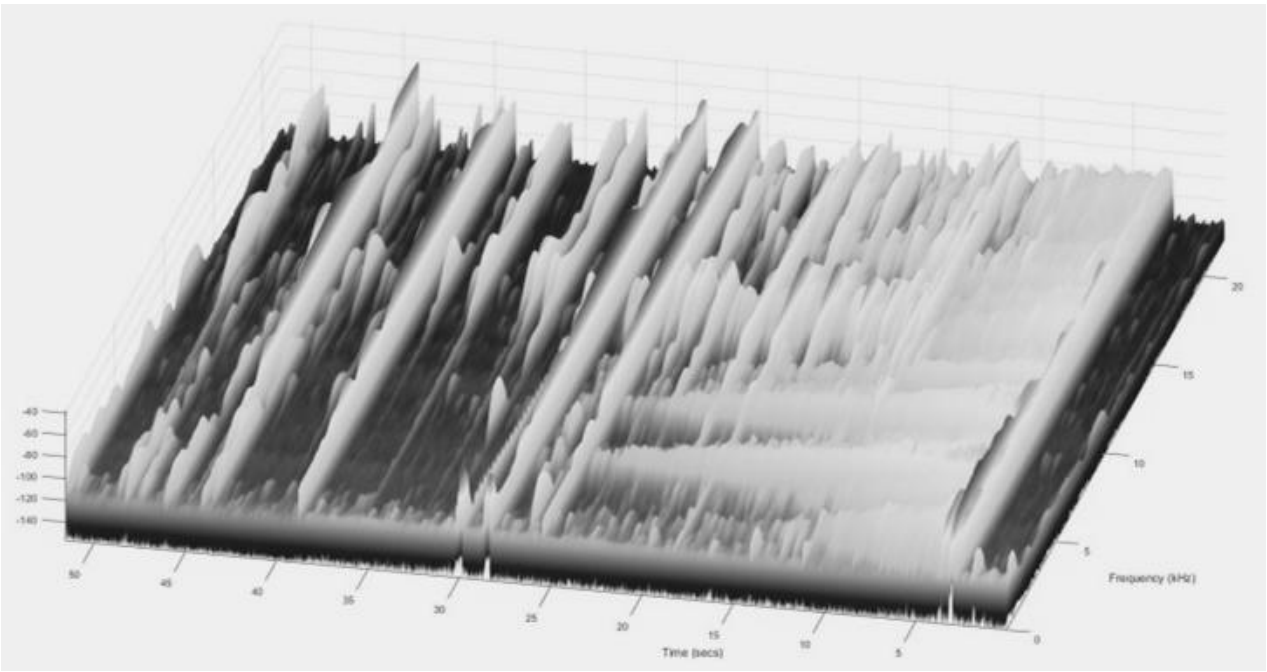

Рисунок 3.9 – Акустичні спектри від часу горіння зразка дерева (сосна) після фільтрації від фонових перешкод

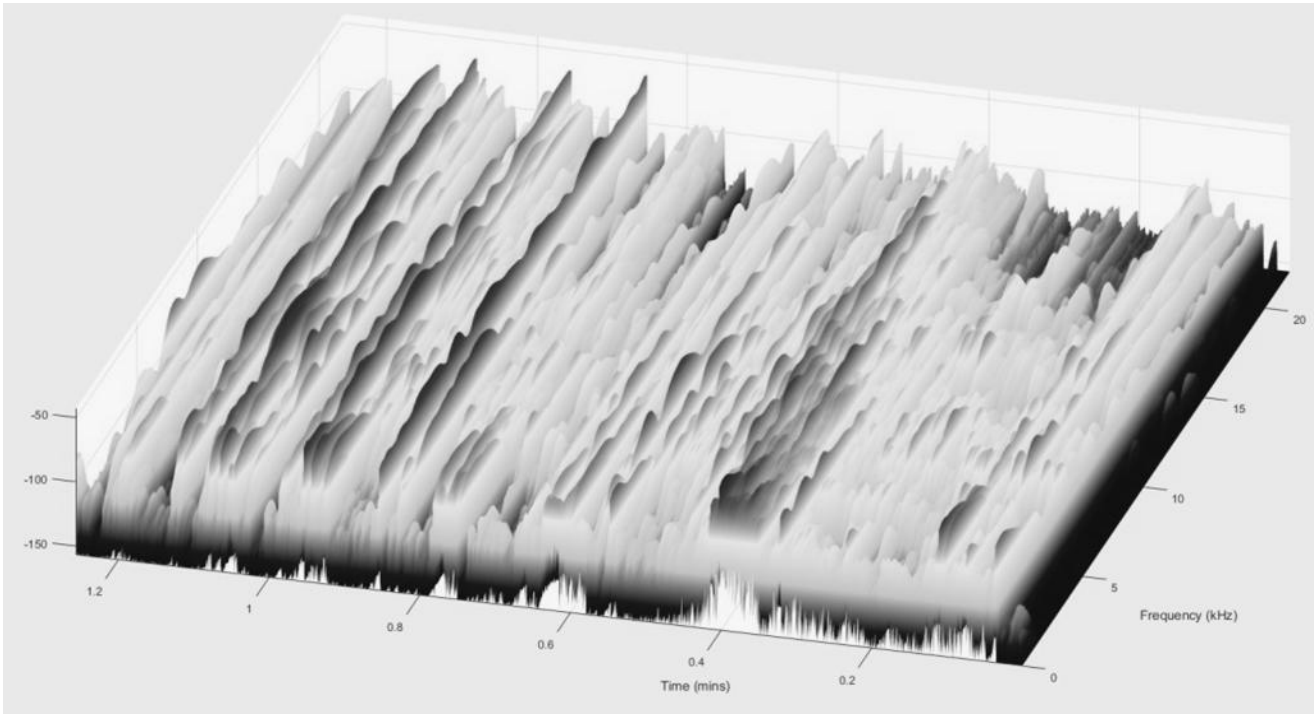

Рисунок 3.10 – Акустичні спектри від часу горіння зразка бумаги після фільтрації від фонових перешкод

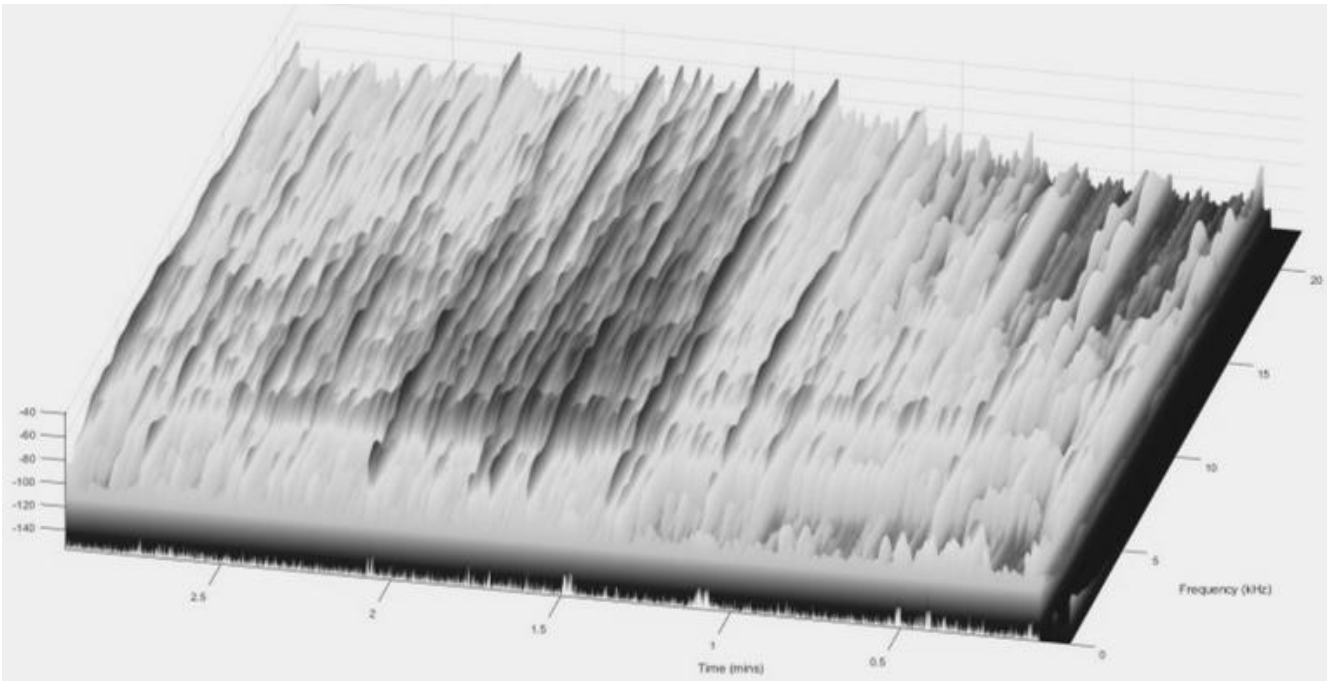

Рисунок 3.11 – Акустичні спектри від часу горіння зразка картону після фільтрації від фонових перешкод

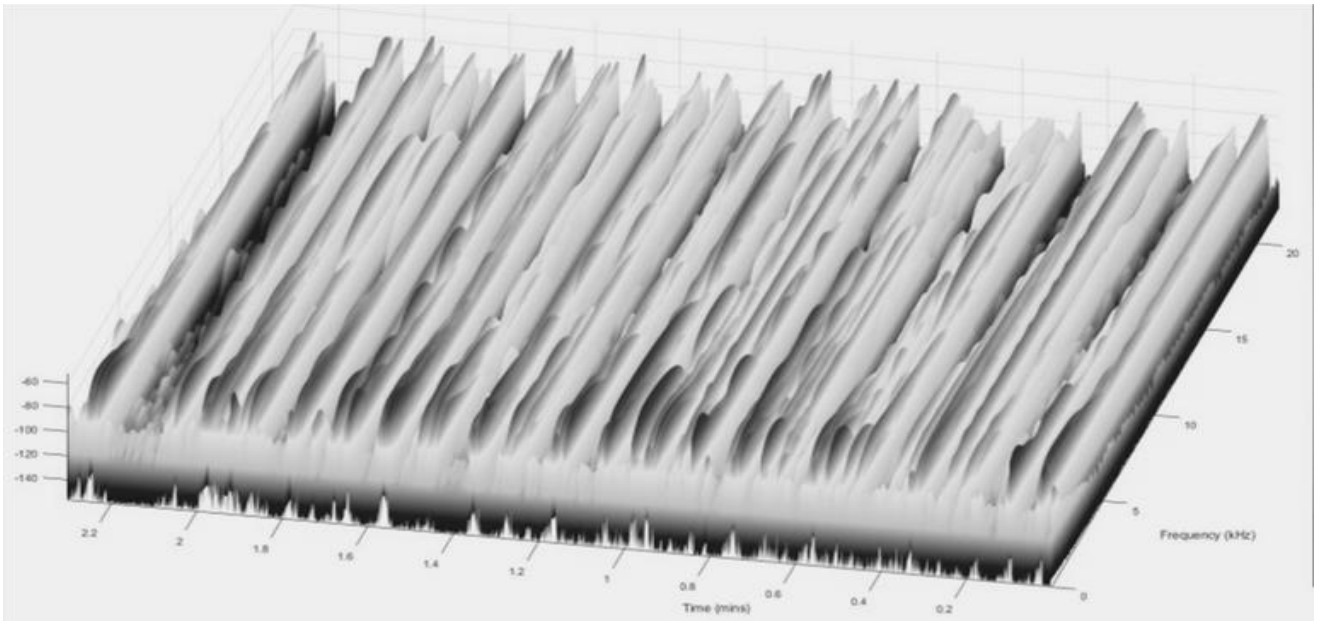

Рисунок 3.12 – Акустичні спектри від часу горіння зразка вати після фільтрації від фонових перешкод

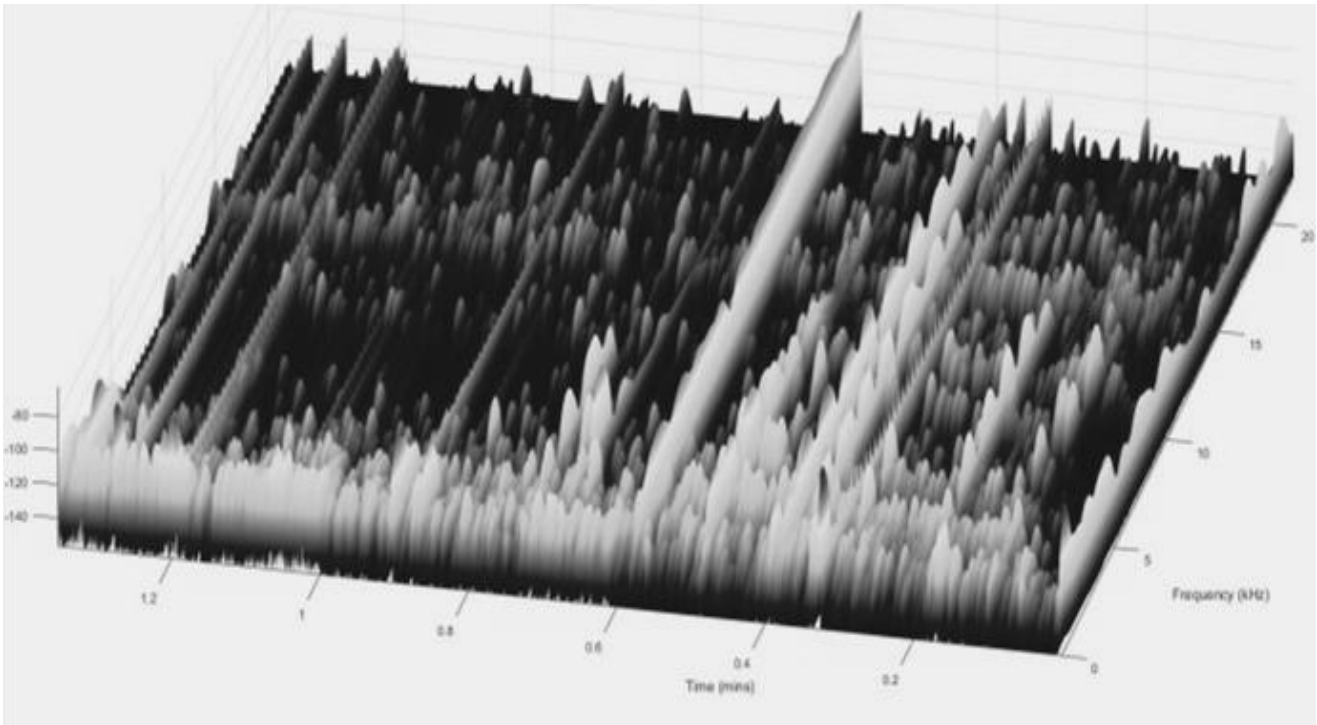

Рисунок 3.13 – Акустичні спектри від часу горіння зразка бинту після фільтрації від фонових перешкод

Обробка цих спектрів в єдиних координатах $P_{\min} / P_a$ (відносна амплітуда сигналу) від f (частота сигналу) показала задовільну збіжність пікових амплітуд досліджуваних зразків в різних діапазонах частот (5 Гц – 25 кГц). Незбіжність для деяких діапазонів частот пояснюється різним вмістом целюлози в зразках, а також специфікою самого процесу високотемпературного окислення, який істотно залежить від домішкових компонент матеріалу та структури досліджуваних зразків.

Узагальнену гістограму розподілу пікових амплітуд спектрів акустичної емісії для досліджених матеріалів (дослідження проведені на трьох зразках кожного типу целлюлозовмісного матеріалу) представлено на рис. 3.14. Усередненні для кожного типу целлюлозовмісного матеріалу амплітудно-частотних характеристики спектрів акустичної емісії при їх горінні представлені на рис. 3.15.

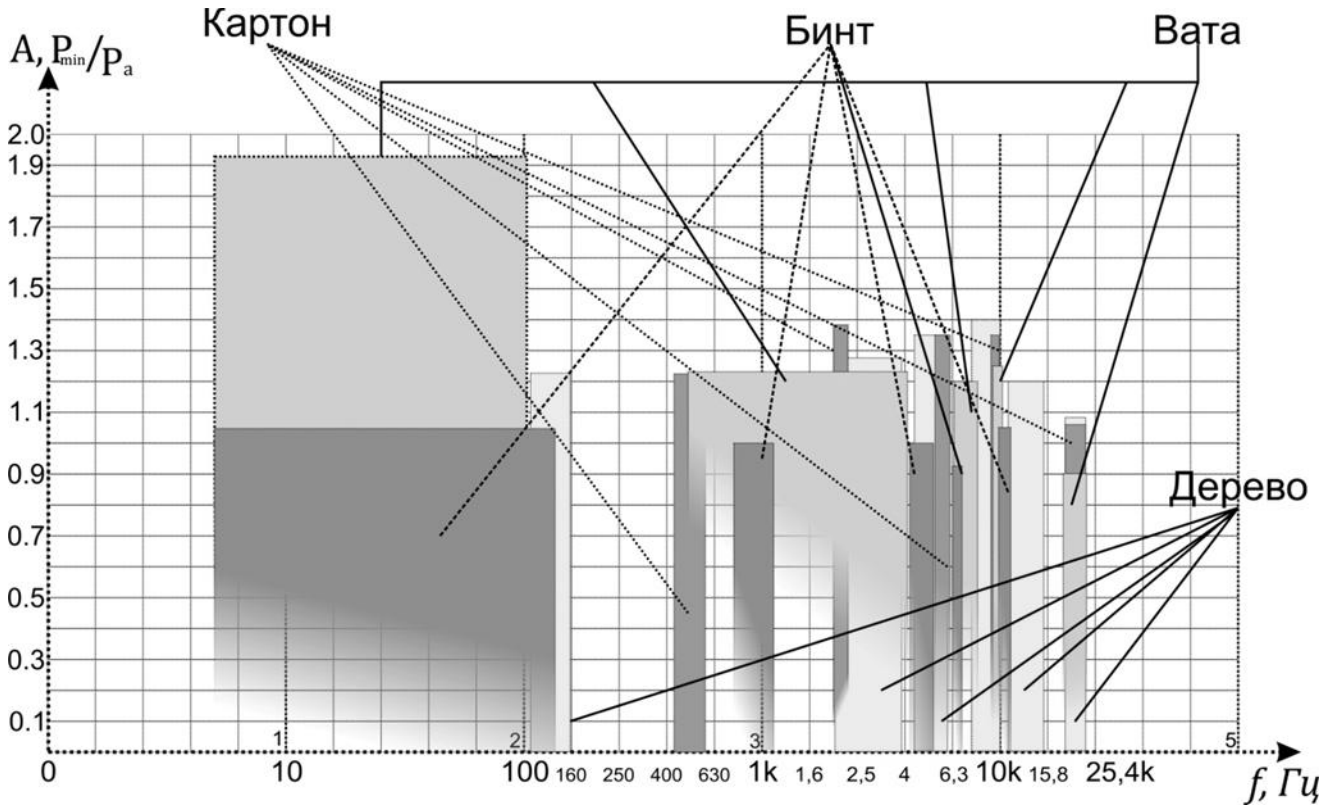

Рисунок 3.14 – Узагальнена гістограма характерних в діапазоні частот 5 Гц ÷ 20,4 кГц пікових відносних амплітуд спектрів акустичної емісії при горінні целлюлозовмісних матеріалів

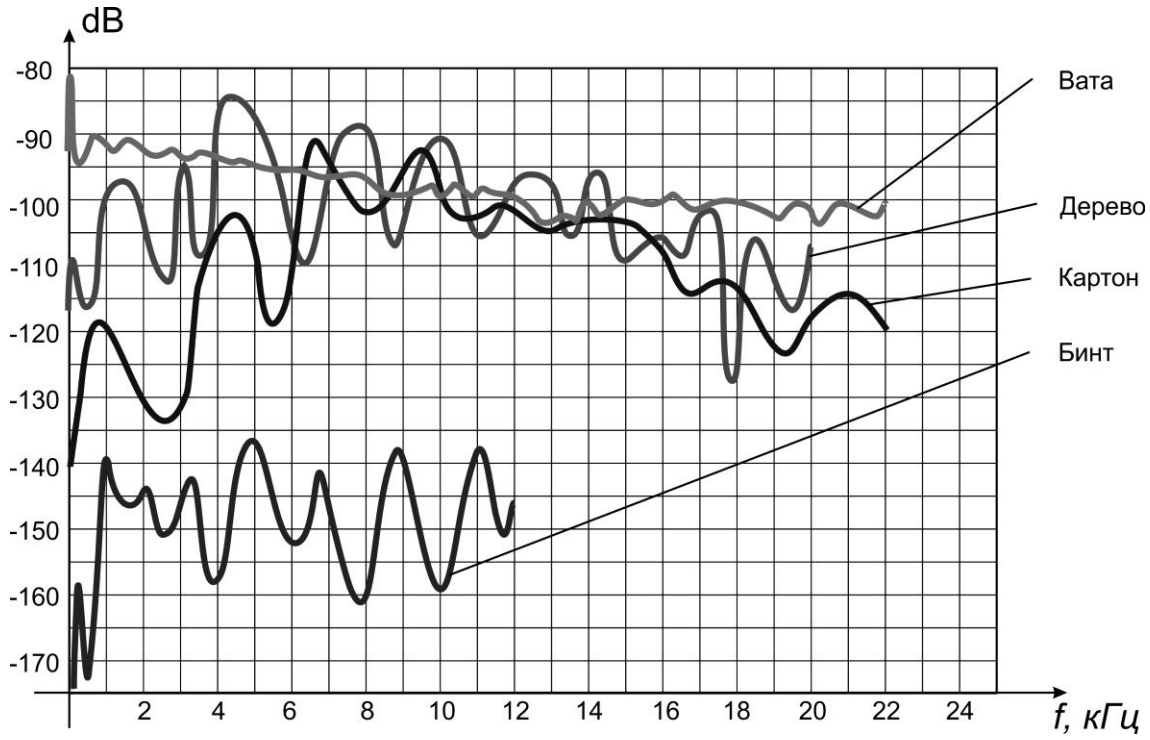

Рисунок 3.15 – Усередненні амплітудно-частотні характеристики спектрів акустичної емісії для кожного типу целлюлозовмісного матеріалу при їх горінні

Як видно з даних рис. 14, процес горіння досліджених матеріалів характеризується високою щільністю максимальних амплітуд в областях частот від 5 до 200 Гц і від 400 Гц до 25кГц. Максимальна збіжність амплітуд найбільш характерна для діапазону частот 1 – 11 кГц.

Наведені на рис. 14 та 15 результати досліджень показали, що процес горіння целлюлозовмісних матеріалів характеризується наявністю спектрів акустичної емісії в низькочастотних (від 0 до 1000 Гц) так і в високочастотних (від 1 до 25,4 кГц) областях. Амплітудна характеристика максимальна для вати ($P_{\min} / P_a = 1{,}92$, де $P_{\min} = 115\ dB$) в порівнянні з іншими матеріалами ($P_{\min} / P_a = 1{,}00 \div 1{,}40$) як для низькочастотних, так і для високочастотних областей.

Таким чином, виконані дослідження особливостей процесу горіння різних целлюлозовмісних матеріалів методом акустичної емісії однозначно вказують на високу ефективність встановлення фактів можливих підпалів при організації терористичних дій у зоні навколо об’єктів кіберзахисту.

Порівняння акустичних спектрів процесу горіння целлюлозосодержащих матеріалів показує їх стійке схожість, але в той же час і відмінність в залежності від виду матеріалу. Щоб провести повноцінне порівняння результатів, підтвердити їх не випадковість і зробити відповідні висновки про можливість однозначної ідентифікації спектра процесу АЕ різних матеріалів, застосуємо інший метод ідентифікації спектра процесу АЕ.

Для цього переведемо отримані акустичні сигнали в числовий вигляд, скориставшись одним з методів спектральної обробки сигналів. Метод заснований на фрактальному аналізі властивостей часового ряду [129, 130].

У зв'язку з тим, що звуковий сигнал являє собою набір значень, відомих тільки в дискретні моменти часу, тобто $t_n = n\Delta t$, $n = 0 \ldots N-1$, то сигнал можна записати у вигляді:

$$x_n = x(t_n) = \frac{\Delta\omega}{2\pi} \sum_{k=0}^{N-1} X(\omega_k) e^{i2\pi kn/N}, \qquad (3.7)$$

де ω – частота, а k – номер гармоніки [131] або, що зручніше для подальшого аналізу, як

$$x(t) = trend\ (t) + x^h(t) + r(t), \qquad (3.8)$$

де $trend\ (t)$ – тренд, який апроксимується поліномом 1, 2 і більш високого ступеня; $t=t_0,t_1,\ldots,t_n$ – моменти часу (рівні відліки); $x^h(t)$ – компонент, що виражає міру хаотичності ряду, що описує характер процесу і залежить від показника Херста $H(t)$ або показника фрактальної розмірності D_t [131, 132]; $r(t)$ – випадковий шум [133].

Фрактальна розмірність D тимчасового ряду (3.8) дозволяє визначити його властивості, пов'язані з хаотичністю, випадковістю і регулярністю [134], що може бути використано для ідентифікації сигналу АЕ, а, отже, і для виявлення раннього процесу загоряння відповідних матеріалів. Значення величини фрактальної

розмірності знаходиться в межах *1<D<2.*

Якщо значення D сигналу АЕ у зразків в межах однієї вибірки (процес АЕ 3-х зразків) дасть схожі результати і буде відрізнятися від значень D в вибірці іншого зразка, який також дасть схожі значення, то можна стверджувати з високою часткою ймовірності, що такий підхід можна застосувати при ідентифікації процесу АЕ раннього спалаху.

Фрактальна розмірність D пов'язана з показником Херста H [130] залежністю

$$D = 2 - H \text{ ,} \tag{3.9}$$

а показник H визначається з емпіричного закону Херста [130]:

$$\frac{R}{S} = \left(\frac{n}{2}\right)^{H} \text{ ,} \tag{3.10}$$

де R – максимальний розмах досліджуваного ряду, який визначається як $R = x_{\max}(t) - x_{\min}(t)$; S – середньоквадратичне відхилення спостережень; n – кількість спостережень (може приймати будь-яке ціле значення і відповідає відлікам тимчасового інтервалу дослідження сигналу); t – інтервал часу складається з n відліків.

Аналіз рівняння (3.10) показав, що при H = 0,5 – процес випадковий. Якщо 0<H<0,5 – процес антіперсістентний, тимчасовий. При 0,5<H<1, процес є персистентного, тобто довготривалим. І тільки при 1<H <2 процес набуває динамічний характер [133, 134].

Дробная розмірність сигналу, отримана в даному випадку, як сукупність фону та АЕ відповідного процесу горіння, результати розрахунків дробової розмірності для зразків дерева, паперу, вати, бинта і картону наведені на рис. 3.16. Звертає на себе увагу важливий факт суттєвої близькості наведених показників для зразків дерева і пресованого картону.

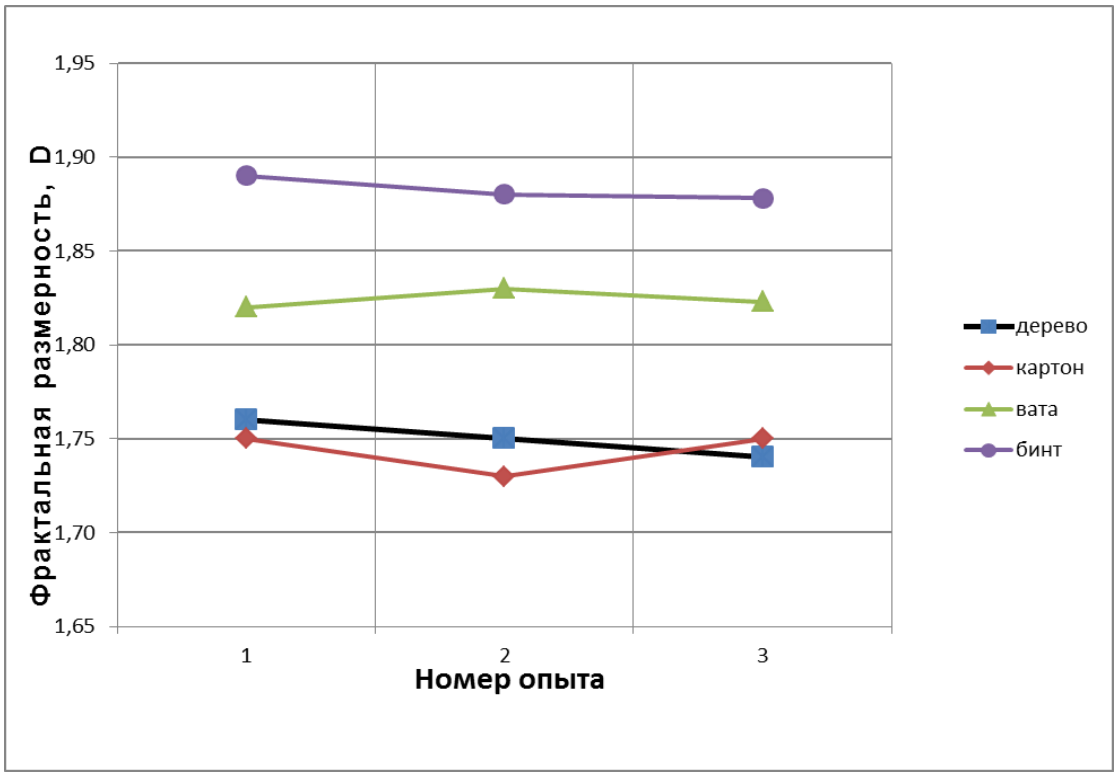

Рисунок 3.16 – Значення фрактальної розмірності випробовуваних зразків

На підставі результатів, отриманих різними методами, досліджень процесу АЕ (були застосовані: аналіз спектра на характерні пікові частоти і метод динаміки фрактальної розмірності) можна стверджувати, що процес АЕ різних матеріалів піддається однозначної ідентифікації і може бути використаний як новий фактор виявлення раннього спалаху.

3.1.2. Дослідження амплітудно-частотних спектрів акустичних сигналів від пострілів вогнепальної зброї при організації терористичних дій у зоні навколо об’єктів кіберзахисту

Однією із форм впливу терористів на умови нормального функціонування локальної території, як зони навколо об’єктів кіберзахисту, є постріли вогнепальної зброї.

Вогнепальна зброя – це механічний пристрій багаторазової дії, призначений для ураження цілі снарядом, що викидається енергією газів, утворюваних при

згоранні вибухової речовини [135–137].

Виділяють такі ознаки вогнепальної зброї:

1) вогнепальність, тобто надання снаряду кінетичної енергії пороховими газами при згоранні пороху. Проте виштовхнути снаряд зі ствола і передати йому достатню вражаючу силу можна й без вогню, наприклад стисненим повітрям, електромагнітною енергією. Це зброя іншого класу, але не вогнепальна;

2) наявність ствола – порожньої трубки для спрямування снаряда і спалення вибухової речовини, причому один кінець ствола герметично закривається при пострілі;

3) наявність пристрою для запалювання вибухової речовини. Найпростіший пристрій для запалювання – отвір у стволі, до якого для ініціювання пострілу підносять вогонь, складніший – ударно-спусковий механізм сучасної автоматичної зброї;

4) достатня вражаюча дія снаряда – енергетична характеристика снаряда, що визначає його здатність заподіяти людині чи тварині небезпечні для життя або смертельні ушкодження. Вона характеризується величиною питомої кінетичної енергії стріляного снаряда, яка повинна дорівнювати або бути більшою ніж 0,5 Дж/мм2;

5) достатня міцність конструкції – зброя повинна зробити не менш як два постріли, при цьому не зруйнувавшись.

Далі розглянемо основні типи вогнепальної зброї.

Револьвер (від англ. гєуоіує – обертатися) –- це особиста багатозарядна неавтоматична стрілецька зброя з обертовим барабаном, призначене для поранення супротивника на відстані до 100 м. Калібр бойових револьверів складає 7,62-11,56 мм, маса – 0,7-1,3 кг, ємність барабана 5-7 патронів, скорострільність 6-7 пострілів за 15-20 секунд.

Пістолет (франц. різіоіеі) є особистою вогнепальною зброєю , призначеною для поразки супротивника на відстані до 50-70 м (окремі зразки - до 200 м). Сучасні пістолети, як правило, самозарядні. Деякі зразки можуть вести автоматичний вогонь. Для підвищення стійкості при стрільбі і такі моделі мають префіксальний

плечовий упор, а також пристосовані для кріплення жорсткий (дерев'яної чи пластмасовий) чи приклада, оснащені додатково .

Пістолет-кулемет – це індивідуальна вогнепальна автоматична зброя, спроектована під пістолетний патрон. Він поєднує у собі портативність пістолета з безупинним кулеметним вогнем. Перший зразок пістолета-кулемета створений італійцем А. Ревеллі в 1915 р. Широке застосування вони одержали в роки другої світової війни. В даний час на озброєнні спеціальних підрозділів, МВС, поліції, повітрянодесантних військ, екіпажів бойових машин і ін.

Автомат (від грецького аиіотаіоз – самодіючий) –- це індивідуальна автоматична стрілецька зброя, призначена для поразки живої сили супротивника.

Для ведення рукопашного бою до автомата приєднується багнет-ніж. Сучасні автомати мають калібр 5,45-7,62 мм, масу 2,5-4,5 кг, темп стрільби 600 постр./хв і більше, дальність дії вогню до 400-600м, прицільну дальність до 1000-1200 м.

Автомати розроблені під патрон, що займає проміжне положення між пістолетним і гвинтівковим патроном, а також під малоімпульсний патрон малого калібру. Зі створенням бойової малокаліберної зброї різниця між автоматом і автоматичною гвинтівкою практично зникла.

У ряді країн подібні зразки стрілецької зброї називають штурмовими гвинтівками.

Гвинтівка – це індивідуальна стрілецька зброя з гвинтовою нарізкою в каналі ствола, призначена для поразки супротивника вогнем, багнетом і прикладом. Автоматична гвинтівка. Після другої світової війни в основному використовуються автоматичні гвинтівки й карабіни. Є також снайперські і спортивні гвинтівки. В автоматичній гвинтівці передбачене ведення як автоматичного вогню, так і одиночної стрільби. У порівнянні з неавтоматичною (магазинною) вона має більш високу скорострільність, забезпечує меншу стомлюваність стрільця і зручність спостереження за цілями.

Кулемет – це автоматична стрілецька зброя для стрільби зі спеціальної опори (верстата, сошок), призначене для поразки кулями наземних, повітряних і надводних цілей.

Далі розглянемо основні складові частини вогнепальної зброї.

Ствол – це порожнистий циліндр, передня частина якого називається дулом, її торець (кінець) – дульним зрізом; задня частина стволу – це казенна частина, а її торець – казенний зріз.

Усередині казенної частини стволу є патронник, або камора для компонентів заряду. В патронник вкладають патрон з пороховим зарядом і снарядом. Внутрішні стінки ствола бойової і спортивної зброї мають гвинтоподібні заглиблення, які називаються нарізами, а виступи, що утворюються між ними, - полями. У більшості вітчизняної ручної вогнепальної зброї в стволі є чотири гвинтові нарізи. У деяких зарубіжних зразках зустрічається більше чотирьох нарізів. Нарізи слугують для надання кулі обертального руху, що впливає на влучність стрільби. Стволи мисливських рушниць не мають нарізів і виготовляються менш тонкими, ніж стволи бойової зброї. Для поліпшення бойових властивостей (купчастості бою) дульна частина ствола незначно звужується, утворюючи «чок», а іноді й нарізи.

Ударно-спусковий механізм – це взаємопов’язана система частин зброї, призначена для подачі патрона в патронник (зарядження), замикання каналу ствола в момент пострілу, запалювання капсуля і заряду, виймання відстріляної гільзи з патронника. Ударно-спусковий механізм приводиться в дію енергією порохових газів в момент пострілу або вручну. Ударні механізми бувають куркові (револьвер «Наган» зразка 1895 р.), ударникові (револьвер ТК калібру 6,35 мм), курково-ударникові (автомат Калашникова, пістолет Макарова) і затворні (пістолет-кулемет Шпагіна).

Вогнепальну зброю поділяють:

1) за ступенем автоматичності – на автоматичну, напівавтоматичну і неавтоматичну. В автоматичній зброї енергією вибухової речовини, що згорає, здійснюється зарядження, установка на бойовий звід, а після пострілу - виймання гільзи. Коли при натисканні на спусковий гачок здійснюється кілька пострілів, така зброя називається автоматичною – це пістолет конструкції І.Я. Стєчкіна (ПС), автомат М.Т. Калашникова (АК), пістолет-кулемет Г.С. Шпагіна (ПКШ), І.О. Судаєва (ПКС), В.О. Дегтярьова (ПКД) тощо.

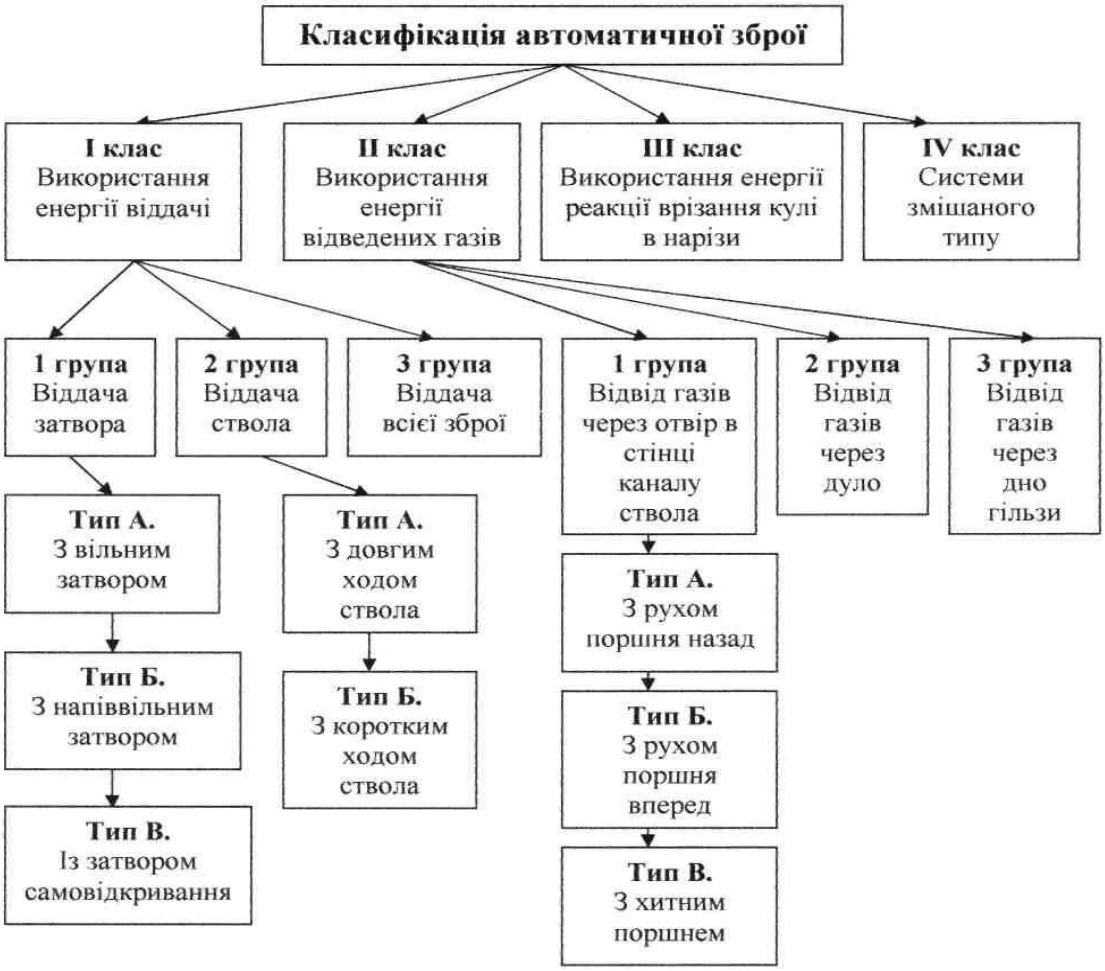

Рисунок 3.17 – Класифікація стрілецької зброї за принципом дії автоматики та призначенням

Якщо при натисканні на спусковий гачок відбувається один постріл і цикл повторюється знову, таку зброю називають напівавтоматичною. Наприклад, такі моделі пістолетів, як тульський конструкції Ф.В. Токарева (ТТ), М.Ф. Макарова (ПМ), німецькі Г. Люгера «Парабеллум», «Вальтер» та інші.

У неавтоматичній зброї перезарядження і установка затвора на бойовий звід здійснюються вручну. Так, для підготовки гвинтівки до стрільби слід відвести затвор назад, дослати його до упора вперед і замкнути ствол. До неавтоматичної зброї належать револьвери, більшість мисливських рушниць, гвинтівки, карабіни. Останнім часом поміж спортивної та мисливської зброї зустрічається й

напівавтоматична;

2) за цільовим призначенням – на бойову, мисливську, спортивну та багатоцільову. Бойова зброя призначена для ураження людей або техніки у бою (гвинтівки, карабіни, автомати, пістолети, револьвери та ін.); мисливська - для ураження тварин і птахів під час полювання (рушниці, карабіни, штуцери); спортивна – для ураження цілей під час спортивних змагань (малокаліберні гвинтівки, пістолети); багатоцільова передбачає можливість її використання для різних цілей - полювання, самооборони, спорту тощо;

3) за способом виготовлення – на заводську, кустарну, саморобну, перероблену. Заводська зброя виготовляється в умовах промислового виробництва на технічно обладнаному підприємстві за відповідними державними або фірмовими стандартами; саморобна - як правило, з підручних матеріалів, іноді з використанням деталей заводської зброї без додержання якихось стандартів. Кустарна зброя відрізняється від саморобної тим, що вона збирається в майстернях, як правило, кустарями з використанням промислового обладнання. Іноді кустарну зброю важко відрізнити від заводської. Перероблена – це заводська зброя, яка має відхилення від стандартної, наприклад по довжині ствола (обрізи). До переробленої зброї також відносять газову, пневматичну зброю або пристрої господарсько-побутового призначення, у конструкцію яких саморобним способом внесено зміни та які внаслідок цього набули властивостей вогнепальної зброї;

4) за ступенем зарядження – однозарядна, багатозарядна. До однозарядної відносять одноствольні мисливські рушниці, деякі спортивні гвинтівки й пістолети.

Багатозарядними є револьвери й магазинні гвинтівки, карабіни, пістолети, автомати, дво-, три- і чотириствольні рушниці. Наприклад, дискові магазини пістолетів-кулеметів Шпагіна (ППШ-41) та Дегтярьова (ППД-40), що знаходились на озброєнні радянських військ під час Великої вітчизняної війни, вміщували 71 патрон калібру 7,62 мм; магазини пістолетів-кулеметів МП-38, МП- 40, що у той же час знаходились на озброєнні військ німецького вермахту, - лише 32 патрони калібру 9 мм;

5) за довжиною ствола – довгоствольна, середньоствольна і короткоствольна;

6) за кількістю стволів – одноствольна, двоствольна, багатоствольна;

7) за характером обробки ствола – нарізна, гладкоствольна і комбінована. Внутрішні стінки ствола бойової і спортивної зброї мають гвинтоподібні повздовжні заглиблення, що роблять один виток від казенної частини до дульного зрізу. Такі заглиблення називаються нарізами, а виступи, що утворюються між ними - полями. Нарізи надають кулі не тільки поступальний, але й обертальний рух, чим забезпечується її стабільне положення в польоті й заглиблення у перешкоду головною частиною. Нарізів у каналі стволу може бути чотири або шість, рідше - вісім. Вони мають лівий або правий нахил. За відстанню між полями нарізів визначається калібр зброї. Стволи мисливських рушниць виготовляються, як правило, гладкоствольними (без нарізів). Для покращення бойових властивостей (купчастості бою) дульну частину ствола незначно звужують, утворюючи «чок» або «напівчок». Іноді вона має й нарізи в кінці стволу («парадокс»). До комбінованої належить вогнепальна зброя, що має стволи як з нарізними, так і з гладкими каналами;

8) за калібром – малокаліберна (до 6,5 мм), середньокаліберна (6,5-9 мм) і крупнокаліберна (понад 9 мм). В Україні калібр розраховується в міліметрах, в Англії - в тисячних, у США – в сотих дюйма. Найпоширеніші калібри: 5,6 мм (відповідно 220 або 22 дюйми); 6,35 мм (250 й 25); 7,65 мм (300 й 30); 9 мм (350 й 35); 11,43 мм (450 й 45). Вітчизняна бойова зброя має калібри: 5,45; 6,35; 7,62; 9,0 мм, спортивна – 5,6 мм. Калібр мисливської гладкоствольної зброї вимірюється кількістю шарових куль, виготовлених із одного англійського фунта свинцю (453,592 г). Якщо виготовити 12 куль до стволу відповідного діаметру, то це й буде 12-й калібр; чім більше куль, тим менше діаметр стволу, тобто калібр. Найбільш поширені калібри сучасної мисливської рушниці – 12 (відповідає діаметру 18,2 мм), 16 (16,8 мм), 20 (15,7 мм). Калібр позначається на казенній частині ствола та на денці гільзи;

9) за способом заряджання – дульнозарядна, казнозарядна. Одним з найбільш суттєвих недоліків вогнепальної зброї, що заряджається з дула, є її надто низька скорострільність. Наприклад, після появи перших зразків вогнепальної зброї у XIV

ст. вона тривалий час не могла конкурувати з такою метальною зброєю, як луки чи арбалети. Якщо лучник протягом хвилини міг випустити до 12 стріл, то мушкетер міг перезарядити мушкет з інтервалом у декілька хвилин. Сучасна вогнепальна зброя є казнозарядною, тобто заряджається з казенної частини стволу.

Для проведення лабораторних досліджень амплітудно-частотних спектрів акустичних сигналів від пострілів вогнепальної зброї використано лабораторну установку, структурну схему якої представлено на рис. 3.18.

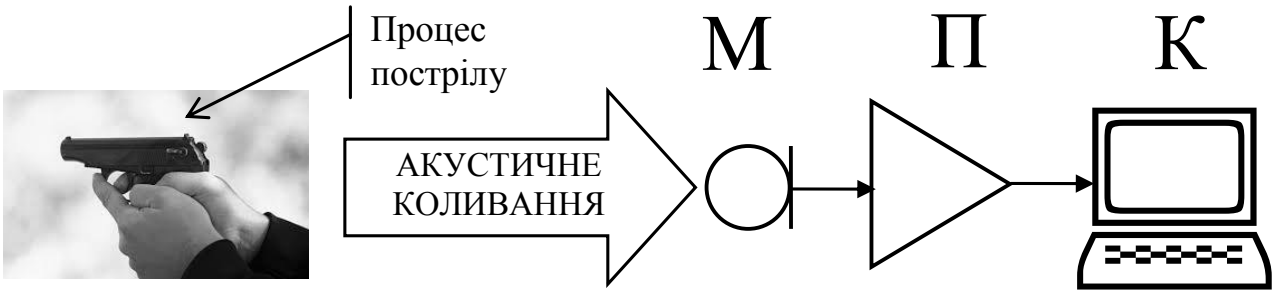

Рисунок 3.18 – Схема лабораторної установки для дослідження амплітудно-частотних спектрів акустичних сигналів від пострілів вогнепальної зброї: М – мікрофон; П – підсилювач; К – комп'ютер

Результати експериментів представлені на рис. 3.19–3.21 в вигляді амплітудно-частотних акустичних спектрів від пострілів пістолету Макарова (ПМ), автомату Калашникова (АК-45) та травматичного пістолету Форт (Форт-12Р).

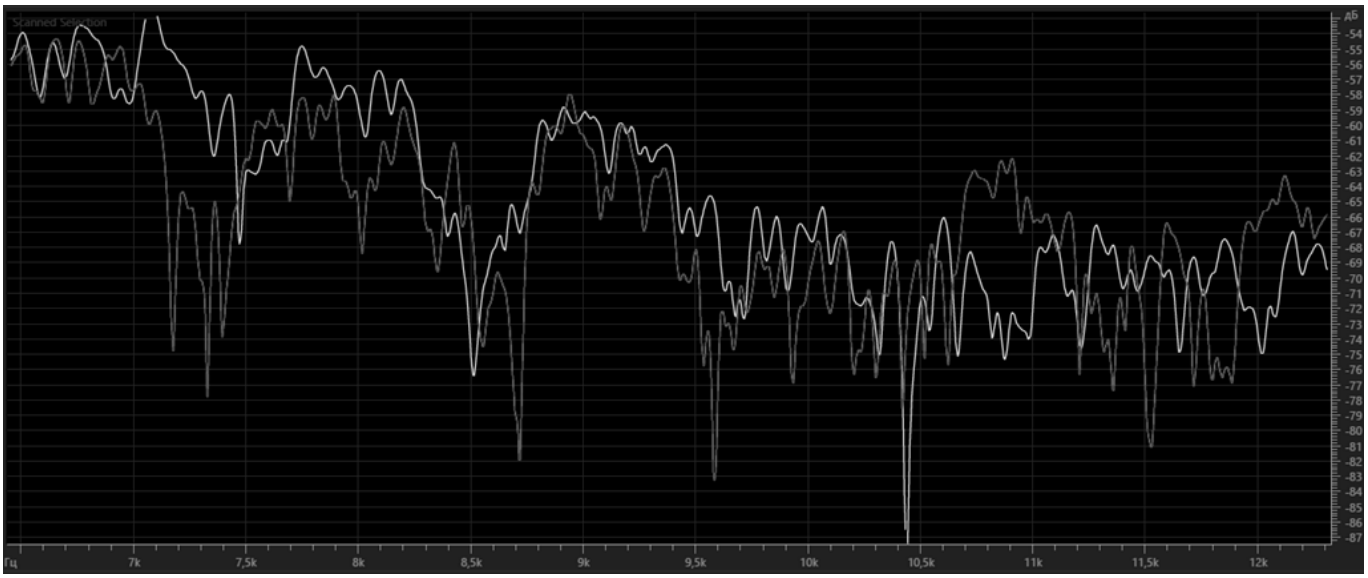

Рисунок 3.19 – Акустичні спектри від пострілів двох різних пістолетів Макарова після фільтрації від фонових перешкод

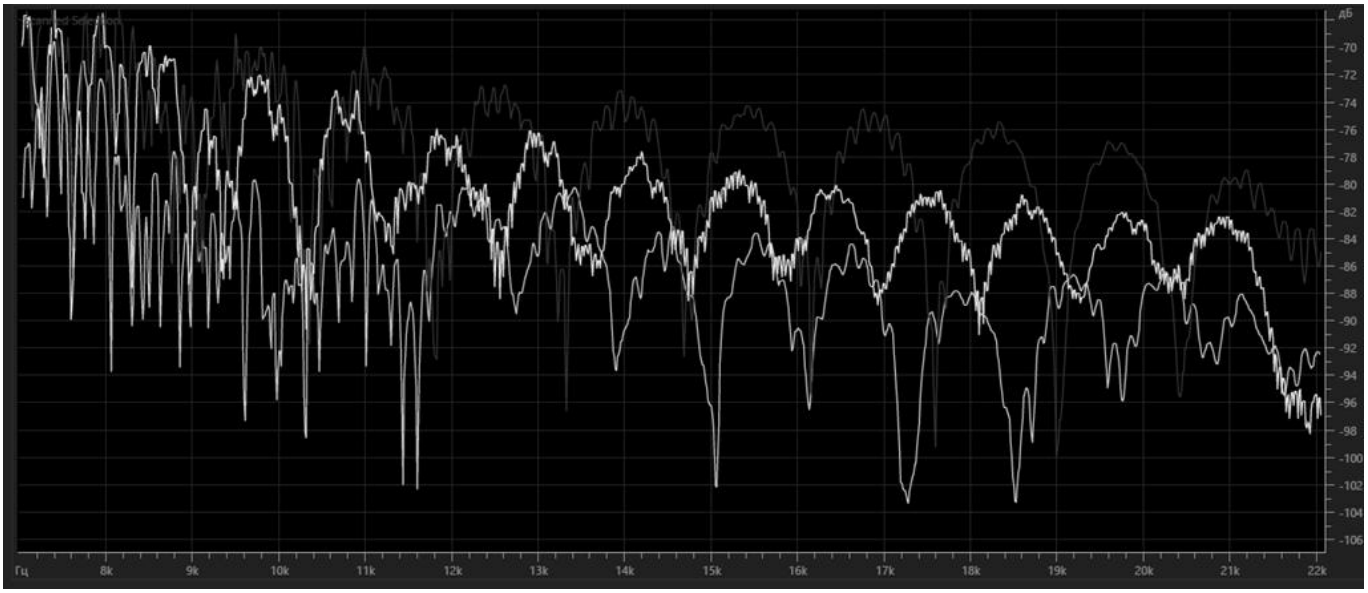

Рисунок 3.20 – Акустичні спектри від трьох автоматних черг АК-45 з різною кількістю пострілів після фільтрації від фонових перешкод

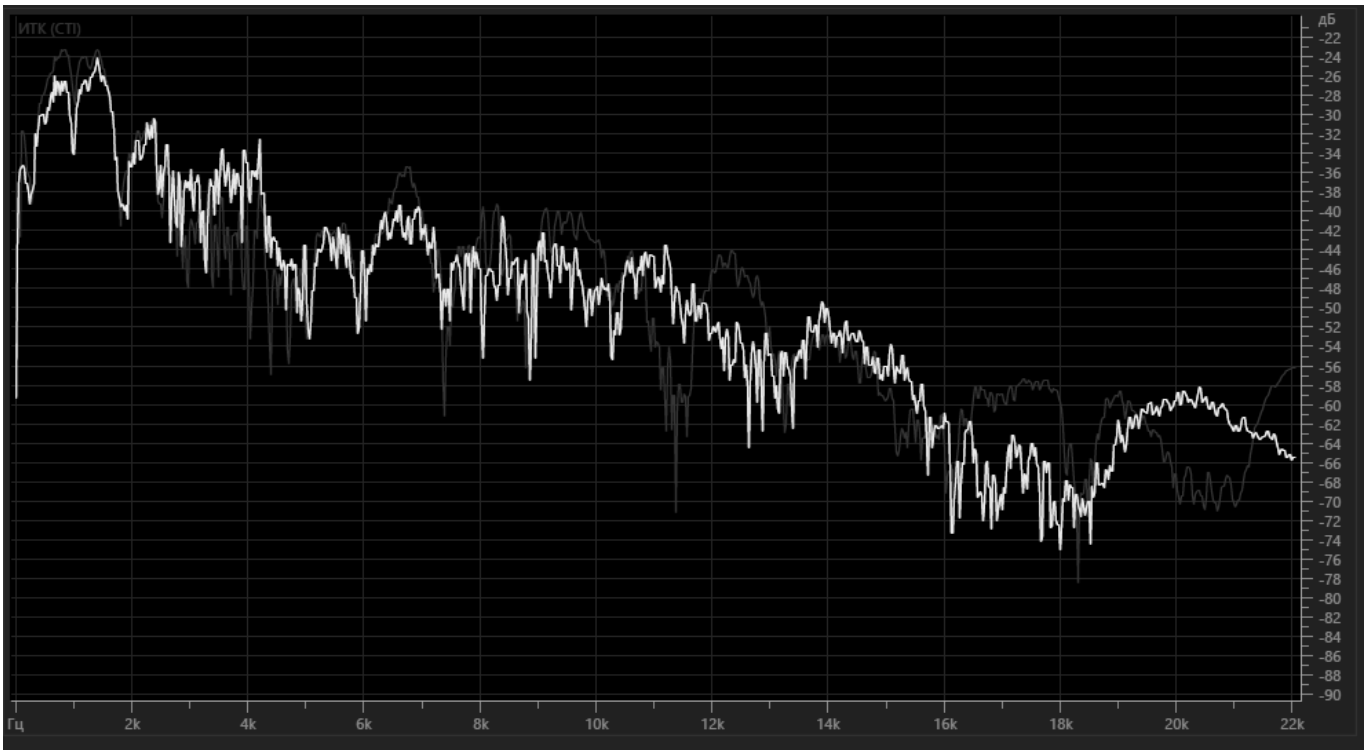

Рисунок 3.21 – Акустичні спектри від трьох автоматних черг АК-45 з різною кількістю пострілів після фільтрації від фонових перешкод

Таким чином, виконані дослідження амплітудно-частотних спектрів акустичних сигналів від пострілів вогнепальної зброї однозначно вказують на ефективність контролю акустичного простору в зоні навколо об’єктів кіберзахисту щодо встановлення факту використання та типу вогнепальної зброї при організації терористичних дій у зоні навколо об’єктів кіберзахисту.

3.2. Розробка функціональної схеми комплексу оперативного моніторингу (контролю) акустичного простору на об’єктах кіберзахисту

Тероризм, у відповідності за даними рис. 3.1, є суспільно-небезпечною діяльністю, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя і здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей

[81–91].

Терористична діяльність охоплює: 1) планування, організацію, підготовку і реалізацію терористичних актів; 2) підбурювання до вчинення терористичних актів, насильство над фізичними особами або організаціями, знищення матеріальних об'єктів у терористичних цілях; 3) організацію незаконних збройних формувань, злочинних угруповань (злочинних організацій), організованих злочинних груп для вчинення терористичних актів, так само як і участь в таких актах; 4) вербування, озброєння, підготовку та використання терористів; 5) пропаганду і поширення ідеології тероризму; 6) фінансування завідомо терористичних груп (організацій) або інше сприяння їм.

Безперервний та тривалий у реальному масштабі часу оперативний моніторинг за зоною терористичних дій здійснюється за рахунок: а) сумісного об’єднання у систему моніторингу БПЛА та наземних пристроїв акустичного контролю факторів небезпек; б) оперативної доставки наземних мобільних пристроїв акустичного контролю у зону терористичних дій за допомогою БПЛА; в) створення в зоні терористичних дій та в її околиці тимчасової (на період ліквідації небезпеки) контролюючої мережі з автоматизованих наземних мобільних пристроїв акустичного контролю; г) отримання й обробки інформації від наземних мобільних пристроїв акустичного контролю диспетчерським пунктом, який розташовано на наземній рухомій платформі.

Функціональну схему цієї підсистеми оперативного моніторингу за зоною терористичних дій, рівнем небезпеки в ній та прогнозування виникнення нових ризиків представлено на рис. 3.22 [138–142].

Функціонування розробленої підсистеми оперативного акустичного моніторингу зони терористичних дій повинно здійснюватись у складі функціонуючої в Україні ЄДСЦЗ та в межах класичного контуру управління, який забезпечує: 1) збір, обробку та аналіз інформації; 2) моделювання НС терористичного характеру на території міста, регіону, держави; 3) розробку та ухвалення (в рамках ситуаційного центру) управлінських рішень щодо попередження та ліквідації НС терористичного характеру, а також мінімізації їх

наслідків; 4) виконання рішень щодо попередження та ліквідації НС терористичного характеру, а також мінімізації їх наслідків.

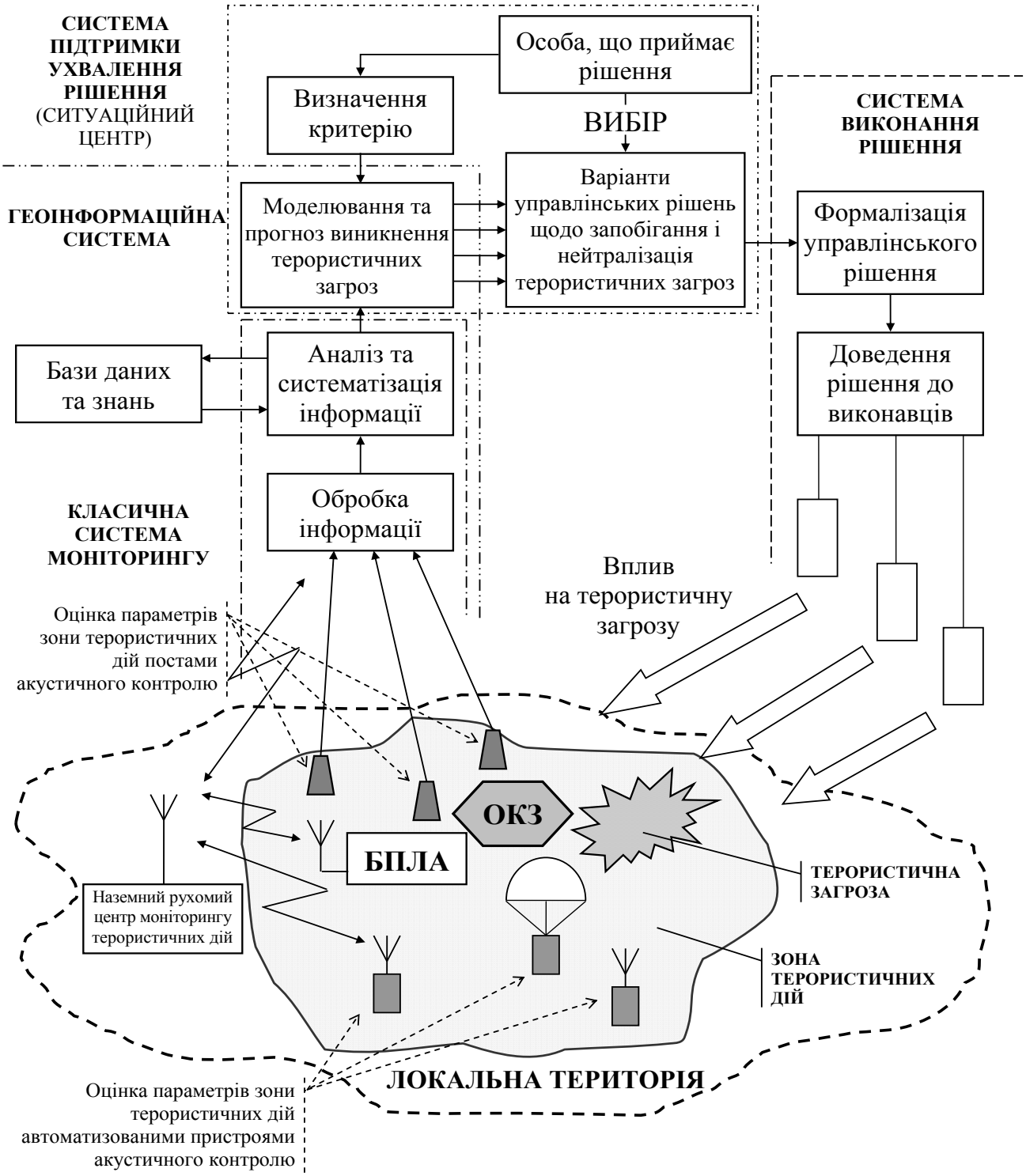

Рисунок 3.22 – Комплексна функціональна схема системи моніторингу зони терористичних дій навколо об’єктів кіберзахисту засобами акустичного контролю

У розробленій підсистемі отримання інформації про параметри зони терористичних дій здійснюється шляхом використання стаціонарних постів моніторингу акустичного простору та автоматизованими пристроями акустичного контролю, доставка яких у зону терористичних дій виконується БПЛА.

Отримана стаціонарними постами акустичного моніторингу первинна інформація про дії терористів на локальній території по кабелях передається до пристроїв другого рівня.

Первинну інформацію, що отримано автоматизованими пристроями акустичного контролю, які доставлено у зону терористичних дій за допомогою БПЛА, спочатку транслюють по радіоканалу до наземного рухомого центру моніторингу терористичних дій, де відбувається первинний аналіз та систематизація цієї інформації. Від наземного рухомого центру моніторингу терористичних дій інформація по радіоканалу транслюється також до пристроїв другого рівня.

Пристрої другого рівня призначені виконувати обробку отриманої інформації та представляти її у вигляді, необхідному для третього рівня.

Обробка отриманої інформації може виконуватися як в одному місці, так і на декількох, залежно від конкретної системи моніторингу та розмірів контрольованої нею локальної території. Оброблена інформація у відповідному вигляді надходить на третій рівень, де виконується її аналіз та систематизація даних, на основі чого робиться висновок про стан небезпеки локальної території. Особливо важливо для забезпечення швидкодії системи використання автоматизованих засобів обробки інформації, яке значно прискорить процеси на другому та третьому рівнях системи моніторингу, дозволить створити електронні, доступні в реальному масштабі часу, бази даних та знань. Використання відповідних математичних методів дозволить на основі отриманої інформації у відносно нетривалі терміни часу виконати моделювання небезпечної ситуації, прогнозування її розвитку та рівня, відображати прогнозовану динаміку катастрофічних подій графічно (у тому числі з використанням мап).

Друга інформаційна підсистема є системою підтримки ухвалення рішення. Особа, що приймає рішення (ОПР), визначає один або декілька критеріїв, відповідно

до яких здійснюється прогностичне моделювання розвитку небезпеки та виробляються варіанти управлінських рішень, які обґрунтовані відповідними розрахунками. З набору варіантів управлінських рішень ОПР обирає один, або задає ще додаткові критерії, відповідно до яких виконується моделювання та розробка управлінських рішень, направлених на недопущення розвитку небезпеки до рівня катастрофи. Якщо ж катастрофи вже не уникнути, то розробка управлінських рішень направлена на мінімізацію наслідків від неї.

Затверджене ОПР рішення надходить до третьої системи – системи виконання рішення, де виконується його формалізація та доведення до виконавців. Зміни стану локальної території та зміни стану небезпеки на ній викликатимуть зміни у величинах вимірюваних параметрів, що фіксуються пристроями контролю. Подальше моделювання покаже ефективність виконання управлінського рішення – контур управління замкнувся.

Висновки до розділу 3

1. Тероризм, як суспільно-небезпечна діяльність, полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя і здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей. Системний підхід і принцип оцінки небезпеки життєдіяльності в зоні безпеки навколо об’єктів кіберзахисту в умовах виникнення терористичних загроз повинні базуватися на використані функціональної поверхні, горизонтальні проекції якої співпадають з конфігурацією локальної території, а її випуклості відповідають рівням небезпеки в містах з конкретними географічними координатами.

2. Однією із небезпечних форм впливу терористів на умови нормального функціонування зони безпеки навколо об’єктів кіберзахисту є підпали. Реалізація режиму раннього виявлення джерел загоряння для ефективної боротьби з терористичними діями свідчить про необхідність технічної реалізації пристроїв

контролю за зоною терористичних дій на нових фізико-технічних методах аналізу властивостей середовища загоряння, спрямованих на практично миттєвому контролі хвильових факторів небезпеки на етапі зародження та прояву джерел загорянь. Запропоновано контроль джерела загоряння проводити по спектральним характеристикам акустичних коливань, що генеруються джерелом загоряння в результаті прояву ефекту акустичної емісії при протіканні окисно-відновної реакції горіння різних (твердих, рідких та газоподібних) речовин і матеріалів.

3. Прикладні результати проведених досліджень: а) розроблено та створено установку для вимірювання спектрів акустичної емісії з високою чутливістю, для широкого частотного діапазону (5Гц – 25кГц); б) розроблено комплексну методику та алгоритм фільтрації спектру фону із загальної акустичної спектрограми для визначення характеристичних гармонік прояви реакції горіння; в) показано стійку залежність амплітудно-частотних характеристик акустичної емісії процесу горіння від природи і хімічного складу целлюлозовмісних матеріалів; г) виконані дослідження особливостей процесу горіння різних целлюлозовмісних матеріалів методом акустичної емісії однозначно вказують на високу ефективність встановлення фактів можливих підпалів при організації терористичних дій у вигляді порушень правопорядку на локальній території.

4. Однією із небезпечних форм впливу терористів на умови нормального функціонування зони безпеки навколо об’єктів кіберзахисту також є постріли вогнепальної зброї. Виконані в роботі дослідження амплітудно-частотних спектрів акустичних сигналів від пострілів вогнепальної зброї однозначно вказують на ефективність контролю акустичного простору в зоні навколо об’єктів кіберзахисту щодо встановлення факту використання та типу вогнепальної зброї при організації терористичних дій у зоні навколо об’єктів кіберзахисту.

5. З метою забезпечення безперервного та тривалого у реальному масштабі часу моніторингу за зоною навколо об’єктів кіберзахисту розроблено функціональну схему комплексу оперативного моніторингу акустичної інформації від джерел терористичних небезпек на об’єктах кіберзахисту, який характеризується тим, що: а) сумісно застосовуються БПЛА та наземні пристрої контролю факторів

небезпек; б) оперативна доставка наземних мобільних пристроїв контролю у зону терористичних дій здійснюється за допомогою БПЛА; в) проводиться створення в зоні терористичних дій та в її околиці тимчасової (на період ліквідації небезпеки) контролюючої мережі з автоматизованих наземних мобільних пристроїв контролю; г) отримання й обробка інформації від наземних мобільних пристроїв контролю проводиться диспетчерським пунктом, який розташовано на наземній рухомій платформі.

ВИСНОВКИ

1. Сьогодні Україна зазнає значного впливу інцидентів та атак в кібернетичній сфері, що обумовлює необхідність своєчасного виявлення, запобігання й нейтралізації реальних і потенційних кібернетичних втручань і загроз особистим, корпоративним та національним інтересам.

2. Державна політика в сфері кібербезпеки заснована на чинних нормативно-правових актах, які спрямовані на реалізацію функцій держави стосовно забезпечення безпечності кіберпростору, мінімізації наслідків будь-яких кібератак, кіберінцидентів та кіберзагроз, нейтралізацію потенційно шкідливих наслідків як на рівні держави, так і приватних користувачів Інтернету, недопущення посягань на об'єкти національної критичної інформаційної інфраструктури з метою своєчасного запровадження дієвих заходів, адекватних характеру і масштабам реальних та потенційних кіберзагроз, спрямованих на захист інтересів людини, суспільства та держави у кіберпросторі.

3. Встановлено, що модель державного управління кібернетичною безпекою повинна містити такі основні складові: управлінську, забезпечуючу, результативну, а також комплекс засобів і інструментів управлінського впливу та є основою для забезпечення кібернетичної безпеки, спрямованої на створення безпечного кібернетичного простору.

4. Основу системи безпеки в умовах виникнення кіберзагроз становить класичний контур управління, який забезпечує: 1) збір, обробку та аналіз інформації; 2) моделювання розвитку обстановки на об’єкті кіберзахисту та розвитку рівня кіберзагроз на території міста, регіону, держави; 3) розробку та ухвалення управлінських рішень щодо запобігання та ліквідації небезпечних дій в умовах кібервійни, кібертероризму, кіберзлочинності та кібершпигунства, а також мінімізації їх наслідків; 4) виконання рішень щодо запобігання та ліквідації небезпечних дій в умовах кібервійни, кібертероризму, кіберзлочинності та кібершпигунства, а також мінімізації їх наслідків.

5. Створення ефективної інформаційно-аналітичної системи управління процесами попередження й локалізації наслідків небезпечних дій в умовах кібервійни, кібертероризму, кіберзлочинності та кібершпигунства відбувається шляхом комплексного включення в діючу систему безпеки держави по вертикалі від об’єктового до державного рівнів різних функціональних елементів територіальної системи моніторингу НС та складових системи ситуаційних центрів, які жорстко пов’язані між собою на інформаційному та виконавчому рівнях для прийняття відповідних антикризових рішень, для розв’язання різних функціональних задач моніторингу, попередження та ліквідації небезпечних дій.

6. Базуючись на уявленнях про класичний контур управління, в магістерській роботі представлені результати розповсюдження ризико-орієнтованого підходу для оцінки ефективності функціонування системи інформаційної безпеки ОКЗ в умовах розголошення та витоку інформації, а також в умовах виникнення загроз для комп’ютерної інформації. На базі отриманих результатів в роботі розроблено структурно-логічну схему процесу антикризового управління щодо запобігання виникнення загроз для інформації, що обертається у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків.

7. Тероризм, як суспільно-небезпечна діяльність, полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя і здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей. Системний підхід і принцип оцінки небезпеки життєдіяльності в зоні безпеки навколо об’єктів кіберзахисту в умовах виникнення терористичних загроз повинні базуватися на використані функціональної поверхні, горизонтальні проекції якої співпадають з конфігурацією локальної території, а її випуклості відповідають рівням небезпеки в містах з конкретними географічними координатами.

8. Однією із небезпечних форм впливу терористів на умови нормального функціонування зони безпеки навколо об’єктів кіберзахисту є підпали. Реалізація режиму раннього виявлення джерел загоряння для ефективної боротьби з

терористичними діями свідчить про необхідність технічної реалізації пристроїв контролю за зоною терористичних дій на нових фізико-технічних методах аналізу властивостей середовища загоряння, спрямованих на практично миттєвому контролі хвильових факторів небезпеки на етапі зародження та прояву джерел загорянь. Запропоновано контроль джерела загоряння проводити по спектральним характеристикам акустичних коливань, що генеруються джерелом загоряння в результаті прояву ефекту акустичної емісії при протіканні окисно-відновної реакції горіння різних (твердих, рідких та газоподібних) речовин і матеріалів.

9. Прикладні результати проведених досліджень: а) розроблено та створено установку для вимірювання спектрів акустичної емісії з високою чутливістю, для широкого частотного діапазону (5Гц – 25кГц); б) розроблено комплексну методику та алгоритм фільтрації спектру фону із загальної акустичної спектрограми для визначення характеристичних гармонік прояви реакції горіння; в) показано стійку залежність амплітудно-частотних характеристик акустичної емісії процесу горіння від природи і хімічного складу целлюлозовмісних матеріалів; г) виконані дослідження особливостей процесу горіння різних целлюлозовмісних матеріалів методом акустичної емісії однозначно вказують на високу ефективність встановлення фактів можливих підпалів при організації терористичних дій у вигляді порушень правопорядку на локальній території.

10. Однією із небезпечних форм впливу терористів на умови нормального функціонування зони безпеки навколо об’єктів кіберзахисту також є постріли вогнепальної зброї. Виконані в роботі дослідження амплітудно-частотних спектрів акустичних сигналів від пострілів вогнепальної зброї однозначно вказують на ефективність контролю акустичного простору в зоні навколо об’єктів кіберзахисту щодо встановлення факту використання та типу вогнепальної зброї при організації терористичних дій у зоні навколо об’єктів кіберзахисту.

11. З метою забезпечення безперервного та тривалого у реальному масштабі часу моніторингу за зоною навколо об’єктів кіберзахисту розроблено функціональну схему комплексу оперативного моніторингу акустичної інформації від джерел терористичних небезпек на об’єктах кіберзахисту, який характеризується

тим, що: а) сумісно застосовуються БПЛА та наземні пристрої контролю факторів небезпек; б) оперативна доставка наземних мобільних пристроїв контролю у зону терористичних дій здійснюється за допомогою БПЛА; в) проводиться створення в зоні терористичних дій та в її околиці тимчасової (на період ліквідації небезпеки) контролюючої мережі з автоматизованих наземних мобільних пристроїв контролю; г) отримання й обробка інформації від наземних мобільних пристроїв контролю проводиться диспетчерським пунктом, який розташовано на наземній рухомій платформі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355

2. Ліпкан В.А., Ліпкан О.С., Яковенко О.О. Національна і міжнародна безпека в визначеннях та поняттях . К.: Текст, 2006. 256 с.

3. Кондратьєв Я.Ю., Ліпкан В.А. Концепція національної безпеки України: теоретико-правові аспекти зарубіжного досвіду. – К.: Національна академія внутрішніх справ України, 2003. 20 с.

4. Петрів І. Конституційно-правове поняття національної безпеки / І. Петрів. // Право України. – 2005. – № 5. – С. 105–107.

5. Дзьобань О.П. Національна безпека України: концептуальні засади та світоглядний сенс: Монографія / О.П. Дзьобань. – Харків: Майдан, 2007. – 283 с.

6. Горбулін В.П. Стратегічне планування: вирішення проблем національної безпеки: Монографія / В.П. Горбулін, А.Б. Качинський. – Київ: Національний інститут стратегічних досліджень, 2011. – 286 с.

7. Качинський А.Б. Індикатори національної безпеки: визначення їх граничних значень: Монографія / А.Б. Качинський. – Київ: Національний інститут стратегічних досліджень, 2013. – 102 с.

8. Ліпкан В.А. Національна безпека та національні інтереси України / В.А. Ліпкан. – Київ: КНТ, 2006 – 68 с.

9. Ліпкан В.А. Національна безпека України / В.А. Ліпкан URL: http://westudents.com.ua/knigi/368-natsonalna-bezpeka-ukrani-lpkan-va.html

10. Циганов В.В. Національна безпека: проблеми визначення та оцінки ефективності / В.В. Циганов // Стратегічні пріоритети. – 2013. – № 3. – С. 122 – 127.

11. Bell D. The Social Framework of the Information Society. Oxford, 1980, 650 p.

12. Gates B. Business and the Speed of Thought: Level 6. London: Pearson Education Limited, 2008. 112 p.

13. Кастельс М. Информационная эпоха, общество и культура; Пер. с англ. под науч. ред. О.И. Шкаратана. М.: ГУ ВШЭ, 2000. 608 с.

14. Тоффлер Элвин Третья волна. Перевод на русский язык: А. Мирер, И. Москвина-Тарханова, В. Кулагина-Ярцева, Л. Бурмистрова, К. Бурмистров, Е. Комарова, А. Микиша, Е. Руднева, Н. Хмелик. М., 2010, 784с.

15. Information systems defence and security: France's strategy. French Network and Information Security Agency, 2011. C. 23. URL: www.gouvernement.fr/sites/default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf

16. International Strategy for Cyberspace. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

17. Internet Security Threat Report. 2017. Volume 23 URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

18. Internet World Stats. URL: https://www.internetworldstats.com/stats.htm

19. GA0-10-628. Key Private and Public Cyber Expectations Need to Be Consistently. URL: http://web.ebscohost.com

20. Growing pains 2018 Global CEO Outlook. KPMG International. URL: kpmg.com/CEOoutlook

21. Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійнотермінологічного апарату кібербезпеки. *Актуальні проблеми управління інформаційною безпекою держави:* Матеріали наук.-практ. конф., (22 березня 2011 р.). Київ, Вид-во НА СБ України, 2011. Ч. 2. С.43-48.

22. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки. *Інформація і право: науковий журнал.* К.: НДЦПІ НАПрН України, 2012. № 1(4). С.46-56.

23. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика.* 2014. № 2(42). URL: http://ippi.org.ua/baranov-oa-pro-tlumachennya-ta-viznachennya-ponyattya-"kiberbezpeka"

24. Дубов Д. Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка. URL: http://www.niss.gov.ua/articles/294

25. Панченко В. М. Співвідношення понять: інформаційна та кібернетична безпека. *Інформаційна безпека людини, суспільства, держави.* 2013. № 2 (12). С. 20-23.

26. Інформаційна та кібербезпека: соціотехнічний аспект / [авт. кол.: В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. В.Б. Толубко. – Київ: Державний університет телекомунікацій, 2015. – 288 с.

27. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19

28. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» URL: https://zakon.rada.gov.ua/laws/show/96/2016

29. Проект Концепції інформаційної безпеки України. URL: http://www.osce.org/uk/fom/175056?download=true

30. Діордіца І. Класифікація кіберзагроз та їх легітимація у нормативно-правових актах України. *Підприємництво, господарство і право.* 2017. № 10. С. 206-211.

31. Стратегічні комунікації: словник / за заг. ред. доктора юридичних наук В. А. Ліпкана. К. : ФОП Ліпкан О.С., 2016. 416 с.

32. Про сприяння розвитку громадянського суспільства в Україні: Указ Президента України від 26 лютого 2016 р. № 68/2016 URL: http://zakon3.rada.gov.ua/laws/show/68/2016

33. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. К.: Видавничий дім «АртЕк», 2017. 107 с.

34. Євсеєв С.П., Рзаєв Х.Н., Мамедова Т.А., Самедов Ф.Г., Ромащенко Н.В. Класифікатор кіберзагроз інформаційних ресурсів автоматизованих банківських систем. *Кібербезпека: освіта, наука, техніка.* 2018. №2. С. 47- 67.

35. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони: підручник. Одеса: ОНАЗ ім. О.С. Попова, 2018. 228 с.

36. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: монографія / за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с.

37. Петренко І. Сутність державної політики та державних цільових програм. *Вече.* 2011. №10. С. 23-25. URL: http://www. viche.info/journal/2566/

38. Юлдашев О.Х. Проблеми вдосконалення державної регуляторної політики в Україні. Київ: МАУП, 2005. 336 с.

39. Островий О.В. Формування державної політики забезпечення кібернетичної безпеки в Україні. Дисертація на здобуття наукового ступеня кандидата наук з державного управління. Маріуполь: Донецький державний університет управління, 2019. 253 с.

40. Черногор Л.Ф. Физика и экология катастроф / Л.Ф. Черногор – Харьков: Харьковский национальный университет имени В.Н. Каразина, 2012. – 556 с.

41. Тютюник В.В. Системний підхід до оцінки небезпеки життєдіяльності при територіально часовому розподілі енергії джерел надзвичайних ситуацій / В.В. Тютюник, Л.Ф. Чорногор, В.Д. Калугін // Проблеми надзвичайних ситуацій. – Харків: Національний університет цивільного захисту України, 2011. – Вип. 14. – С. 171 – 194.

42. Тютюник В.В. Дослідження умов раннього моніторингу та попередження надзвичайних ситуацій природного та техногенного характеру: звіт про НДР (№ держреєстрації 0112U002587) / керівник роботи: В.В. Тютюник; виконавці: В.Д. Калугін, Б.Б. Поспєлов, Р.І. Шевченко, М.В. Кустов, С.С. Говалєнков – Харків: Національний університет цивільного захисту України, 2014. – 266 с.

43. Тютюник В.В. Системний підхід до оцінки динаміки прояву надзвичайних ситуацій на території України / В.В. Тютюник, В.Д. Калугін // Проблеми надзвичайних ситуацій. – Харків: Національний університет цивільного захисту України, 2015. – Вип. 22. – С. 137 – 149.

44. Тютюник В.В. Моделирование энергетических зон суммарного риска от стационарных потенциально опасных объектов / В.В. Тютюник, А.В. Попова,

А.Н. Соболь, В.Д. Калугин, Е.А. Сушко // Научный вестник Воронежского государственного архитектурно-строительного университета. Строительство и архитектура. – Воронеж: Воронежский государственный архитектурно-строительный университет, 2014. – Вып. 1(33). – С. 159 – 166.

45. Тютюник В.В. Моделирование процесса формирования энергетических зон суммарного риска от стационарных и подвижных потенциально опасных объектов / В.В. Тютюник, Ю.С. Чапля, А.Н. Соболь, В.Д. Калугин, Е.А. Сушко // Фундаментальные исследования. – Москва: Академия естествознания, 2014. – № 11. – Ч. 4. – С. 799 – 803.

46. Тютюник В.В. Оценка уровня техногенной опасности территории по основным показателям жизнедеятельности методами факторного анализа и анализа главных компонент / В.В. Тютюник, Н.В. Бондарев, Р.И. Шевченко, Л.Ф. Черногор, В.Д. Калугин // Научные и образовательные проблемы гражданской защиты. – Химки: Академия гражданской защиты МЧС РФ, 2014. – № 3(22). – С. 47 – 57.

47. Тютюник В.В. Кластерный анализ территории Украины по основным показателям повседневного функционирования и проявления техногенной опасности / В.В. Тютюник, Н.В. Бондарев, Р.И. Шевченко, Л.Ф. Черногор, В.Д. Калугин // Геоінформатика. – Київ: Інститут геологічних наук НАН України, 2014. – 4(52). – С. 63 – 72.

48. Тютюник В.В. Оцінка відносної інтенсивності між надзвичайними ситуаціями природного та техногенного характеру в регіонах України / В.В. Тютюник // Проблеми надзвичайних ситуацій. – Харків: Національний університет цивільного захисту України, 2015. – Вип. 21. – С. 112 – 120.

49. Калугін В.Д. Системний підхід до оцінки ризиків надзвичайних ситуацій в Україні / В.Д. Калугін, В.В. Тютюник, Л.Ф. Чорногор, Р.І. Шевченко // Восточно-Европейский журнал передовых технологий. – 2012. – 1/6 (55). – С. 59 – 70.

50. Черногор Л.Ф. О нелинейности в природе и науке / Л.Ф. Черногор. – Харьков: Харьковский национальный университет имени В.Н. Каразина, 2008. – 528 с.

51. Абрамов Ю.А. Взаимосвязь инициирующих и поражающих факторов чрезвычайных ситуаций природного характера на территории Украины / Ю.А. Абрамов, В.В. Тютюник, Р.И. Шевченко // Проблеми надзвичайних ситуацій. – Харків: Університет цивільного захисту України. – 2007. – № 5. – С. 8–17.

52. Андронов В.А. Природні та техногенні загрози, оцінювання небезпек / В.А. Андронов, А.С. Рогозін, О.М. Соболь, В.В. Тютюник, Р.І. Шевченко – Харків: Національний університет цивільного захисту України, 2011. – 264 с.

53. Топольский Н.Г. Потенциальная опасность массового поражения при крупных техногенных авариях / Н.Г. Топольский, Н.П. Блудчий. – М.: ВИПТШ МВД России, 1994. – 75 с.

54. Серебровский А.Н. Об оценках ситуаций на потенциально опасных объектах на этапе превентивного мониторинга / А.Н. Серебровский // Мат. машини і системи. – 2000. – № 1. – С. 57–64.

55. Брушлинский Н.Н. Снова о рисках и управлении безопасностью / Н.Н. Брушлинский // ВИНИТИ. Пробл. безоп. при чрезв. ситуациях. – 2002. – Вып. 4. – С. 230–234.

56. Белов П.Г. Системный анализ и моделирование опасных процессов в техносфере / П.Г. Белов. – М.: Академия, 2003. – 506 с.

57. Короленко Ц.П. Психология человека в экстремальных условиях / Ц.П. Короленко. – М.: Медицина, 1978. – 178 с.

58. Александровский Ю.А. Психогении в экстремальных условиях / Ю.А. Александровский, О.С. Лобастов, Л.И. Спивак, Б.П. Щукин. – М.: Медицина, 1991. – 96 с.

59. Євсюков О.П. Психологічне прогнозування надійності діяльності працівників аварійно-рятувальних підрозділів МНС України / О.П. Євсюков, О.В. Тімченко. – Харків: Університет цивільного захисту України, 2007. – 288 с.

60. Моляко В.А. Особенности проявления паники в условиях экологического бедствия (на примере Чернобыльской атомной катастрофы) / В.А. Моляко // Психологический журнал. – 1992. – № 2. – С. 66–74.

61. Грубов В.М. Європейська колективна безпека в умовах глобалізації: ліберальна парадигма: монографія / В.М. Грубов. – Київ: Тов. «ФАДА, ЛТД», 2007. – 554 с.

62. Баймуратов М.О. Міжнародно-правові аспекти становлення і розвитку європейської безпеки на порозі XXI століття: монографія (рос. мовою) / М.О. Баймуратов, О.А. Делінський. – Одеса: Юридична література, 2004. – 184 с.

63. Бодрук О.С. Структури воєнної безпеки: національний та міжнародний аспекти: монографія / О.С. Бодрук. – Київ: Національний інститут проблем міжнародної безпеки, 2001. – 300 с.

64. Тютюник В.В. Основоположні принципи створення у Єдиній державній системі цивільного захисту інформаційно-аналітичної підсистеми управління процесами попередження й локалізації наслідків надзвичайних ситуацій / В.В. Тютюник, В.Д. Калугін, О.О. Писклакова // Системи управління, навігації та зв'язку. – Полтава: Полтавський національний технічний університет імені Юрія Кондратюка, 2018. – Вип. 4(50). – С. 168 – 177.

65. Тютюник В.В. Оцінка умов створення у Єдиній державній системі цивільного захисту інформаційно-аналітичної підсистеми управління процесами попередження й локалізації наслідків надзвичайних ситуацій на основі аналізу динаміки прояву небезпек на території України / В.В. Тютюник, В.Д. Калугін, О.О. Писклакова // Комунальне господарство міст. – Харків: Харківський національний університет міського господарства імені О.М. Бекетова, 2019. – т. 1. – №147. – С. 66 – 82.

66. Постанова кабінету міністрів України від 19.06.2019 р. № 518 Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури.

67. Козлова О.Ю., Кононович В.Г., Кононович І.В., Романюков М.Г., Тимошенко Л.М. Динамічні властивості процесів забезпечення кібербезпеки на прикладі аудиту кібербезпеки. Інформатика та математичні методи в моделюванні. 2017, Том 7, №3, С. 205–212.

68. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. СПб.: БХВ-Петербург, 2003, 752 с.

69. Ярочкин В.И. Система безопасности фирмы. М.: Ось-89, 2003, 352 с.

70. Андронов В.А., Дівізінюк М.М., Калугін В.Д., Тютюник В.В. Науково-конструкторські основи створення комплексної системи моніторингу надзвичайних ситуацій в Україні: Монографія. Харків: Національний університет цивільного захисту України, 2016, 319 с.

71. Тютюник В.В., Шевченко Р.І. Принцип комплектування технічними засобами складової «інформаційна безпека» інтегральної системи безпеки за критерієм «ефективність–інтегральна ціна». Системи озброєння і військова техніка. Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2009, №2(18), С. 159–165.

72. Заболотний В.І., Задорожна Є.В. Обґрунтування вибору заходів захисту характеристик продукції від конкурентної розвідки. Прикладная радиоэлектроника. Харків: Харківський національний університет радіоелетроніки, 2013, Том12, №2, С. 351–355.

73. Гражданкин А.И., Белов П.Г. Экспертная система оценки техногенного риска опасных производственных объектов. Безопасность труда в промышленности. 2000, №11, С. 6–10.

74. Райншке К., Ушаков И.А. Оценка надежности систем с использованием графов. Москва: Радио и связь, 1988, 180 с.

75. Журин С., Цветков Т. Учет и анализ рисков. Безопасность, достоверность, информация. 2004, №1(52), С. 40–43.

76. Вишняков Я.Д., Радаев Н.Н. Общая теория рисков. Москва: Издательский центр «Академия», 2008, 368 с.

77. Брушлинский Н. Н. Снова о рисках и управлении безопасностью. Проблемы безопасности и чрезвычайных ситуаций. Москва: ВИНИТИ РАН, 2002, №4, С. 230–234.

78. Хакен Г. Синергетика. Москва: Изд. «Мир», 1980, 414 с.

79. Курдюмов С.П., Малинецкий Г.Г. Синергетика и системный синтез. Новое в синергетике: взгляд в третье тысячелетие. Москва: Наука, 2002, 180 с.

80. Малинецкий Г.Г. Математические основы синергетики: Хаос, структуры, вычислительный эксперимент. Москва: Книжный дом «ЛИБРОКОМ», 2012, 312 с.

81. Про боротьбу з тероризмом: Закон України від 20 березня 2003 року № 638-IV [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/638-15

82. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2341-14#n1707

83. Авдеев Ю.И. Терроризм как социально-политическое явление / Ю.И. Авдеев; под ред. Е.И. Степанова. – М.: Культура, 1997. – 423 с.

84. Заявление «Группы восьми» об укреплении программы ООН по борьбе с терроризмом [Электронный ресурс]. – Режим доступа: http://www.krernlm.rn/mterdocs/2006/07/16/2037

85. Доклад Министерства обороны США 1997 г. об антитеррористической деятельности. Responding of Defense's 1997. Annual Defense Report [Электронный ресурс]. – Режим доступа: http://www.terrorism.com/terrorism/Responding. shtml

86. Доклад Генерального секретаря Кофи Аннана от 3 мая 2006 г. «Единство в борьбе с терроризмом: рекомендации по глобальной контртеррористической стратегии». – Режим доступа: http://www.un.org/russian/unitingagainstterrorism/report.html

87. Грачев С.И. Терроризм. Вопросы теории: монография. – Н. Новгород: Изд-во ННГУ им. Н.И. Лобачевского, 2007. – 269 с.

88. Васильев Н.Т. Биологический терроризм: прошлое, настоящее, будущее / Н.Т. Васильев, М.Ю. Тарасов, Д.Л. Поклонский // Химическая и биологическая безопасность. – 2002. – № 6. – С. 3 – 10.

89. Татаринов В.В. Радиационный, химический и биологический терроризм / В.В. Татаринов // Интернет-журнал "Технологии техносферной безопасности" – 2012. – Вып. 3 (43) [Электронный ресурс]. – Режим доступа: http://ipb.mos.ru/ttb

90. Антипенко В.Ф. Борьба с современным терроризмом: междунар.-правовые подходы / В.Ф. Антипенко – Институт государства и права им. В.М. Корецкого. – Киев: Юнона-М, 2002 – 722 с.

91. Tucker J.B. Historical trends related to bioterrorism: an empirical analysis / J.B. Tucker // Emerg. Infec. Disease – 1999. – V.5 – № 4. – P. 498 – 504.

92. Иванов Е.Н. Расчет и проектирование систем противопожарной защиты / Е.Н. Иванов. – М.: Химия, 1990. – 384 с.

93. Христич В.В. Системи пожежної та охоронної сигналізації / В.В. Христич, О.А. Дерев'янко, С.М. Бондаренко, О.А. Антошків. – Харків: Академія пожежної безпеки України. [Електронний ресурс]. – Режим доступу: http://univer.nuczu.edu.ua/tmp_metod/297/Signal.pdf

94. Автоматизовані системи управління та зв'язок у сфері цивільного захисту: Навчальний посібник / І.А. Чуб, В.Є. Пустоваров, Г.Е. Винокуров, П.М. Бортничук, Л.А. Клименко; за заг. ред. Г.В. Щербака. – Харків: Академія цивільного захисту України, 2005. – 272 с

95. Деревянко А.А. Применение и эксплуатация приборов пожарной автоматики / А.А. Деревянко, А.А. Антошкин, С.Н. Бондаренко, В.А. Дуреев, М.Н. Мурин. – Харьков: Университет гражданской защиты Украины, 2007. – 205 с.

96. Дерев'янко О.А. Автоматичний протипожежний захист об'єктів / О.А. Дерев'янко, В.В. Христич, С.М. Бондаренко, М.М. Мурін, О.А. Антошків. – Харків: Національний університет цивільного захисту України, 2014. – 282 с.

97. Членов А.Н. Автоматические пожарные извещатели / А.Н. Членов. – М.: НИЦ «Охрана» ВНИИПО МВД России, 1997. – 51 с.

98. Извещатели пожарные дымовые оптико-электронные линейные. Общие технические требования. Методы испытаний: НПБ 82-99. – М., 1999. [Электронный ресурс]. – Режим доступа: http://files.stroyinf.ru/Data2/1/4294847/4294847692.pdf

99. Извещатели пожарные дымовые радиоизотопные. Общие технические требования. Методы испытаний: НПБ 81-99. – М., 2000. [Электронный ресурс]. – Режим доступа:

http://ohranatruda.ru/ot_biblio//normativ/data_normativ/7/7693/index.php

100. Извещатели пожарные тепловые. Технические требования пожарной безопасности. Методы испытаний: НПБ 85-2000. – М., 2001. [Электронный ресурс]. – Режим доступа: http://www.ohranatruda.ru/ot_biblio/normativ/data_normativ/8/8923/

101. Левтеров А.А. Использование эффекта акустической эмиссии при раннем обнаружении возгорания целлюлозосодержащих материалов объектовой подсистемой универсальной системы мониторинга чрезвычайных ситуаций в Украине / А.А. Левтеров, В.В. Тютюник, В.Д. Калугин, С.В. Ольховиков // Прикладная радиоэлектроника. – 2017. – Т.16. – № 1-2. – С. 23 – 40.

102. Абдурагимов И.М. Физико-химические основы развития и тушения пожаров / И.М. Абдурагимов, В.Ю. Говоров, В.Е. Макаров. – М.: ВИПТШ МВД СССР, 1980. – 255 с.

103. Померанцев В.В. Основы практической теории горения / В.В. Померанцев. – Л.: Энергоатомиздат, 1986. – 312 с.

104. Пожаровзрывоопасность веществ и материалов и средства их тушения. Справочник. Книга 1 – 2. Под ред. Баратова А.Н. и Корольченка А.Я. – М.: Химия, 1990. – 495 с. + 384 с.

105. Киселев Я.С. Физические модели горения в системе предупреждения пожаров / Я.С. Киселев. – С.-П.: СПУ МВД России, 2000. – 264 с.

106. Єлагін Г.І. Основи теорії розвитку і припинення горіння / Г.І. Єлагін, М.Г. Шкарабура, М.А. Кришталь, О.М. Тищенко. – Черкаси: Черкаський інститут пожежної безпеки, 2001. – 448 с.

107. Тарахно О.В. Теоретичні основи пожежовибухонебезпеки / О.В. Тарахно. – Харків: Академія цивільного захисту України, 2006. – 395 с.

108. Корольченко А.Я. Процессы горения и взрыва / А.Я. Корольченко. – М.: Пожнаука, 2007. – 266 с.

109. Кусковець С.Л. Основи теорії горіння та вибуху / С.Л. Кусковець, О.С. Шаталов, В.О. Турченюк. – Рівне: Національний університет водного господарства та природокористування, 2012. – 374 с.

110. Грешников В.А. Акустическая эмиссия / В.А. Грешников, Ю.Б. Дробот. – М.: Изд-во стандартов, 1976. – 276 с.

111. Eitzen D.G. Acoustic Emission: Establishing the Fundamentals / D.G. Eitzen, H.N.G. Wadley // JOURNAL OF RESEARCH of the National Bureau of Standards. – 1984. – Vol. 89. – № 1. – January-February. – P. 75 – 100.

112. Grosshandler W.L. Acoustic Emission of Structural Materials Exposed to Open Flames / W.L. Grosshandler, M. Jackson // Fire Safety Journal. – 1994. – Vol. 22. – P. 209 – 228.

113. Членов А.Н. Ультразвуковые охранные и охранно-пожарные извещатели для закрытых помещений / А.Н. Членов // Системы безопасности, связи и телекоммуникаций, март-апрель, – М., 1999. – С. 25 – 27.

114. Пузач С.В. Обоснование возможности раннего обнаружения возгорания в помещении с помощью датчиков давления / Пузач С.В., Поляков Ю.А. // Проблемы безопасности при чрезвычайных ситуациях. – 1999. – Вып. 3. – С. 53 – 56.

115. Асминг В.Э. Анализ инфразвуковых сигналов, генерируемых техногенными источниками / В.Э. Асминг, З.А. Евтюгина, Ю.А. Виноградов, А.В. Федоров // Вестник МГТУ. – 2009. – т. 12. – № 2. – С. 300 – 307.

116. Климчук Е.Г. Акустическая диагностика процессов «твердофазного горения» смесей органических кристаллов / Е.Г. Климчук, А.Л. Парахонский // Ученые записки физического факультета. – 2014. – № 6. – С. 146322-1 – 146322-5.

117. Беликов В.Т. Использование результатов наблюдений акустической эмиссии для изучения структурных характеристик твердого тела / В.Т. Беликов, Д.Г. Рывкин // Акустический журнал. – 2015. – т. 61. – № 5. – С. 622 – 630.

118. Смирнов А.Н. Генерация акустических колебаний в химических реакциях и физико-химических процессах / А.Н. Смирнов // Российский химический журнал. – 2001. – т. XLV. – № 1. – С. 29 – 34.

119. Роменский А.В. Ультразвук в гетерогенном катализе / А.В. Роменский, В.В. Казаков, Г.И. Гринь, А.П. Кунченко, И.В. Волохов, А.Я. Лобойко. – Северодонецк: Северодонецкая городская типография, 2006. – 289 с.

120. Кузнецов Д.М. Акустическая эмиссия при фазовых превращениях в водной среде / Д.М. Кузнецов, А.Н. Смирнов, А.В. Сыроешкин // Российский химический журнал. – 2008. – т. LII. – № 1. – С. 114 – 121.

121. Дорофеев Б.М. Влияние статического давления на звуковые импульсы, генерируемые пузырьками пара при насыщенном кипении / Б.М. Дорофеев, В.И. Волкова // Акустический журнал. – 2011. – т. 57. – № 6. – С. 778 – 785.

122. Фадеев Г.Н. Акустическая резонансная частота химических реакций / Г.Н. Фадеев, В.С. Болдырев, Н.Н. Кузнецов // Инженерный журнал: наука и инновации. – 2013. – Вып. 6. [Электронный ресурс]. – Режим доступа: http://engjournal.ru/catalog/fundamentals/chem/787.html

123. Иванов Н.И. Инженерная акустика. Теория и практика борьбы с шумами / Н.И. Иванов. – М.: Университетская книга, Логос, 2008. – 424 с.

124. Справочник проектировщика. Защита от шума в градостроительстве. Под ред. Г.Л. Осипова. – М.: Стройиздат, 1993.

125. Zaporozhets O. Aircraft noise modelling for environmental assessment around airports / O. Zaporozhets, V. Tokarev // Applied Accoustics. – 1998. – V.55. – No2. – P. 99 – 127.

126. Левтеров А.А. Использование эффекта акустической эмиссии при раннем обнаружении возгорания целлюлозосодержащих материалов объектовой подсистемой универсальной системы мониторинга чрезвычайных ситуаций в Украине / А.А. Левтеров, В.В. Тютюник, В.Д. Калугин, С.В. Ольховиков // Прикладная радиоэлектроника. – 2017. – Т.16. – № 1-2. – С. 23 – 40.

127. Левтеров А.А. Методы идентификации процесса горения целлюлозосодержащих материалов на основе эффекта акустической эмиссии / А.А. Левтеров, В.В. Тютюник, В.Д. Калугин // Проблемы пожарной безопасности. – 2017. – Вып. 42. – С. 72 – 84.

128. Пат. 127254 Україна, МПК (2006) A62C 3/00, G01R 29/26 (2006.01), G08C 19/00, G08B 31/00. Спосіб раннього виявлення осередку займання / О.А. Левтеров, В.Д. Калугін, В.В. Тютюник. Власник патенту: Національний університет цивільного захисту України. – № u201801387; заявл. 12.02.2018; опубл. 25.07.2018, бюл. № 14.

129. Федер Е. Фракталы / М.: Мир, 1991. – 258 с.

130. Мачехин Ю. Фрактальная шкала для временных рядов результатов измерений / Ю. Мачехин // Измерительная техника. – 2008. – Вып. 08. – С. 40–43.

131. Зорич В.А. Математический анализ. В 2-хЧастях. – Изд. 4-е, испр. – М.: МЦНМО, 2002.

132. Фрактальный анализ процессов, структур и сигналов. Коллективная монография / Под ред. Р.Э. Пащенко.– Харьков.– ХООО «НЭО «Эко Перспктива», 2006.– 348с.

133. Кроновер Р. М. Фракталы и хаос в динамических системах. Основы теории / пер. с английского / М.: Постмаркер, 2000. — 352 с.

134. Mandelbrot B. B. The Fractal Geometry of Nature / San Francisco: Freeman, 1982. – 491 p.

135. Герасименко О.І., Рахманов В.О. Вогнева підготовка. – Київ: НАУ, 2007. – 118 с.

136. Глущенко В.Ф., Безносюк Л.В., Колоколов А.О. та ін. Вогнева підготовка. – Вінниця: «ДТП», 1998. – 160 с.

137. Ляпа М.М., Петренко В.М., Судніков О.І. та ін. Вогнева підготовка. – Суми: Сумський державний університет, 2011. – 283 с.

138. Тютюник В.В. Оцінка ефективності покриття території надзвичайної ситуації за допомогою автоматизованих пристроїв контролю небезпечних факторів при їх розкиданні із зависаючого над точкою скидання безпілотного літального апарату / В.В. Тютюник, В.Д. Калугін, Г.В. Іванець, М.Г. Іванець, Ю.В. Захарченко // Техногенно-екологічна безпека та цивільний захист. – Київ: Інститут геохімії навколишнього середовища НАН України, 2016. – Вип. 10. – С. 34 – 43.

139. Іванець Г.В. Алгоритм оцінки ефективності покриття території надзвичайної ситуації автоматизованими пристроями контролю небезпечних факторів при їх розкиданні з безпілотного літального апарату в умовах нестабільностей повітряного середовища / Г.В. Іванець, В.В. Тютюник, В.Д. Калугін, Б.Б. Поспєлов, Ю.В. Захарченко // Проблеми надзвичайних ситуацій. – Харків: Національний університет цивільного захисту України, 2017. – Вип. 25. – С. 45 – 56.

140. Пат. 105339 Україна, МПК(2016.01) B64D1/08 (2006.01), G08B19/00, G08B25/00, G08B26/00. Пристрій для скидання автоматизованих засобів контролю факторів небезпеки та вантажів для постраждалих з безпілотного літального апарату / Андронов В.А., Калугін В.Д., Тютюник В.В., Тютюник (Захарченко) Ю.В; Власник патенту: Національний університет цивільного захисту України. – № u201510075; заявл. 15.10.2015; опубл. 10.03.2016, бюл. № 5.

141. Пат. 114393 Україна, МПК(2017.01) B64D1/02 (2006.01), G08B19/00, G08B17/00, G08B21/00. Пристрій для скидання автоматизованих засобів контролю небезпечних факторів надзвичайних ситуацій з безпілотного літального апарату / Андронов В.А., Калугін В.Д., Лєвтєров О.А., Тютюник В.В., Тютюник (Захарченко) Ю.В; Власник патенту: Національний університет цивільного захисту України. – № u201608736; заявл. 11.08.2016; опубл. 10.03.2017, бюл. № 5.

142. Тютюник В.В., Калугін В.Д., Заболотний В.І., Писклакова О.О. Розвиток науково-технічних основ оперативного моніторингу кіберпростору навколо об’єктів кіберзахисту за допомогою безпілотних літальних апаратів. Збірник тез науково-практичної конференції «Проблеми теорії та практики інформаційного протиборства в мовах ведення гібридних війн», МОУ ЖВІ ім. С.П. Корольова. 24-25 жовтня 2019 р.: – 2019. – С. 288-292.