# Шляхи підвищення ефективності систем фізичного захисту об'єктів критичної інфраструктури держави, що охороняються

**Олена Азаренко * [1 A] Юлія Гончаренко [2 B]; Михайло Дівізінюк [3 C]; Володимир Мірненко [4 D]; Валерій Стрілець [5 A]**

[A] Науково-дослідний лабораторно-експериментальний центр "БРАНД ТРЕЙД", м. Київ, Україна
[B] Європейський університет, м. Київ, Україна
[C] Інститут геохімії та навколишнього середовища НАН України, м. Київ, Україна
[D] Департамент військової освіти та науки Міністерства оборони України, м. Київ, Україна

**Received:** August 15, 2021 | Revised: August 24, 2021 | Accepted: August 31, 2021

**DOI:** 10.33445/sds.2021.11.4.18

***Анотація***

Стаття присвячена визначенню нових напрямків підвищення ефективності систем фізичного захисту об'єктів критичної інфраструктури, що охороняються, які є головним технічним засобом недопущення терористичних актів проти цих об'єктів. Спочатку дано характеристика систем охорони приміщень і контролю прилеглих територій об'єктів критичної інфраструктури, що охороняються. Показано, що за функціональним призначенням в систему фізичного захисту входять пристрої та системи сигналізації виявлення, збору і обробки інформації, тривожно викличної сигналізації, контролю і управління доступом, оптоелектронного спостереження, оперативного зв'язку та оповіщення, забезпечення електроживлення і електроосвітлення, системи забезпечення фізичного захисту ядерних матеріалів при транспортуванні. Вони розподіляються по трьох зонах: внутрішньої, охоронюваному периметру і зовнішньої (санітарній) зоні. Головним засобом збору інформації про обстановку на периметрі і підходах до нього є оптоелектронні засоби. Потім розглянути особливості процесу управління надзвичайної ситуацій терористичного характеру на об'єкті критичної інфраструктури, що охороняється. Показано, що головна мета управління надзвичайними ситуаціями терористичного характеру – це недопущення терористичного акту на об'єкті, що охороняється, який є об'єктом управління. Структурно-логічна модель управління надзвичайною ситуацію складається з шести блоків: блоку моніторингу ситуації; блоку виявлення ризику; блоку аналізу ризиків; блоку підготовки варіантів управлінських рішень; блоку прийняття рішення і доведення його виконавців; блоку впливу на ситуацію, яка через структуру виконавців впливає на об'єкт управління і замикає його контур управління, забезпечуючи тим самим безперервність процесу управління надзвичайною ситуацією терористичного характеру в інтересах її недопущення та запобігання. Після чого визначити шляхи підвищення ефективності систем фізичного захисту об'єктів критичної інфраструктури держави, що охороняються. Показано, що одним з перспективних напрямків підвищення ефективності процесу управління надзвичайною ситуацією терористичного характеру на об'єктах критичної інфраструктури держави, що охороняються є вдосконалення систем фізичного захисту шляхом розробки нових пристроїв і систем акустичного контролю приміщень і територій об'єкта і знімання мовної інформації з використанням параболічних, трубчастих і градієнтних мікрофонів і плоских акустичних фразованих решіток, які

[1] * **Corresponding author:** д.ф.-м.н., професор, заступник керівника, e-mail: azarenko_ev@ukr.net, ORCID: 0000-0003-2927-5545
[2] к.т.н., доцент, професор кафедри, e-mail: vup@e-u.in.ua, ORCID: 0000-0003-2045-0263
[3] д.ф-м., професор, головний науковий співробітник, e-mail: divizinyuk@ukr.net, ORCID: 0000-0002-5657-2302
[4] д.т.н., професор, Заслужений працівник освіти України, директор, e-mail: mirnenkovi@gmail.com, ORCID: 0000-0002-7484-1035
[5] керівник, e-mail: v.strelec.brand@gmail.com, ORCID: 0000-0003-1913-7878

забезпечують прийом акустичних сигналів на видаленні від ніс кількох десятків до кількох сотень метрів і забезпечують повну інформацію про дії та наміри людей, що реєструються в відео системах.

***Ключові слова:*** надзвичайна ситуація, терористичного акт, система фізичного захисту, акустичний контроль, спрямований мікрофон.

## Постановка проблеми

Головна мета управління надзвичайними ситуаціями (НС) терористичного характеру (ТХ) – це недопущення терористичного акту на об'єкті, що охороняється [1-3]. Одним із напрямів протидії терору, тобто недопущення терористичних актів, є оперативно-розшукова діяльність, що визначається законом України "Про оперативно-розшукову діяльність" (ОРД) [4]. Основним завданням ОРД є збір інформації, що неможливо одержати легальним (офіційним) шляхом, внаслідок чого необхідну секретну інформацію одержують неофіційним (нелегальним) шляхом. Строго говорячи, ОРД – це система гласних і негласних пошукових, розвідувальних і контр розвідувальних заходів, які здійснюються із застосуванням розвідувальних і оперативно-технічних засобів [3-7].

Основними завданнями оперативно-розшукової діяльності є пошук і фіксація фактичних даних про протиправні дії окремих осіб і груп, відповідальність за які передбачена Кримінальним кодексом України, виявлення ознак розвідувально-підривної діяльності спеціальних служб іноземних держав і різних організацій з метою припинення правопорушень, а також одержання інформації із забезпечення безпеки громадян та держави в цілому.

Знімання мовної інформації є однією з форм оперативно-розшукової діяльності, яка дозволяє визначити наявність та ідентифікувати склад злочинних груп, їхні задуми, плани реалізації намірів, а також уточнити множина інших аспектів оперативної обстановки [8-12]. Усе вище зазначене визначає активний цілеспрямований процес збору інформації.

## Постановка завдання

На відміну від нього акустичний контроль – це пасивний процес панорамного прийому акустичних сигналів і шумів з їх подальшим оперативним аналізом для вирішення певного кола прикладних завдань [13-20]. З погляду запобігання надзвичайним ситуаціям терористичного характеру на об'єктах критичної інфраструктури, що охороняються, між ними можна поставити знак рівності.

Мета даної роботи полягає у визначенні нових напрямків підвищення ефективності систем фізичного захисту об'єктів критичної інфраструктури, що охороняються, які є головним технічним засобом недопущення терористичних актів проти цих об'єктів.

Для досягнення поставленої мети необхідно вирішити наступні наукові завдання.

Спочатку дати характеристику систем охорони приміщень і контролю прилеглих територій об'єктів критичної інфраструктури, що охороняються. Потім розглянути особливості процесу управління надзвичайної ситуацій терористичного характеру на об'єкті критичної інфраструктури, що охороняється. Після чого визначити шляхи підвищення ефективності систем фізичного захисту об'єктів критичної інфраструктури держави, що охороняються.

## Виклад основного матеріалу

**Характеристика систем охорони приміщень і контролю прилеглих територій об'єктів критичної інфраструктури, що охороняються**

За функціональним призначенням в систему фізичного захисту входять пристрої та системи сигналізації виявлення, збору і обробки інформації, тривожно викличної

сигналізації, контролю і управління доступом, оптоелектронного спостереження, оперативного зв'язку та оповіщення, забезпечення електроживлення і електроосвітлення, системи забезпечення фізичного захисту ядерних матеріалів при транспортуванні [14].

Засоби сигналізації поділяються на технічні засоби охоронної, пожежної і тривожної сигналізації [2, 3, 17]. На ряді об'єктів охоронна і пожежна сигналізація з економічних міркувань об'єднуються в одну – пожежно-охоронну сигналізацію, яка призначена як для видачі сигналів тривоги при спробах проникнення, так і для сигналізації при виникненні пожеж. Це можуть бути пожежні центри типу Артон, Тирос, Кристал або охоронні централі типу Оріон, DSC, Інтеграл. До складу цих систем входять засоби виявлення (датчики), засоби передачі інформації (канали зв'язку), засоби прийому та обробки інформації, джерела світлових і звукових сигналів. За принципом дії датчики поділяються на електромеханічні, теплові, ємнісні, ультразвукові, оптико-електронні, мікрохвильові. Сполучені датчики утворюють електричний ланцюг, звану шлейфом блокування, при порушенні якої видається сигнал тривоги.

Системи збору і обробки інформації [1, 10, 15] виконують функції інтеграції всіх інженерно-технічних засобів охорони в єдиний комплекс, що дозволяє мати актуальну інформацію про стан об'єктів і оперативно реагувати на негативні події. До них відносяться XVmatic, Кодос та ін.

Тривожно-виклична сигналізація призначена для виклику оперативної групи.

Система контролю і управління доступом – сукупність апаратно-програмних засобів безпеки, призначених для обмеження і реєстрації виходу – входу людей і транспорту на заданій території через пункти переходу. Прикладами типових систем можуть бути зразки типу Anviz BL-300 та ін.

Системи оптоелектронного спостереження і оцінки обстановки в загальному випадку являють систему телевізійного спостереження замкнутого периметра [3, 9, 16, 17], які регулюють процес візуального контролю з використанням оптико-електронних пристроїв, в тому числі і інфрачервоних, а також автоматичного аналізу зображень (розпізнавання осіб, номерів машин та ін.). Вони також дають можливість вести спостереження за об'єктом на будь-яких відстанях, переглядати архів подій, що відбуваються раніше. Розрізняють системи зовнішнього і внутрішнього використання. Як засоби, вони мають різну ступінь захищеності від впливу природних факторів.

Засоби зв'язку та оповіщення повинні забезпечувати стійкий зв'язок і можливість управління в критичних ситуаціях, що виникають на об'єктах. Найбільш оперативної вважається стільниковий зв'язок, яка за відносно нетривалий проміжок часу дозволяє оповістити досить велика кількість працівників. При цьому необхідною умовою безвідмовності роботи оповіщення є дублювання оповіщення телефонним зв'язком. Для функціонування всіх служб фізичного захисту необхідно мати не тільки стільникові телефони, а й переносні радіостанції різного діапазону, як правило, від 120 до 160 МГц.

Засоби електроживлення та електро-освітлення є традиційними і для багатьох інших сфер діяльності, де пред'являються в якості основних вимог забезпечення надійності і безвідмовності роботи.

Системи забезпечення фізичного захисту ядерних матеріалів при транспортуванні представляють собою набір контейнерів різної форми і розмірів з відповідними засобами радіаційного контролю і попередження про розгерметизацію контейнера.

Особливість всіх розглянутих комплексів в системі фізичного захисту полягає в тому, що вони використовують акустичне поле тільки в датчиках, що забезпечують контроль приміщень від проникнення. У всіх інших засобах акустичне поле не використовується,

хоча первинне акустичне поле, створюване зловмисниками, дозволяє не тільки констатувати їх наміри, а й дізнатися, як вони збираються здійснювати задумане [3, 9, 13-15, 18-20].

У загальному випадку система фізичного захисту об'єктів критичної інфраструктури ділиться на три зони: внутрішня, огороджена периметром, сам периметр і зовнішня зона, що знаходиться за межами периметра. У ряді випадків законодавством передбачена спеціальна санітарна (контрольована) зона навколо об'єктів критичної інфраструктури, ширина яких становить до півтора *км*, а в деяких випадках і більше.

Система виявлення, яка приймається для контролю санітарної зони, оснащується телевізійними камерами візуального та інфрачервоного діапазону, що дозволяють завчасно виявити наближення порушників до охоронюваного периметру. Поблизу периметра використовуються електромагнітні та інші пристрої для виявлення зловмисників.

Типовою є екстремальна ситуація, коли на об'єкт критичної інфраструктури намагаються проникнути 1-2 людини. Події, що відбулися на Україні в останні роки, показують, що треба очікувати групи з 15-20 осіб і більше. У цьому випадку на перше місце виходять системи, які контролюють обстановку на підходах до об'єкта в санітарній зоні. У разі підходу групи порушників до периметру і прориву через нього викликані додаткові сили підтримки, які прибувають на допомогу охороні, можуть вже не знадобитися. Наближення таких груп, навіть потайне, можна виявити з використанням телевізійних і інфрачервоних систем. Але тут можлива ситуація, коли камери відео спостереження, навіть призначені для таємного спостереження, можуть бути досить швидко виявлені і наступними пострілами снайперів знищені. Однак в цьому випадку пропадає фактор раптовості. Можливий інший варіант – обстріляти оптику камер з пейнтбольних рушниць, снайперські зразки яких дозволяють прицільно стріляти на дистанцію 200-300 м. У цьому випадку "сліпі" камери не дозволяють завчасно виявити зловмисників, і вони потай підходять до охоронюваного периметру. Наявність пасивних акустичних пристроїв виявлення, контролюють санітарну зону, дозволило б ліквідувати цю діру в системі фізичного захисту.

Таким чином, системи охорони приміщень і контролю прилеглої території на потенційно небезпечних об'єктах, що охороняються розподіляються по трьох зонах: внутрішньої, охоронюваному периметру і зовнішньої (санітарній) зоні. Головним засобом збору інформації про обстановку на периметрі і підходах до нього є оптоелектронні засоби. Впровадження акустичних засобів контролю значно б підвищило інформативність охоронних систем і поліпшило б систему фізичного захисту об'єкта.

**Особливості процесу управління надзвичайної ситуацій терористичного характеру на об'єкті критичної інфраструктури, що охороняється**

Головна мета управління НС ТХ – це недопущення теракту на об'єкті критичної інфраструктурі, що охороняється, який з точки зору термінології теорії управління прийнято називати об'єктом управління. Виходячи зі специфіки розвитку НС ТХ, описаної вище, и особливо процесу управління НС в других областях, розроблено и використовується структурно-логічна модель управління надзвичайною ситуацією терористичного характеру на АЕС [1-3], яка представлена на рис. 1.

Ця модель містить шість структурних блоків, яким відповідають конкретні фази процесу управління.

Перший блок – блок моніторингу ситуації на об'єкті управління і навколо нього, в який входить:

- комплекс режимних заходів з контролю пропускного режиму при вході на об'єкт і виході з нього співробітників, контрагентів, керівників та інших відвідувачів;

- перевірка порядку в'їзду на об'єкт і виїзду з нього транспортних засобів, порядку

доставки та вивезення вантажів;

- спостереження за периметром об'єкта та прилеглої до нього санітарною зоною;

- здійснення кадрового контролю за співробітниками при прийомі їх на роботу, просуванні по службі, періодична перевірка, пов'язана з оформленням спеціальних допусків;

- оперативна робота в містах-супутниках об'єкта управління, вивчення публікацій, телерепортажів, інтернет – інформації про діяльність об'єкта управління, отримання конфіденційних відомостей від вищих державних структур (СБУ, МВС та ін.).

Кожному виду режимного заходу відповідає цілком певна організаційно технічна структура, яка позначається елементом системи моніторингу.

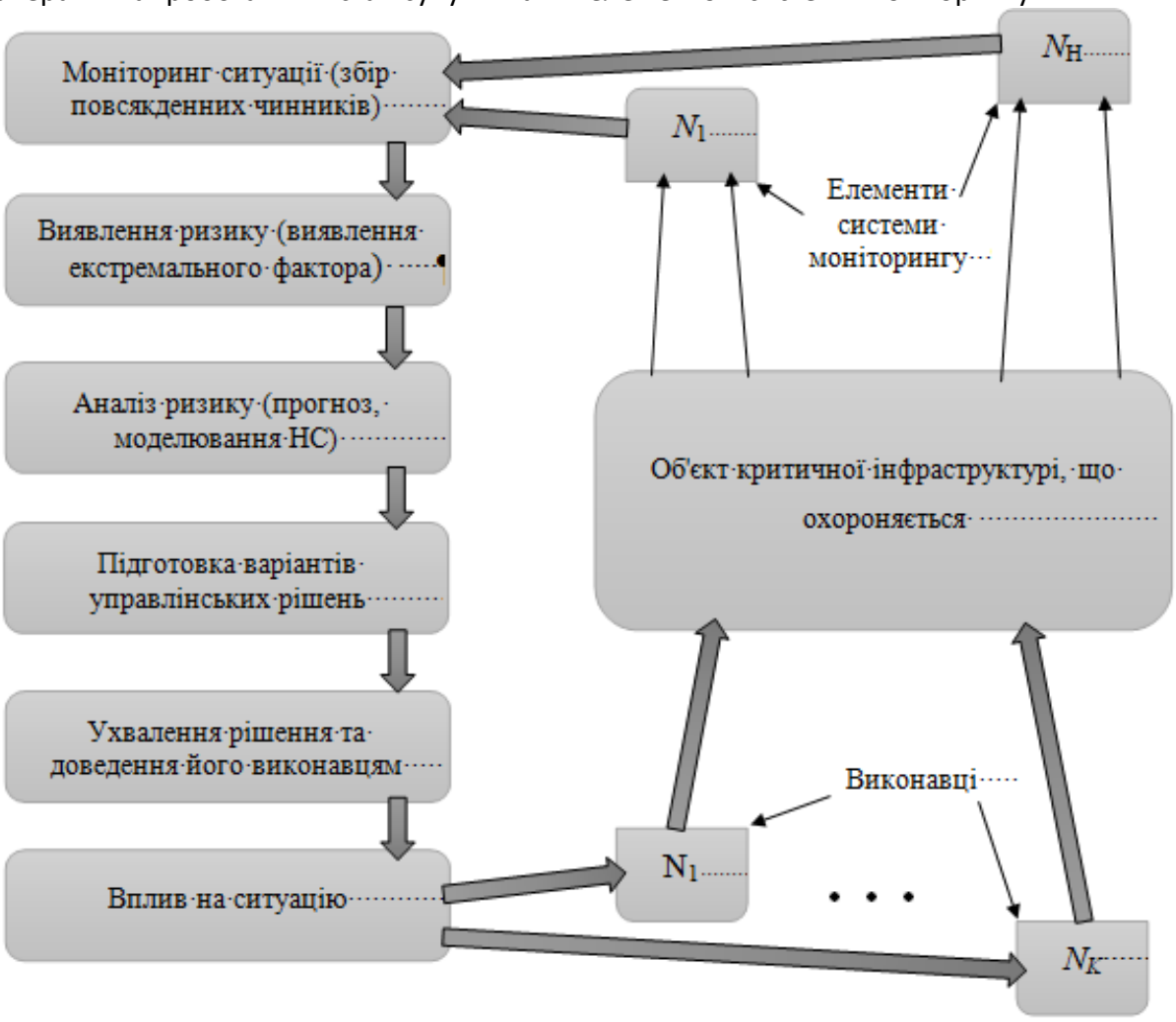


Рисунок 1 – Структурно-логічна модель управління надзвичайною ситуацією терористичного характеру на АЕС

Описаний блок системи управління призначений для постійного збору інформації про повсякденні фактори, які супроводжують функціонування об'єкта управління, і про працюючих на ньому працівників. Постійна систематизація отриманої інформації дозволяє виявити тенденцію до формування негативного фактора або виявити ознаки його можливого виникнення.

Другий блок спрямований на виявлення ризику виникнення НС, яке здійснюється шляхом скрупульозного аналізу і систематизації даних про стан об'єкта управління, отриманих від усіх можливих, навіть випадкових, джерел інформації.

До ознак ризику НС терористичного характеру можуть бути віднесені найрізноманітніші факти з повсякденних подій, що відносяться до розряду нетипових і підозрілих, що сприяють накопиченню негативного фактора. Їх виявлення залежить від професіоналізму і передбачливості відповідних посадових виконавців.

Наприклад, нещасний випадок, що стався з начальником варти позавідомчої охорони, сприяє кар'єрному росту його підлеглих, висунення яких по кадровим міркувань раніше взагалі не розглядалися, що сприяє призначенням на таку відповідальну посаду потрібного зловмисникам кандидата. Або в лісосмузі, припадають до санітарної зони об'єкта, впало дерево, що відповідно до інструкції вимагає огляду цього місця нарядом для з'ясування причин і можливих наслідків. Однак повторне падіння дерева вимагає вже детального розбору і осмислення, які характеристики системи ФЗ об'єкта при цьому розкриваються. Виявлення зрубів на стовбурі може означати, що цей випадок викликаний цілком умисними діями.

Третій блок структурно-логічної моделі управління НС служить для аналізу можливих ризиків, який в кінцевому підсумку зводиться до прогнозу і моделювання можливих сценаріїв розвитку надзвичайної ситуації.

Наприклад, в описаному вище випадку падіння дерев, що стався в результаті вирубки (планової, затвердженої лісгоспом, або несанкціонованої), нарядом проведена робоча перевірка і огляд місця події. В результаті гіпотетично можливі наступні варіанти розвитку подій. По-перше, створюється напружена обстановка у периметра, керівництво нервує і затримує вивезення радіоактивних відходів або відкладає своєчасну доставку ядерного палива. По-друге, таким чином привертається увага до дій на кордоні санітарної зони, а в цей час відбувається інцидент на транспортному пропускному пункті, і зловмисники таємно проникають на об'єкт. По-третє, падіння дерева використовується для стрільби з гранатометів по периметру з метою порушення його цілісності і забезпечення прориву виконавців теракту на об'єкт.

Наведені приклади показують, що аналіз покликаний змоделювати ряд можливих сценаріїв, серед яких можна виділити найкращий (перший) і найгірший (третій) в сенсі можливих наслідків. Між цими крайніми варіантами розглядається, як правило, не менше двох-трьох проміжних сценаріїв, при цьому враховується час року (зима, літо та ін.) гідрометеоумов (опади, туман, вітер та ін.), час доби і інші чинники, і робиться це зазвичай задовго до фактичного виникнення НС. Наявність в банку даних опрацьованих, тобто заздалегідь обдуманих сценаріїв, полегшує функціонування наступного блоку.

Четвертий блок здійснює підготовку варіантів управлінських рішень, які розробляються виходячи з наявних сил і засобів, а також відповідно до фактично складається обстановкою. Іноді розвиток форс-мажорній ситуації таке, що немає можливості його попередити або зупинити (третій з вищеописаних сценаріїв). Для таких випадків повинні розроблятися і пропонуватися варіанти профілактичних, превентивних заходів, спрямованих на запобігання такого роду катастрофічних подій. Наприклад, проводити профілактичний огляд підходів до санітарної зони, конкретизувати оперативну роботу на виявлення негативно налаштованих осіб (прихильників Грін-Писа, інших громадських організацій та ін.), Завчасно перейти на посилений варіант охорони об'єкта і залучити сили і засоби взаємодіючих підрозділів.

П'ятий блок структурно-логічної моделі управління НС відповідає за прийняття управлінського рішення і доведення його до виконавців за допомогою не тільки усну зв'язку, а й письмово у вигляді наказів, інструкцій, правил, настанов, а також у вигляді оперативних та інших планів. Він є ключовим етапом в управлінні надзвичайною

ситуацією терористичного характеру.

Шостий блок - це блок впливу на ситуацію відповідно до прийнятого рішення, яке здійснюють призначені виконавці, і, таким чином, замикається контур управління, чим забезпечується безперервність процесу управління НС терористичного характеру.

Отже, структурно-логічна модель управління НС складається з шести блоків:

- блоку моніторингу ситуації (збір повсякденних чинників);
- блоку виявлення ризику (виявлення екстремального фактора);
- блоку аналізу ризиків (прогноз і моделювання НС);
- блоку підготовки варіантів управлінських рішень;
- блоку прийняття рішення і доведення його виконавців;
- блоку впливу на ситуацію, яка через структуру виконавців впливає на об'єкт управління і замикає його контур управління, забезпечуючи тим самим безперервність процесу управління надзвичайною ситуацією терористичного характеру в інтересах її недопущення та запобігання.

Кожен з названих блоків, в свою чергу, може розглядатися як самостійний метод запобігання терористичного акту на об'єкті управління.

Таким чином, основним завданням управління надзвичайної ситуацію є зменшення ступеня небезпеки або загрози, одним з підходів до оцінки якої є концепція ризику. Тут під ризиком розуміють можливість настання подій з негативними наслідками, тобто можливість реалізації передбачуваної небезпеки. З такої точки зору ефективність управління надзвичайний ситуації оцінюється ступенем зменшення ймовірності настання негативних подій і (або) їх наслідків шляхом виконання певних заходів, які вимагають розумних витрат.

**Шляхи підвищення ефективності систем фізичного захисту об'єктів критичної інфраструктури держави, що охороняються**

Між процесом управління НС терористичного характеру на об'єкті, що охороняється і процесом управління ризиками вчинення терористичного акту на об'єкті, що охороняється критичної інфраструктури можна поставити знак рівності, так як безпосереднє запобігання терористичного акту покладається на системи фізичного захисту (ФЗ), коли дії зловмисників носять явно ворожий характер, і повинні рішуче припинятися.

По суті система ФЗ конкретного об'єкта повинна протистояти системі терористичного вторгнення на об'єкт. Від того, наскільки ефективно система ФЗ здатна протистояти підготовленої акції, залежить захищеність і цілісність об'єкта, що охороняється.

Складовою частиною системи ФЗ є комплексна система безпеки, яка являє собою організаційно-технічну систему, що складається з алгоритмічно об'єднаних систем, що забезпечують захист об'єкта від загроз різної природи. До складу цієї системи входять сигналізаційні рубежі, фізичні бар'єри, персонал контролерів контрольно-пропускних пунктів, стаціонарних і мобільних постів спостереження, оператори центрального пульта управління [1, 10, 17, 20].

Головний принцип побудови будь-якої системи забезпечення безпеки – це превентивність. Стосовно до систем ФЗ об'єкта реалізація цього принципу означає, що чим раніше буде виявлена загроза вторгнення на об'єкт, і чим своєчасне вона буде усунена, тим ефективніше працює система. Інакше кажучи, дальність виявлення зловмисників на підходах до об'єкта є ключовою характеристикою, яка і визначає ймовірність виявлення зловмисників.

При побудові і оцінці ефективності системи ФЗ існує два полярних підходу. Перший має на увазі введення в систему великого штату сил охорони і розробку організаційних заходів, при цьому основний акцент робиться на людський фактор. Другий підхід, навпаки, полягає в максимальному використанні технічних засобів, а сили охорони використовуються в основному для

припинення дій порушників або зловмисників. Безумовно, оптимальне рішення носить проміжний характер між першим і другим підходом.

Головною проблемою побудови систем ФЗ є розробка сценарію вторгнення. У цьому плані передбачається, що порушник (зловмисник, терорист, диверсант та ін.) певним чином рухається до охоронюваного об'єкту – об'єкту терористичного акту. На лінії точок старту порушника (ТСП) спрацьовує система виявлення порушника, і сигнал тривоги передається на центральний пульт управління (ЦПУ).

Тут особою, яка приймає рішення, дається команда підрозділу охорони, яке реагує і присікає дії порушників, які повинні бути такими, щоб вони встигали перехопити порушника до його зближення з об'єктом, де він може виконати запланований терористичний акт.

Критична точка виявлення – це найближча до об'єкта точка на можливу траєкторії руху порушника, в якій підрозділ охорони встигає його нейтралізувати. Побудована лінія критичних точок виявлення навколо об'єкту, що охороняється дозволяє визначити необхідну кількість підрозділів для його захисту. Однак слід враховувати той факт, що зловмисник може просуватися самим різним, часом несподіваним, чином, наприклад, поповзом, використовуючи засоби маскування, на автомобілі, розвиваючи величезну швидкість, на парашуті або дельтаплані, скориставшись висхідними потоками повітря, та ін.

Крім того, при розробці сценарію вторгнення необхідно враховувати, що для досягнення мети терористичного акту зловмисники можуть використовувати найсучасніші досягнення науки і техніки. Тому в сценарії вторгнення для кожного виду засобів виявлення (оптоелектронних, інфрачервоних, акустичних, радіолокаційних та ін.). Приймається певне значення дальності виявлення зловмисника, який прийнято називати стандартної дальністю виявлення. Вона визначає конкретне значення ймовірності виявлення зловмисника в контрольованій зоні, що охороняється. Це значення є стандартною ймовірністю виявлення зловмисника і характеризує ефективність роботи системи фізичного ФС щодо запобігання або управління НС ТХ на об'єкті, що охороняється.

У реальному, постійно змінюються, в залежності від часу доби (ранок, день, ніч, вечір), пори року (зима, весна, літо, осінь), гідрометеоумов (дощ, туман, сніг), природних і штучних перешкод дальність виявлення зловмисника змінюється, що призводить до зміни ймовірності виявлення зловмисника в контрольованій зоні. Відповідно, зменшення поточної ймовірності в порівнянні зі стандартною свідчить про зменшення ефективності роботи системи фізичного захисту щодо запобігання або управління надзвичайною ситуацією терористичного характеру на об'єкті, що охороняється.

Коли вжитими заходами поточний значення дальності виявлення зловмисника збільшується, і, відповідно, поточне значення ймовірності виявлення зростає і стає більше, ніж стандарт, ефективність роботи системи фізичного захисту щодо запобігання або управління надзвичайною ситуацією терористичного характеру на об'єкті, що охороняється зростає.

Іншими словами, критерієм оцінки ефективності управління надзвичайною ситуацією терористичного характеру на об'єкті, що охороняється є ймовірність виявлення зловмисника на підходах до об'єкта в контрольованій зоні в певних стандартних умовах, передбачених сценарієм вторгнення, яка дозволяє системі ФЗ своєчасно реагувати і припиняти дії зловмисників. Ефективність управління ситуацією в поточний момент часу буде визначатися різницею значень поточної і стандартної ймовірностей виявлення зловмисника в контрольованій зоні, що охороняється. Позитивне значення різниці

буде говорити про позитивний, а негативний – про негативний ефект управління.

Одним з напрямків оптимізації процесу управління надзвичайною ситуацією терористичного характеру на об'єкті, що охороняється потенційно-небезпечному об'єкті – вдосконалення систем ФЗ шляхом розробки нових пристроїв і систем акустичного контролю приміщень і територій об'єкта і знімання мовної інформації.

На думку зарубіжних [10, 12, 13, 18, 20] і вітчизняних [7, 8, 14, 15, 19] фахівців, технічні засоби, що забезпечують знімання мовної інформації, діляться на дві великі групи: дистанційні та позиційні. До першої групи входять кошти, що забезпечують знімання мовної інформації на досить великій відстані від джерела звуку. Це спрямовані мікрофони, що дозволяють реєструвати звукові сигнали на відкритих майданчиках, які служать для відтворення мови та інших акустичних сигналів. До другої групи належать всі види закладних пристроїв, які реєструють мова, незалежно від подальшого способу передачі знятої інформації (радіоканал, провідні лінії, винос та ін.).

Спрямовані мікрофони використовуються найчастіше на відкритому повітрі, коли головним послаблює фактором є розширення фронту акустичної хвилі з відстанню і значне ослаблення звуку через розсіювачів в атмосфері (турбулентність, вітер, туман, мряка, опади та ін.). Виходить що, ступінь гучності звичайного розмови в точці прийому, розташованої в сотні метрів, виявиться ослабленим в сотні разів. Такий тиск істотно менше не тільки рівня реальних зовнішніх акустичних перешкод, але і порогової чутливості звичайних мікрофонів, внаслідок чого спрямовані мікрофони повинні мати не тільки високу чутливість, але і спеціальні антенні пристрої. Це забезпечить для ослабленого сигналу перевищення рівня власних шумів приймача. Під високою спрямованістю дії розуміється здатність пригнічувати зовнішні акустичні перешкоди з напрямків, які не збігаються з напрямом на джерело звуку.

Технічно реалізувати таке завдання досить складно, тому на практиці використовують один з двох варіантів пристроїв: слабо направлений мікрофон з високою чутливістю або високо направлений мікрофон з малою чутливістю, що призвело до різноманітності видів спрямованих мікрофонів. В даний час їх поділяють на чотири види: параболічні, плоскі акустичні – фазовані решітки, трубчасті (мікрофони біжучої хвилі) і градієнтні.

Параболічний мікрофон являє собою відбивач параболічної форми, в фокусі якого розташований звичайний мікрофон. Відбивач може виготовлятися як з оптично непрозорого, так і оптично прозорого матеріалу, наприклад, акрилової пластмаси. Акустичні хвилі, що приймаються на осьовому напрямку, відбиваються від параболічного дзеркала і надходять в фазі в фокальну точку, де відбувається їх підсумовування. За рахунок цього і виникає ефект посилення звукового сигналу. Чим більше параболічне дзеркало, тим вище коефіцієнт його посилення. Якщо прихід звукових хвиль не збігається з осьовим напрямком параболічного мікрофона, то додавання їх відображень від різних частин дзеркала в фокусі дасть менший результат, так як не всі складові будуть у фазі. Параболічний мікрофон є типовим прикладом високочутливого, але слабо-направленого мікрофона.

Плоскі акустичні фазовані решітки реалізують ідею одночасного прийому звукового поля в дискретних точках певної плоскої панелі, ортогональної до напрямку на джерело звуку. У цих точках розміщуються або мікрофони, або відкриті кінці спеціально виконаних звуководів, які забезпечують синфазне складання звукових хвиль, що надходять від джерела звуку в акустичному суматорі. Якщо звук приходить з осьового напрямку, то всі сигнали, що поширюються по звуководам, будуть в фазі, і додавання в акустичному суматорі дасть максимальний результат. Якщо мовний сигнал приходить під деяким кутом до осі, то сигнали від різних

звуководів будуть приходити не в фазі, що призведе до ослаблення результуючого сигналу. Конструктивно плоскі фазовані решітки вбудовуються в передню стінку кейса з подальшим камуфляжом, або в майку-жилет, яка одягається під піджак або сорочку. Необхідні електронні блоки, такі як підсилювач, блок живлення і інші, розташовуються в кейсі або під одягом залежно від конкретного конструктивного виконання. З цієї причини фазовані решітки з камуфляжом більш конспіративно, в порівнянні з параболічним мікрофоном.

Трубчасті мікрофони або мікрофони біжучої хвилі, приймають звук уздовж деякої лінії, що збігається з спрямованим на джерело звуком. Основою мікрофона є щілинний звуковід – жорстка порожниста трубка зі спеціальними щілинними отворами по всій його довжині, з круговою геометрією розташування для кожного з рядів. При прийомі сигналу з осьового напрямку відбувається складання синфазних сигналів, що проникають через щілини в звуководі. Коли ж звук приходить під деяким кутом до осі мікрофона, то виникає фазовий неузгодженість, і сумарний сигнал слабшає. В кінці звуководу вбудований мікрофон, вихід якого підключається через підсилювач до магнітофона і навушників. Для отримання більшої чутливості трубчастого мікрофону збільшують його довжину. Чим більше його довжина, тим сильніше придушуються перешкоди з бічних напрямків. Однак це демаскує його застосування.

В градієнтних мікрофонах, на відміну від усіх попередніх, використовується не операція додавання, а операція віднімання у напрямку приходу сигналу. Градієнтним мікрофоном першого порядку є мікрофон, який реалізує градієнт першого порядку. Він являє собою два досить мініатюрних мікрофона, розташованих досить близько один до одного. Вихідні сигнали мікрофонів електричні або акустичні віднімаються одне з одного, реалізуючи першу похідну звукового поля по осі мікрофона, і формують вузьку діаграму спрямованості від кута приходу звуку. Градієнтними мікрофонами високих порядків вважаються системи, що реалізують похідні другого, третього і більш високих порядків.

Таким чином, одним з перспективних напрямків підвищення ефективності процесу управління надзвичайною ситуацією терористичного характеру на об'єктах критичної інфраструктури держави, що охороняються є вдосконалення систем фізичного захисту шляхом розробки нових пристроїв і систем акустичного контролю приміщень і територій об'єкта і знімання мовної інформації з використанням параболічних, трубчастих і градієнтних мікрофонів і плоских акустичних фазованіх решіток, які забезпечують прийом акустичних сигналів на видаленні від ніс кольких десятків до кількох сотень метрів і забезпечують повну інформацію про дії та наміри людей, що реєструються в відео системах.

## Висновки

1. Системи охорони приміщень і контролю прилеглої території на потенційно небезпечних об'єктах, що охороняються розподіляються по трьох зонах: внутрішньої, охоронюваному периметру і зовнішньої (санітарній) зоні. Головним засобом збору інформації про обстановку на периметрі і підходах до нього є оптоелектронні засоби. Впровадження акустичних засобів контролю значно б підвищило інформативність охоронних систем і поліпшило б систему фізичного захисту об'єкта.

2. Основним завданням управління надзвичайної ситуацію є зменшення ступеня небезпеки або загрози, одним з підходів до оцінки якої є концепція ризику. Тут під ризиком розуміють можливість настання подій з негативними наслідками, тобто можливість реалізації передбачуваної небезпеки. З такої точки зору ефективність

управління надзвичайний ситуації оцінюється ступенем зменшення ймовірності настання негативних подій і (або) їх наслідків шляхом виконання певних заходів, які вимагають розумних витрат.

3. Одним з перспективних напрямків підвищення ефективності процесу управління надзвичайною ситуацією терористичного характеру на об'єктах критичної інфраструктури держави, що охороняються є вдосконалення систем фізичного захисту шляхом розробки нових пристроїв і систем акустичного контролю приміщень і територій об'єкта і знімання мовної інформації з використанням параболічних, трубчастих і градієнтних мікрофонів і плоских акустичних фазованіх решіток, які забезпечують прийом акустичних сигналів на видаленні від ніс кількох десятків до кількох сотень метрів і забезпечують повну інформацію про дії та наміри людей, що реєструються в відео системах.

## Список використаних джерел


1. Азаренко Е. В. Защита критической инфраструктуры государства от террористического воздействия / Е.В. Азаренко, Ю.Ю. Гончаренко, М.М. Дивизинюк, М.И. Ожиганова // К.: ИГНС НАНУ, 2018. 84 с. (ISBN 978-617-7187-25-6).
2. Азаренко, О., Гончаренко, Ю., Дівізінюк, М., Мірненко, В., & Сириця, Ю. (2020). Структурно-логічна модель управління надзвичайно ситуацією терористичного характеру та її особливостей, вбудованих скритим електромагнітним впливом на оперативний состав охороняемого об'єкта критичної інфраструктури. *Journal of Scientific Papers «Social Development and Security»*, *10*(1), 177-187. DOI : 10.33445/sds.2020.10.1.18
3. Азаров, С., Дівізінюк, М., Лобойченко, В., Мірненко, В., & Шевченко, Р. (2020). Нові підходи до розробки комплексних методів цивільної безпеки. *Journal of Scientific Papers «Social Development and Security»*, *10*(3), 51-63. DOI : 10.33445/sds.2020.10.3.5
4. Про оперативно-розшукову діяльність: Закон України. URL : http://zakon.rada.gov.ua
5. Основы оперативно-розыскной деятельности / Под ред. Б.А. Воронцова-Вельяминова. – Харьков: Изд-во АстроПринт, 2011. – 287 с.
6. Основы оперативно-розыскной деятельности / Под ред. Э.А. Дидаренко. – Харьков: Изд-во Твирпс, 2010. – 282 с.
7. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: Серія "Національна і международна безпека". – К.: КНТ, 2006. –206 с.
8. Лайда К. С. Психология оперативно-розыскной деятельности. – Харьков: Прайс, 2012. – 285 с.
9. Видеосъемка и звукозапись – средства, формирующие доказательную базу в ОРД. URL : http://ezop.ua/osnovy-operativ...
10. Защита критической инфраструктуры. Концепция основных мер защиты. Рекомендации для предприятий. URL : http://www.bmi.bund.de
11. Некоторые особенности оперативно-розыскной деятельности. URL : http://kharkov.kha.slando.ua
12. Оперативная звукозапись / Пер. с англ. под ред. М. А. Феликса. – М.: Интерпол, 2005. – 456 с.
13. Wenzel F. D6.1 – Decision-analytic frameworks for multi-hazard mitigation and adaptation, New methodologies for multi-hazard and multi-risk assessment meth-ods for Europe, Deliverable 6.1, 2012. 34 p. URL : http://matrix.gpi.kit.edu/ downloads/MA-TRIX-D6.1.pdf.
14. Идентификация речи как обвинительный аспект доказательного процесса. URL : http://worldandwe.com
15. Изменение акустических параметров речевых сигналов как фактор оперативной обстановки. URL : http://www.youtube.com
16. Инженерные средства физической защиты периметра. URL : http://www.algoritm.org/arch/arch.php?id=

41&a=734
17. Средства сигнализации в охране стационарных объектов. Интернет публикация. 10.09.2009. – 5 с. URL : http//www.karabiner.ua
18. Xovard B. Lazeracustic // Optronics. Sincepress. 1991. vol. 10. №10. p. 89-100.
19. Азаренко Е. В. Анализ экспериментов по определению дальности съема речевой информации / Е.В. Азаренко, О.В. Бас, Ю. Ю. Гончаренко, М. М. Дивизинюк, М. И. Ожиганова, А. С. Рыжкин // Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні". – Київ: Державна служба спеціального звуку та захисту інформації в Україні НТУУ «КПІ», 2019. – Вип. 1 (37). – С. 89 – 97.
20. Audio Inteligence Devices // Product Catalog, 2012. – 402 p.

# Пути повышения эффективности систем физической защиты охраняемых объектов критической инфраструктуры государства

**Елена Азаренко * [1 A]; Юлия Гончаренко [2 B]; Михаил Дивизинюк [3 C]; Владимир Мирненко [4 D]; Валерий Стрелец [5 A]**

*** Corresponding author:** [1] д.ф-м.н., профессор, заместитель руководителя, e-mail: azarenko_ev@ukr.net, ORCID: 0000-0003-2927-5545
[2] к.т.н., доцент, профессор кафедры, e-mail: vup@e-u.in.ua, ORCID: 0000-0003-2045-0263
[3] д.ф-м., профессор, главный научный сотрудник, e-mail: divizinyuk@ukr.net, ORCID: 0000-0002-5657-2302
[4] д.т.н., профессор, директор департамента, e-mail: mirnenkovi@gmail.com, ORCID: 0000-0002-7484-1035
[5] руководитель, e-mail: v.strelec.brand@gmail.com, ORCID: 0000-0003-1913-7878

[A] Научно-исследовательский лабораторно-экспериментальный центр "БРАНД ТРЕЙД", Киев, Украина.
[B] Европейский университет, г. Киев, Украина.
[C] Институт геохимии и окружающей среды НАН Украины, Киев, Украина.
[D] Департамент военного образования и науки Министерства обороны Украины, г. Киев, Украина.

***Аннотация***

Статья посвящена определению новых направлений повышения эффективности систем физической защиты охраняемых объектов критической инфраструктуры, которые являются главным техническим средством недопущения террористических актов против этих объектов. Сначала дана характеристика систем охраны помещений и контроля прилегающих территорий охраняемых объектов критической инфраструктуры. Показано, что по функциональному назначению в систему физической защиты входят устройства и системы сигнализации обнаружения, сбора и обработки информации, тревожно-вызывной сигнализации, контроля и управления доступом, оптоэлектронного наблюдения, оперативной связи и оповещения, обеспечения электропитания и электроосвещения, системы обеспечения физической защиты. ядерных материалов при транспортировке Они распределяются по трем зонам: внутренней, охраняемому периметру и наружной (санитарной) зоне. Главным средством сбора информации об обстановке на периметре и подходах к нему являются оптоэлектронные средства. Затем рассмотреть особенности процесса управления чрезвычайной ситуаций террористического характера на охраняемом объекте критической инфраструктуры. Показано, что главная цель управления чрезвычайными ситуациями террористического характера – это недопущение террористического акта на охраняемом объекте, который является объектом управления. Структурно-логическая модель управления чрезвычайной ситуацией состоит из шести блоков: блока мониторинга ситуации; блока обнаружения риска; блока анализа рисков; блока подготовки вариантов управленческих решений; блока принятия решения и доказывание его исполнителей; блока влияния на ситуацию, которая через структуру исполнителей влияет на объект управления и замыкает его контур

управления, обеспечивая тем самым непрерывность процесса управления чрезвычайной ситуацией террористического характера в интересах ее недопущения и предотвращения. После чего определить пути повышения эффективности систем физической защиты охраняемых объектов критической инфраструктуры государства. Показано, что одним из перспективных направлений повышения эффективности процесса управления чрезвычайной ситуацией террористического характера на охраняемых объектах критической инфраструктуры государства является совершенствование систем физической защиты путем разработки новых устройств и систем акустического контроля помещений и территорий объекта и снятия языковой информации с использованием параболических, трубчатых и градиентных микрофонов и плоских акустических решеток, которые обеспечивают прием акустических сигналов на удалении от нескольких десятков до нескольких сотен метров и обеспечивают полную информацию о действиях и намерениях людей, регистрируемых в видео системах.

***Ключевые слова:*** чрезвычайная ситуация, террористический акт, система физической защиты, акустический контроль, направленный микрофон.

# Ways to increase the effectiveness of physical protection systems of critical infrastructure of the state, protected

**Olena Azarenko * [1 A]; Yulia Honcharenko [2 B]; Mykhailo Divizinyuk [3 C]; Volodymyr Mirnenko [4 D]; Valeriy Strilets [5 A]**

* **Corresponding author:** [1] Dr, Professor, Deputy Head, e-mail: e-mail: azarenko_ev@ukr.net, ORCID: 0000-0003-2927-5545
[2] Ph.D., Associate Professor, Professor of Department, e-mail: vup@e-u.in.ua, ORCID: 0000-0003-2045-0263
[3] Dr, Professor, Head of Department, e-mail: divizinyuk@ukr.net, ORCID: 0000-0002-5657-2302
[4] Dr, Professor, Director of the Department, e-mail: mirnenkovi@gmail.com, ORCID: 0000-0002-7484-1035
[5] Head, e-mail: v.strelec.brand@gmail.com, ORCID: 0000-0003-1913-7878

[A] Research laboratory-experimental center "BRAND TRADE"
[B] European University, Kyiv, Ukraine
[C] Institute of Environmental Geochemistry of the NAS of Ukraine, Kyiv, Ukraine
[D] Department of Military Education and Science of the Ministry of Defense of Ukraine, Kyiv, Ukraine

***Abstract***

The article is devoted to the definition of new ways to increase the effectiveness of physical protection systems of critical infrastructure, which are the main technical means of preventing terrorist acts against these objects. The characteristic of premises protection systems and control objects adjoining territories of critical infrastructure is described. It is shown that the functional purpose of the physical protection system includes devices and alarm systems for detection, collection and processing of information, alarm, access control and management, optoelectronic surveillance, operational communication and notification, power supply and lighting, physical protection systems nuclear materials during transportation.

***Keywords:*** emergency, terrorist act, physical protection system, acoustic control, directional microphone.

## References

1. Azarenko E.V., Goncharenko Yu. Yu., Divizinyuk M. M., Ozhiganova M.I. Protection of critical infrastructure of the state from terrorist impact. Kyiv: IGNS NASU, 2018. 84 p. ISBN 978-617-7187-25-6.
2. Azarenko, E., Honcharenko, Y., Divizinyuk, M., Mirnenko, V., & Syrytsia, I. (2020). Structural-logical model of emergency situation management of terrorist character and its features caused by latent electromagnetic influence on the operational staff of the guarded facility of critical infrastructure. *Journal of Scientific Papers «Social Development and Security»*, *10*(1), 177-187.

DOI : 10.33445/sds.2020.10.1.18

3. Azarov, S., Divizinyuk, M., Loboichenko, V., Mirnenko, V., & Shevchenko, R. (2020). New approaches to the development of integrated methods of civil security. *Journal of Scientific Papers «Social Development and Security»*, *10*(3), 51-63. DOI : 10.33445/sds.2020.10.3.5
4. On operative-search activity: Law of Ukraine. URL : http://zakon.rada.gov.ua
5. Fundamentals of operational and investigative activities / Ed. B.A. Vorontsov-Velyaminov. – Kharkiv: AstroPrint Publishing House, 2011. 287 p.
6. Fundamentals of operational and investigative activities / Ed. E.A. Didarenko. – Kharkiv, 2010. 282 p.
7. Lipkan V. A. (2006). Information security of Ukraine in terms of European integration. *Series "National and International Security"*. – Kyiv, 2006. 206 p.
8. Laida K. S. Psychology of operational and investigative activities. – Kharkiv: Praise, 2012. 285 p.
9. Video recording and sound recording – the means that form the evidence base in the ORD. Available from : http: //ezop.ua/osnovy-operativ ...
10. Critical infrastructure protection. The concept of basic protection measures. Recommendations for companies. Available from : http://www.bmi.bund.de
11. Some features of operational and investigative activities. Available from : http://kharkov.kha.slando.ua
12. Operational sound recording / Per. with English under ed. M. A. Felix. – Moscow : Interpol, 2005. 456 p.
13. Wenzel F. D6.1 – Decision-analytical frameworks for multi-hazard mitigation and adaptation, New methodologies for multi-hazard and multi-risk assessment meth-ods for Europe, Deliverable 6.1, 2012. 34 p. URL: http://matrix.gpi.kit.edu/ downloads / MA-TRIX-D6.1.pdf.
14. Speech identification as an accusatory aspect of the evidentiary process. Available from : http://worldandwe.com
15. Change of acoustic parameters of speech signals as a factor of an operational situation. Available from : http://www.youtube.com
16. Engineering means of physical protection of the perimeter. Available from : http://www.algoritm.org/arch/arch.php?id=41&a=734
17. Means of the alarm system in protection of stationary objects. Internet publication. 10.09.2009. 5 p. Available from : http // www.karabiner.ua
18. Xovard B. Lazeracustic. *Optronics. Sincepress*. 1991. vol. 10. №10. p. 89-100.
19. Azarenko E.V., Bass O.V., Goncharenko Yu. Yu., Divizinyuk M.M., Ozhiganova M.I., Ryzhkin A.S. (2019). Analysis of experiments to determine the range of speech information. *Scientific and technical collection "Legal, regulatory and metrological support of information security systems in Ukraine"*. Kyiv: State Service for Special Sound and Information Protection in Ukraine NTUU "KPI", 2019. Issue. 1 (37). P. 89 – 97.
20. Audio Inteligence Devices // Product Catalog, 2012. – 402 p.