

1. А. Дослідження стійкості серверних технологій Java від атак на відмову // *Захист інформації*. – 2004. – №4, с.11 – 18. 4. Шохін Б. П., Юдін О. М., Мазулевський О. Є. Вдосконалення контролю за станом захищеності комп'ютерної мережі на основі адаптивного моніторингу // *Зб. н. п. військового інституту телекомунікацій та інформатизації національного технічного університету України "КПІ"*. – 2004. – Випуск №4, с.208 – 217. 5. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: Термінологічний навчальний довідник. // К.: ООО „Д.В.К”, 2004. – 508 с. 6. Кузнецов Г. В., Иванов А. М. Методы анализа данных для обнаружения атак в компьютерных системах и сетях банковских структур. *Защита информации*. Сб. н. тр. НАУ, Киев – 2004, С.34-42. 7. Воробьев В. Г., Глухов В. В., Козлов Ю. В. *Диагностирование и прогнозирование технического состояния авиационного оборудования*. – М.: Транспорт, 1984.-191 с. 8. Игнатов В. А., Маньшин Г. Г., Трайнев В. А. *Статистическая оптимизация качества функционирования электронных систем*. М.: Энергия, 1974,-264 с. 9. Хорошко В. О., Кудінов В. А. *Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України. Захист інформації*. – 2004. – №4, с.11 – 18.

УДК 681.3

## ЕКСПЕРТНА ОЦІНКА БЕЗПЕКИ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ЗА КРИТЕРІЄМ “РИЗИК БЕЗПЕКИ-ГАРАНТІЯ БЕЗПЕКИ”

**Вячеслав Шорошев**

*Державний науково-дослідний інститут МВС України*

*Анотація:* Надаються узагальнені критерії експертної оцінки стану безпеки інформації в комп'ютерних системах за критерієм “ризик безпеки-гарантія безпеки”.

*Summary:* The generalized yardsticks of an expert estimation of safety of the information in computer systems by yardstick « of risk the safety - safe conduct » are esteemed.

*Ключові слова:* Ризик безпеки, гарантія безпеки, послуга безпеки, стандартний профіль захищеності інформації.

### Вступ

Складність проблеми полягає в тому, що стан безпеки інформації в комп'ютерних системах України необхідно оцінювати за умови її обробки, захисту та поширення з широким використанням сучасних інформаційних технологій. На цей час їх основою є комп'ютерні дані та системи, а також суворе дотримання вимог чинних нормативних документів Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України щодо забезпечення конфіденційності, цілісності та доступності оброблюваної інформації. Це вже висвітлювалось у роботах [1 – 6].

Це не така проста проблема. Провідними країнами світу вона вирішувалась понад 14 років (1983 – 1997 роки), поки на було розроблено міжнародні критерії і стандарти щодо експертної оцінки стану захищеності інформації в комп'ютерних системах від загроз несанкціонованого доступу. Було інвестовано і успішно реалізовано дослідження щодо розробки міжнародних критеріїв і стандартів комп'ютерної безпеки в США, Канаді, Франції, Англії, Німеччині, Нідерландах, Російській Федерації. Аналогічна проблема протягом 9 років (1991 – 1999 роки) кардинально вирішувалась і в Україні. З 1999 р. в Україні було введено в дію вітчизняні критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

При розробці критеріїв у провідних країнах світу в основу було покладено велику сукупність критеріїв – від 6 – 10 простих універсальних критеріїв (1983 – 1991 р. р.) до 70 – 160 (1992 – 1999 р. р.) складних часткових критеріїв [6]. Користуватись такими критеріями і робити експертну оцінку стану безпеки інформації в комп'ютерних системах за такими підходами дуже непросто. Така проблема стояла і при використанні вітчизняних критеріїв щодо експертної оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Треба було знайти якийсь вихід.

Але для цього треба перейти від сукупності 110 часткових критеріїв оцінки стану захищеності (безпеки) інформації в комп'ютерних системах згідно з вимогами НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99 до двох-трьох узагальнених критеріїв, які треба розробити та реалізувати. Це обумовлено тим, що прийняття рішення за багатьма критеріям саме по собі теоретично проблемне і поки що фундаментально розроблено ще не до кінця. Так, на цей час в теорії прийняття рішень за багатьма критеріями обмежуються золотим

правилом "сім плюс/мінус два" – по кількості самих критеріїв, а далі використовуються різні методи апроксимації для зменшення великої кількості критеріїв [6 – 8].

## I Основна частина

Пропонується при експертній оцінці стану безпеки інформації в комп'ютерних системах (КС) використовувати наступні узагальнені критерії замість множини з 110 часткових критеріїв згідно з чинними вимогами НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99, а саме:

- рівень гарантії безпеки інформації Г-1...Г-7 згідно з вимогами НД ТЗІ 2.5-004-99, який задається в певній КС;
- ризик безпеки R інформації в КС, який чисельно оцінюється імовірністю ненадання жодної послуги безпеки з повної низки регламентованих в НД ТЗІ 2.5-004-99 елементарних функціональних ПБ-ЕФ, умовно-необхідних ПБ-УН та елементарних гарантійних ПБ-ЕГ послуг безпеки для кожної обраної профільної послуги безпеки ПБ-П у певній КС; ризик безпеки визначається як функціонал F послуг безпеки ПБ-П, ПБ-ЕФ, ПБ-УН, ПБ-ЕГ, Г-1...Г-7;
- рейтинг E стандартного профілю захищеності інформації, який чисельно оцінюється імовірністю надання для кожної профільної послуги безпеки (ПБ-П) повної (максимально можливої) низки елементарних функціональних послуг безпеки (ПБ-ЕФ): конфіденційності, цілісності, доступності і спостереженості інформації в КС, аналогічно умовно-необхідним (ПБ-УН) та елементарним гарантійним (ПБ-ЕГ) послугам безпеки; рейтинг E визначається як функціонал F послуг безпеки ПБ-П, ПБ-ЕФ, ПБ-УН, ПБ-ЕГ згідно з вимогами критеріїв захищеності інформації в НД ТЗІ 2,5-004-99.

Таким чином, у загальному вигляді математичне співвідношення запропонованих узагальнених критеріїв можна визначити функціоналами:

$$E = F(\text{ПБ-П, ПБ-ЕФ, ПБ-УН, ПБ-ЕГ}), \quad (1)$$

$$R = F(E, \text{Г-1...Г-7}). \quad (2)$$

Програмно-математична реалізація наведених співвідношень досить складна і вирішується різними програмно-математичними методами шляхом обчислення певних ймовірностей – графа (дерева) подій, співвідношення числа успішних подій до їх можливої повної сукупності, використання формул Байеса тощо. Але при цьому за основу приймається обов'язкове дотримання елементарних послуг безпеки, регламентованих в НД ТЗІ 2.5-004-99, тобто послуг безпеки ПБ-ЕФ, ПБ-УН, ПБ-ЕГ.

Для практичного використання за даними [6] нижче надається універсальна розрахункова таблиця для вибору варіанту сукупності стандартних функціональних профілів захищеності інформації (СПЗІ) у певній КС залежно від їх складу, загального рейтингу E та одержаного ризику R безпеки при заданому рівні гарантії безпеки Г-1...Г-7 (табл. 1).

На основі аналізу даних табл. 1 можна зробити наступні висновки і рекомендації.

1. Рейтинг профілю захищеності поступово зростає або при збільшенні кількості профільних послуг безпеки ПБ-П, або при збільшенні рівня певної обраної профільної послуги безпеки, наприклад, КК-1, КК-2, КК-3 чи КА-2, КА-3, КА-4, чи НР-1, НР-2, НР-3, НР-4, НР-5 тощо (профільні послуги безпеки надаються в умовних позначеннях згідно з НД ТЗІ 2.5-004-99).

2. Послуги спостереженості ПБ-Н є обов'язковими і необхідними для надання послуг конфіденційності ПБ-К, цілісності ПБ-Ц, доступності ПБ-Д, тому що ними гарантується нормальне функціонування ядра безпеки обчислювальної системи КС, тобто контроль цілісності комплексу засобів захисту КЗЗ (НЦ-1, НЦ-2, НЦ-3, НО-1, НО-2, НО-3, НИ-1, НИ-2, НИ-3 тощо). Для КС класу 1 їх визначається шість (реєстрація НР, ідентифікація й автентифікація НИ, достовірний канал НК, розподіл обов'язків НО, цілісність КЗЗ НЦ, самотестування НТ), а для КС класу 2, 3 – дев'ять (шість НР, НИ, НК, НО, НЦ, НТ плюс ідентифікація й автентифікація при обміні НВ, автентифікація відправника НА, автентифікація отримувача НП). Це мінімально необхідні й обов'язкові низки профільних послуг спостереженості ПБ-Н, а саме: шість вище наданих послуг безпеки для КС класу 1 (НР, НИ, НК, НО, НЦ, НТ) і дев'ять для КС класу 2 і 3 (НР, НИ, НК, НО, НЦ, НТ, НВ, НП, НА).

3. Рейтинг профілів захищеності E поступово зростає або при наданні нових профільних послуг безпеки ПБ-П, або при підвищенні їх рівня до максимального від  $E = 0,131868$  (варіант СПЗІ-1 для КС класів 2 та 3 до  $E = 1,000000$  (варіант СПЗІ-12).

4. Аналогічно ризик безпеки R інформації в КС ОВС зменшується від максимального 0,868132 (варіант СПЗІ-1) до мінімального 0,000000 (варіант СПЗІ-12).

5. На основі наведених розрахункових даних табл. 1 можна вибирати відповідні стандартні профілі захищеності інформації в певній КС щодо заданого ризику безпеки при її гарантії на рівні Г-1...Г-7. Рівні гарантії Г-1...Г-7 оцінюються окремо щодо дотримання вимог для надання гарантійних послуг безпеки згідно з НД ТЗІ 2.5-004-99.

6. Універсальна розрахункова таблиця по точності дискретно охоплює весь проміжок значень загального рейтингу Е низки певних стандартних профілів захищеності СПЗІ від мінімально необхідного (0.131868) до максимально можливого (1.000000) та весь проміжок значень одержаного ризику безпеки R від максимального (0.868132) до мінімально можливого (0.000000).

7. Сукупність профільних послуг спостереженості НР, НИ, НК, НО, НЦ, НТ (КС класу 1), НР, НИ, НК, НО, НЦ, НТ, НВ, НА, НП (КС класу 2, 3), послуг конфіденційності КД (конфіденційність довірча), КА (конфіденційність адміністративна), КО (повторне використання об'єктів), КК (аналіз прихованих каналів), КВ (конфіденційність при обміні), послуг цілісності ЦД (довірча цілісність), ЦА (адміністративна цілісність), ЦО (відкат), ЦВ (цілісність при обміні), послуг доступності ДР (використання ресурсів), ДС (стійкість до відмов), ДЗ (гаряча заміна), ДВ (відновлення після збоїв) визначається як вирішальна компонента КЗЗ захищеної КС для вибору належного ризику безпеки інформації в певній КС.

8. Сукупність профільних послуг безпеки ПБ-П п. 7 визначається ядром певного стандартного функціонального профілю захищеності інформації у певній КС. Від неї найбільш суттєво залежить рейтинг R по формулі (1) певного стандартного функціонального профілю захищеності інформації (СПЗІ-1...СПЗІ-12 табл. 1).

9. Вирішальною частиною стандартного функціонального профілю захищеності інформації у певній КС, крім профільних, також визначаються гарантійні послуги безпеки Г-1...Г-7. На цей час в НД ТЗІ 2.5-004-99 враховується тільки рівень Г-3 (в умовно-необхідних послугах безпеки ПБ-УН), але це не остаточно, на нашу думку. Додання до послуг ПБ-УН послуг безпеки рівня Г-3 суттєво важливо, тому що вони додатково регламентують дотримання певних вимог до захищеної КС на всіх стадіях її життєвого циклу (від проектування, розробки і до функціонування, випробувань та документації). При підвищенні вимог до стану безпеки інформації в захищеній КС (до рівня обмеженості) доцільно, на нашу думку, надавати у послугах ПБ-УН й інші, більш високі рівні гарантії безпеки, крім Г-3.

Таблиця 1 – Базова таблиця для вибору стандартних профілів захищеності інформації щодо їх рейтингу та одержаного ризику безпеки при заданому рівні гарантії безпеки

Сукупність СПЗІ	Склад стандартного профілю захищеності інформації СПЗІ щодо надання низки профільних послуг безпеки різного виду та рівня	Рейтинг СПЗІ	Ризик безпеки СПЗІ	Рівні гарантії безпеки Г1...Г7
КС класу 1				
СПЗІ-1	НР-2,НИ-2,НК-1,НО-1,НЦ-1,КА-1,КО-1,ДВ-1	0.194847	0.805153	Г-3
СПЗІ-3	НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1, КД-3, КО-1, ЦД-1, ЦО-1	0.223529	0.776471	Г-3
СПЗІ-2	НР-2, НИ-3, НК-1, НО-2, НЦ-1, НТ-2, КА-2, КО-1, ДВ-1, ЦА-1	0.235104	0.764896	Г-3
СПЗІ-4	НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, КД-2, КО-1, ЦД-1, ЦО-2, ЦА-3	0.294118	0.705882	Г-3
СПЗІ-5	НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, КД-2, КО-1, КА-2, КК-1, ЦД-1, ЦА-3, ЦО-2,	0.541177	0.458823	Г-3
СПЗІ-6	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, КД-4, КО-1, КА-2, КК-1, ЦД-4, ЦА-3, ЦО-2	0.664706	0.335294	Г-3
СПЗІ-7	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, КД-4, КО-1, КА-4, КК-3, ЦД-4, ЦА-4, ЦО-2, ЦВ-3	0.776471	0.223529	Г-3
СПЗІ-8	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, КД-4, КО-1, КА-4, КК-3, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-1	0.847059	0.152941	Г-3
СПЗІ-9	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, КД-4, КО-1, КА-4, КК-3, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3	0.882353	0.117647	Г-3
СПЗІ-10	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, КД-4, КО-1, КА-4, КК-3, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3, ДВ-3, КВ-1	0.941177	0.058823	Г-3
СПЗІ-11	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, КД-4, КО-1, КА-4, КК-3, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3, ДВ-3, КВ-3	0.982353	0.017647	Г-3

СПЗІ-12	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, КД-4, КО-1, КА-4, КК-3, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3, ДВ-3, КВ-4	1.000000	0.000000	Г-3
КС класу 2, 3				
СПЗІ-1	НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1, НП-1, НА-1, НВ-1, КО-1	0.131868	0.868132	Г-3
СПЗІ-2	НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1, НП-1, НА-1, НВ-1, КО-1, ДВ-1	0.159341	0.840659	Г-3
СПЗІ-3	НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1, НП-1, НА-1, НВ-1, КД-2, КО-1, ЦД-1, ЦО-1	0.225275	0.774725	Г-3
СПЗІ-4	НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, КД-2, КО-1, ЦД-1, ЦО-2, ЦА-3	0.280220	0.719780	Г-3
СПЗІ-5	НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НП-2, НА-2, НВ-2, КД-2, КО-1, КА-2, КК-1, ЦД-1, ЦА-3, ЦО-2	0.565934	0.434066	Г-3
СПЗІ-6	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, НП-2, НА-2, НВ-3, КД-4, КО-1, КА-2, КК-1, ЦД-4, ЦА-3, ЦО-2	0.686813	0.313187	Г-3
СПЗІ-7	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, НП-2, НА-2, НВ-3, КД-4, КО-1, КА-4, КК-3, ЦД-4, ЦА-4, ЦО-2, ЦВ-3	0.791209	0.208791	Г-3
СПЗІ-8	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, НП-2, НА-2, НВ-3, КД-4, КО-1, КА-4, КК-3, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-1	0.857143	0.142857	Г-3
СПЗІ-9	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, НП-2, НА-2, НВ-3, КД-4, КО-1, КА-4, КК-3, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3	0.890110	0.109890	Г-3
СПЗІ-10	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, НП-2, НА-2, НВ-3, КД-4, КО-1, КА-4, КК-3, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3, ДВ-3, КВ-1	0.945055	0.054945	Г-3
СПЗІ-11	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, НП-2, НА-2, НВ-3, КД-4, КО-1, КА-4, КК-3, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3, ДВ-3, КВ-3	0.983516	0.016484	Г-3
СПЗІ-12	НР-5, НИ-3, НК-2, НО-3, НЦ-3, НТ-3, НП-2, НА-2, НВ-3, КД-4, КО-1, КА-4, КК-3, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3, ДВ-3, КВ-4	1,000000	0,000000	Г-3

**Примітка:** 1. Для прикладу обрано рівень гарантії безпеки Г-3, але можна вибирати будь-який з низки Г-1...Г-7 з додержанням їх вимог. 2. Якщо СПЗІ містить будь-яку із профільних послуг безпеки КК-1...КК-3 чи КВ-4, то можна вибирати тільки рівні Г-3...Г-7, а якщо ні, то можна вибирати тільки рівні Г-1...Г-2. 3. Якщо відсутні послуги К, Ц, Д, а надаються тільки послуги Н, то ризик безпеки найбільший.

10. У чинних НД ТЗІ 2.5-005-99 надано примірну базову сукупність стандартних профілів захищеності інформації для кожного класу та підкласу (К – підвищені вимоги до захисту від загроз конфіденційності, Ц – підвищені вимоги до захисту від загроз цілісності, Д – підвищені вимоги до захисту від загроз доступності, КЦ – підвищені вимоги до захисту від загроз конфіденційності і цілісності, КД – підвищені вимоги до захисту від загроз конфіденційності і доступності, ЦД – підвищені вимоги до захисту від загроз цілісності і доступності, КЦД – підвищені вимоги до захисту від загроз конфіденційності, цілісності і доступності).

Це необхідно для тлумачення підходу щодо визначення, призначення і складу стандартних профілів захищеності інформації для кожного класу та підкласу КС (АС). Але вони не містять їх повної сукупності щодо можливих сполучень з них профільних послуг безпеки ПБ-П. Доцільні, на нашу думку, розробка та створення Національного каталогу стандартних профілів захищеності інформації для кожного класу і підкласу КС (АС), у якому буде надано та регламентовано повну їх сукупність з визначенням їх рейтингу Е і відповідного ризику безпеки R захищуваної інформації в КС (АС) від загроз несанкціонованого доступу.

11. Запропонована універсальна розрахункова таблиця може бути використана для розробки технічних завдань щодо вибору сукупності стандартних профілів захищеності інформації та створення захищених

КС (АС) по критерию “ризик – гарантія безпеки”. У подальшому доцільна її доробка щодо визначення та надання сукупності стандартних профілів захищеності інформації за критерієм “ефективність – вартість”.

12. Найбільш практично поширеними і типовими чи базовими вважаються стандартні профілі СПЗІ-1 та СПЗІ-3 для КС, АС класу 1, тому що вони містять мінімально необхідний склад профільних послуг безпеки.

### Висновок

Запропонований критеріальний підхід щодо оцінки стану безпеки інформації може бути використаний як варіант для розробки або уточнення базової методики оцінки захищеності інформації від несанкціонованого доступу в КС (АС).

*Література:* 1. Пакет з п'яти нормативних документів з питань захисту інформації від несанкціонованого доступу Департаменту СТСЗІ СБ України, К., 1999. 2. Шорошев В. В. Оцінка стану безпеки інформації за стандартними профілями її захищеності в комп'ютерних (автоматизованих) системах // Науково-технічний збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні”, випуск № 8, 2004, с. 48 – 56. 3. Шорошев В. В. Оцінювання стану безпеки інформації за профілями її захищеності від загроз НСД у комп'ютерних системах // “Зв'язок” № 6, 2004, с. 48 – 50. 4. Шорошев В. В., Ильницький А. Е., Близнюк И. Л. Защита информации компьютерных систем от угроз НСД и национальные критерии ее экспертной оценки. Бизнес и безопасность. № 6. 2000. – С. 5 – 6. 5. В. В. Шорошев. Базова модель експертної системи щодо оцінки безпеки інформації в комп'ютерних системах. // Науково-технічний збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні”, випуск № 3, 2001, с. 79 – 86. 6. А. Ю. Ильницький, В. В. Шорошев та ін. // Монографія “Базова модель експертної системи оцінки безпеки інформації в КС ОВС”. – К., 2002. – 316 с. 7. Д. Уотермен. Руководство по экспертным системам. Издательство “Мир”. – М., 1998. 8. Ларичев О. И. Объективные модели и субъективные решения. Наука. М.: 2000. С.123 – 130.

УДК.621.791

## ОБЕСПЕЧЕНИЕ КОМФОРТНОСТИ ВЫДЕЛЕННЫХ ПОМЕЩЕНИЙ ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМ АКТИВНОЙ ВИБРОАКУСТИЧЕСКОЙ ЗАЩИТЫ

*Игорь Порошин, Александр Сигаев, Юрий Непочатых*  
НИЦ “ТЕЗИС” НТУУ “КПИ”

*Аннотация:* Розглянуто вплив конфігурації обвідної спектра захисного зашумлення на комфортність акустичної обстановки виділеного приміщення. Проаналізовано особливості вимог до технології налагодження й до характеристик віброакустичного генератора, реалізація яких може забезпечити підвищення комфортності. Відмічено, що серед вітчизняних комплексів віброакустичного захисту найбільші можливості щодо підвищення комфортності має прилад віброакустичного захисту ОЦЗІ-ВА.

*Summary:* The influence of protection noise spectrum on the acoustic comfort inside protected places are considered. Peculiarities of demands for the tuning technology of active protection noise systems and for noise generator characteristics are considered providing the better acoustic comfort. It's noted that the vibroacoustic protection set „ОЦЗІ-ВА” has best possibilities to improve the acoustic comfort.

*Ключевые слова:* Активная виброакустическая защита, акустический комфорт, предельные спектры. методика настройки, характеристики виброакустического генератора.

### І Введение

Одной из основных проблем, связанных с применением систем активной виброакустической защиты (АВЗ), является проблема обеспечения акустической комфортности при их функционировании на объектах информационной деятельности [1, 2]. Как показала практика, работа систем АВЗ неизбежно сопровождается наличием побочных акустических шумов, главной причиной которых является вибрация открытых нерабочих поверхностей виброизлучателей [2]. Уровень этих шумов увеличивается с ростом уровня защитного виброзащумления, и поэтому во многих практических случаях он может достигнуть