*Атіка, 2002. – 240 с. **4**. Доповідь Кабінету Міністрів України Верховній Раді України про стан та розвиток інформатизації в Україні за 2003 рік. **5**. http:// www.1plus1.net. **6**. http://www.crime-research.org.**7**. http://itware.com.ua. **8**. В. Бутузов, М. Гуцалюк, В. Цимбалюк Протидія злочинності у сфері високих технологій // Міліція України. – 2002, –- № 9. – С. 20 – 21.*

УДК 681.3

ОЦІНКА СТАНУ БЕЗПЕКИ ІНФОРМАЦІЇ ЗА СТАНДАРТНИМИ ПРОФІЛЯМИ ЇЇ ЗАХИЩЕНОСТІ В КОМП'ЮТЕРНИХ (АВТОМАТИЗОВАНИХ) СИСТЕМАХ

В'ячеслав Шорошев
НДІ Національної академії внутрішніх справ України

Анотація: **Висвітлюються необхідність, правила та проблеми створення каталогу стандартних профілів захищеності інформації в комп'ютерних системах усіх класів і підкласів.**
Summary: **The rules and problems of creation of standard structures of security of the information in computer systems of all classes and subclasses are shined (covered) necessity.**
Ключові слова: **Послуги безпеки, підклас АС (КС), профіль захищеності інформації, конфіденційність, цілісність, доступність, спостереженість інформації.**

Проблема оцінки стану безпеки інформації в комп'ютерних (автоматизованих) системах дуже актуальна як в нормативно-правовому і системно-концептуальному, так і в суто практичному плані.

Справа в тому, що багатий міжнародний досвід інвестиційних програм США, Канади, Англії, Німеччини, Франції, Нідерландів щодо розробки, удосконалення, уніфікації та стандартизації критеріїв комп'ютерної безпеки свідчить про те, що безпека інформації, оброблюваної в комп'ютерних системах, і надалі була, є і буде вічною проблемою для трьох основних категорій: розробників, користувачів й експертів кваліфікаційного аналізу захищених комп'ютерних систем.

За вказаний проміжок часу проблема визначення та уніфікації критеріїв для експертної оцінки стану безпеки інформації в комп'ютерних системах витримила ряд кардинальних концептуальних змін, але ми зосередимося тільки на двох із них, які були використані у вітчизняних нормативних документах з питань технічного захисту інформації та одержали подальший розвиток.

Перша полягала в переході від простої універсальної шкали критеріїв комп'ютерної безпеки (шість критеріїв С1, С2, В1, В2, В3, А1 для стандарту TCSEC, США, 1983 р. та десять критеріїв F-C1, F-C2, F-B1, F-B2, F-B3, F-1N, F-AV, F-DI, F-DC, F-DX для європейських критеріїв ITSEC, 1991 р.) до великої сукупності часткових критеріїв (160 - для Федеральних критеріїв FCITS, США, 1992 р., 70 – для Канадських критеріїв CTCPEC, 1993 р., 280 – для Єдиних міжнародних критеріїв CCITSE, 1996 р.). Цей кращий досвід розвитку міжнародних критеріїв (європейських ITSEC та канадських CTCPEC) було враховано при розробці вітчизняних критеріїв. Так, в нормативних документах з питань технічного захисту інформації від несанкціонованого доступу Департаменту СТСЗІ Служби безпеки України, презентація яких відбулась в 1999 р., таких часткових критеріїв було визначено 110 [1, 2, 4 – 7].

Друга зміна була реалізована в канадських критеріях і полягала в концептуальному визначенні основної універсальної компоненти безпеки – "тег" (tag). Поняття "тег" визначає сукупність атрибутів безпеки, асоційованих з користувачем, процесом або об'єктом. У вітчизняних НД ТЗІ 2.5-004-99 це більш вдало й інформативно реалізовано шляхом регламентування та визначення в простому таблично-текстовому форматі низки так званих "профільних" послуг безпеки різних видів та рівнів (наприклад, послуг конфіденційності довірчої КД рівнів 1...4 та конфіденційності адміністративної КА рівнів 1…4, послуг цілісності довірчої ЦД рівнів 1…3 та цілісності адміністративної ЦА рівнів 1…3, послуг доступності інформації щодо використання ресурсів виду ДР рівнів 1…3, послуг спостереженості інформації та ресурсів щодо цілісності комплексу засобів захисту НЦ рівнів 1…3, щодо реєстрації НР рівнів 1…5, тощо). Кількість, види та рівні профільних послуг безпеки визначають собою так званий стандартний функціональний профіль захищеності інформації (СПЗІ) в автоматизованих (комп'ютерних) системах (АС, КС) різних класів та підкласів. А певний склад СПЗІ вже функціонально регулює стан безпеки інформації в певній захищеній АС, КС [1 – 2].

У провідних західних країнах вже створені каталоги профілів захисту та проектів захисту (профілі захисту плюс специфікації функцій захисту) як обов'язкових нормативних документів щодо стандартизації усіх компонентів ІТ-продуктів (продуктів інформаційних технологій), тобто стандартизації апаратних, програмних та спеціальних засобів, що реалізують функції захисту інформації в комп'ютерних системах. В

Україні профілі та проекти захисту реалізовано в нормативних документах НД ТЗІ 2.5-005-99, НД ТЗІ 2.5-004-99 у вигляді вже визначених вище функціональних стандартних профілів захищеності інформації та "профільних" послуг безпеки як базової низки СПЗІ – всього 90 СПЗІ, у тому числі 22 – для класу 1, 34 – для класу 2 та 34 – для класу 3 [1 – 2, 5 – 6].

Саме тому в Україні доцільна подальша розробка базової низки СПЗІ у вигляді Національного каталогу стандартних профілів захищеності інформації, у тому числі для гармонізації його з профілями та проектами захисту в міжнародних критеріях комп'ютерної безпеки.

Доцільно визначити наступне щодо критеріальних підходів та самого змісту і таксономії (класифікації та семантичної і кількісної змістовності) повної низки складових національного каталогу стандартних профілів захищеності інформації в АС, КС згідно з регламентованими вимогами НД ТЗІ 2.5-005-99, НД ТЗІ 2.5-004-99 [1 – 2]. При експертній оцінці стану безпеки інформації в АС, КС пропонується використовувати наступні узагальнені критерії замість множини 110 часткових критеріїв та наступні методологічні підходи [5, 6].

1. По-перше, визначати рейтинг Е профілю захищеності, який чисельно оцінюється імовірністю надання повної низки регламентованих елементарних функціональних (ПБ-ЕФ), умовно-необхідних (ПБ-УН) та елементарних гарантійних (ПБ-ЕГ) послуг безпеки для кожної обраної профільної послуги безпеки (ПБ-П) в певній АС, КС. Рейтинг Е визначається як функціонал F послуг безпеки ПБ-ЕФ, ПБ-УН, ПБ-ЕГ.

2. По-друге, визначати ризик безпеки R інформації в АС, КС, який чисельно оцінюється імовірністю ненадання жодної послуги безпеки із повної низки регламентованих 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 АС (КС).

Ризик безпеки визначається як функціонал F послуг безпеки ПБ-П, ПБ-ЕФ, ПБ-УН, ПБ-ЕГ та рівнів гарантії безпеки Г-1....Г-7.

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

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

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

Програмно-математична реалізація наведених співвідношень досить складна і вирішується різними програмно-математичними методами шляхом обчислення певних ймовірностей – граф (дерево) подій, співвідношення числа успішних подій до їх можливої повної низки, формули Байеса, але при цьому за основу має прийматися обов'язкове дотримання вимог елементарних послуг безпеки, регламентованих в НД ТЗІ 2.5-004-99, тобто послуг безпеки ПБ-ЕФ, ПБ-УН, ПБ-ЕГ [5]. Для кращого фізичного тлумачення ймовірних подій та надання певних послуг безпеки визначаємо другий варіант кількісної оцінки - співвідношення числа успішних подій до їх можливої повної низки.

3. По-третє, визначати певний рівень гарантії безпеки Г-1…Г-7 для певного рейтингу Е чи ризику безпеки R обраних профілів захищеності інформації СПЗІ для захищених АС, КС певного класу та підкласу.

4. Розробка Delphi-програми "Генерація національного каталогу стандартних профілів захищеності інформації в автоматизованих системах" (програма КСПЗІ) на цей час виконується як подальше удосконалення базової моделі експертної системи [5].

Мета програми КСПЗІ – одержати у базі даних повну низку стандартних профілів захищеності інформації згідно з вимогами НД ТЗІ 2.5-005-99, НД ТЗІ 2.5-004-99. Повна низка повинна містити наступні низки профілів захищеності за класами та підкласами АС.

4.1. Повна низка профілів захищеності інформації для АС класу 1 (профільні послуги безпеки по одній з кожного виду НР-1…-5, НИ-1…-3, НК-1…-2, НО-1…-3, НЦ-1…-3, НТ-1…-3 плюс профільні послуги безпеки підкласу АС):

4.1.1. Каталог профілів захищеності для АС підкласу «К» (профільні послуги безпеки по одній з кожного виду КД-1…-4, КА-1…-4, КО-1, КК-1…-3, КВ-1…-4);

4.1.2. Каталог профілів захищеності для АС підкласу «Ц» (профільні послуги безпеки по одній з кожного виду ЦД-1…-4, ЦА-1…-4, ЦО-1…-2, ЦВ-1…-3);

4.1.3. Каталог профілів захищеності для АС підкласу «Д» (профільні послуги безпеки по одній з кожного виду ДР-1…-3, ДС-1…-3, ДЗ-1…-3, ДВ-1…-3);

4.1.4. Каталог профілів захищеності для АС підкласу «КЦ» (профільні послуги безпеки по одній з кожного виду КД-1…-4, КА-1…-4, КО-1, КК-1…-3, КВ-1…-4, ЦД-1…-4, ЦА-1…-4, ЦО-1…-2, ЦВ-1…-3);

4.1.5. Каталог профілів захищеності для АС підкласу «КД» (профільні послуги безпеки по одній з кожного виду КД-1…-4, КА-1…-4, КО-1, КК-1…-3, КВ-1…-4, ДР-1…-3, ДС-1…-3, ДЗ-1…-3, ДВ-1…-3);

4.1.6. Каталог профілів захищеності для АС підкласу «ЦД» (профільні послуги безпеки по одній з кожного виду ЦД-1…-4, ЦА-1…-4, ЦО-1…-2, ЦВ-1…-3, ДР-1…-3, ДС-1…-3, ДЗ-1…-3, ДВ-1…-3);

4.1.7. Каталог профілів захищеності для АС підкласу «КЦД» (профільні послуги безпеки по одній з

кожного виду КД-1…-4, КА-1…-4, КО-1, КК-1…-3, КВ-1…-4, ЦД-1…-4, ЦА-1…-4, ЦО-1…-2, ЦВ-1…-3, ДР-1…-3, ДС-1…-3, ДЗ-1…-3, ДВ-1…-3);

4.2. Повна низка профілів захищеності інформації для АС класу 2 та 3 (профільні послуги безпеки по одній з кожного виду НР-1…-5, НИ-1…-3, НК-1…-2, НО-1…-3, НЦ-1…-3, НТ-1…-3, НВ-1…-3, НА-1…-2, НП-1…-2 плюс профільні послуги безпеки підкласу АС):

4.2.1. Каталог профілів захищеності для АС підкласу «К» (профільні послуги безпеки по одній з кожного виду КД-1…-4, КА-1…-4, КО-1, КК-1…-3, КВ-1…-4);

4.2.2. Каталог профілів захищеності для АС підкласу «Ц» (профільні послуги безпеки по одній з кожного виду ЦД-1…-4, ЦА-1…-4, ЦО-1…-2, ЦВ-1…-3);

4.2.3. Каталог профілів захищеності для АС підкласу «Д» (профільні послуги безпеки по одній з кожного виду ДР-1…-3, ДС-1…-3, ДЗ-1…-3, ДВ-1…-3);

4.2.4. Каталог профілів захищеності для АС підкласу «КЦ» (профільні послуги безпеки по одній з кожного виду КД-1…-4, КА-1…-4, КО-1, КК-1…-3, КВ-1…-4, ЦД-1…-4, ЦА-1…-4, ЦО-1…-2, ЦВ-1…-3);

4.2.5. Каталог профілів захищеності для АС підкласу «КД» (профільні послуги безпеки по одній з кожного виду КД-1…-4, КА-1…-4, КО-1, КК-1…-3, КВ-1…-4, ДР-1…-3, ДС-1…-3, ДЗ-1…-3, ДВ-1…-3);

4.2.6. Каталог профілів захищеності для АС підкласу «ЦД» (профільні послуги безпеки по одній з кожного виду ЦД-1…-4, ЦА-1…-4, ЦО-1…-2, ЦВ-1…-3, ДР-1…-3, ДС-1…-3, ДЗ-1…-3, ДВ-1…-3);

4.2.7. Каталог профілів захищеності для АС підкласу «КЦД» (профільні послуги безпеки по одній з кожного виду КД-1…-4, КА-1…-4, КО-1, КК-1…-3, КВ-1…-4, ЦД-1…-4, ЦА-1…-4, ЦО-1…-2, ЦВ-1…-3, ДР-1…-3, ДС-1…-3, ДЗ-1…-3, ДВ-1…-3);

5. Проведені дослідження показують, що повна низка СПЗІ (для класів 1. 2. 3 АС, КС та їх підкласів К, Ц, Д, КЦ, КД, КЦД) містить певну кількість математичних сполучень, для генерації яких програмними Delphi-методами на ПЕОМ потрібні досить великі обчислювальні ресурси щодо високої швидкодії та пам‘яті (понад 700 млрд. варіантів перебору та записів в базу даних та базу знань експертної системи). Наприклад, для ПЕОМ з операційною системою Windows 2000 та з тактовою частотою 800 мГц потрібно її безперервної роботи протягом понад 58 годин.

6. При генерації каталогу СПЗІ визначається, що послуги безпеки спостереженості інформації та ресурсів ПБ-Н займають найбільш пріоритетне і специфічне місце в будь-якій захищеній АС, КС. Апріорі визначається, що жодна АС, КС не може вважатися захищеною, якщо, по-перше, самі засоби захисту є об‘єктом НСД та, по-друге, якщо в АС, КС відсутні ідентифікація, автентифікація і контроль за діями користувачів та керованість інформацією і ресурсами АС, КС.

Саме тому послуги спостереженості визначаються обов‘язковими для всіх СПЗІ – шість послуг безпеки НР, НИ, НК, НО, НЦ, НТ для АС, КС класу 1 та дев‘ять послуг безпеки НР, НИ, НК, НО, НЦ, НТ, НВ, НА, НП для АС, КС класу 2, 3.

Повна низка сполучень профільних послуг безпеки спостереженості Н різних видів (НР, НИ, НК, НО, НЦ, НТ, НВ, НА, НП) та рівнів (1…5) оцінюється за наступними співвідношеннями.

6.1. Число сполучень С (6Н) послуг спостереженості з їх низки із шести послуг безпеки видів НР, НИ, НК, НО, НЦ, НТ для АС, КС класу 1 оцінюється за співвідношенням:

$$C\ (6H) = n1*n2*n3*n4*n5*n6, \qquad (3)$$

де n1 – кількість рівнів послуги безпеки (ПБ) реєстрації НР (НР-1…НР-5); n2 – кількість рівнів ПБ ідентифікації й автентифікації НИ (НИ-1…НИ-3); n3 – кількість рівнів ПБ достовірний канал НК (НК-1…НК-2); n4 – кількість рівнів ПБ розподілу обов‘язків НО (НО-1…НО-3); n5 – кількість рівнів ПБ цілісності комплексу засобів захисту НЦ (НЦ-1…НЦ-3); n6 – кількість рівнів ПБ самотестування НТ (НТ-1…НТ-3).

Так, повна низка сполучень послуг спостереженості з їх низки з шести послуг безпеки по одній з кожного виду складає С (6Н) = 5*3*2*3*3*3 = 810 комбінацій.

6.2. Число сполучень С (9Н) послуг спостереженості з їх низки з дев‘яти послуг безпеки видів НР, НИ, НК, НО, НЦ, НТ, НВ, НА, НП для АС, КС класу 2, 3 оцінюється співвідношенням:

$$C\ (9H) = C\ (6H)*n7*n8*n9, \qquad (4)$$

де n7 – кількість рівнів ПБ ідентифікації й автентифікації при обміні НВ (НВ-1…НВ-3); n8 – кількість рівнів ПБ автентифікації відправника НА (НА-1…НА-2); n9 – кількість рівнів ПБ автентифікації отримувача НП (НП-1…НП-2).

Так, повна низка сполучень послуг спостереженості з їх низки з дев‘яти послуг безпеки по одній з кожного виду складає С (9Н) = 810*3*2*2 = 9720 комбінацій.

7. Генерація СПЗІ для підкласів К, Ц, Д, КЦ, КД, ЦД, КЦД захищених АС, КС класу 1, 2, 3 має певні особливості.

7.1. По-перше, визначення їх повної низки підпорядковується іншим математичним співвідношенням, ніж

(3) – (4). Це обумовлено наступним. За співвідношеннями (3) – (4) обчислюється низка шісток та дев'яток базових послуг спостереженості Н усіх їх видів та рівнів, їх мінімальне значення дорівнює 1. Навпаки, для базових послуг безпеки конфіденційності К, цілісності Ц, доступності Д умови формування стандартних профілів захищеності зовсім інші – кожна із них може надаватись чи ні та при надаванні поступово збільшуватись від однієї профільної послуги до максимальної їх кількості за видами та рівнями, їх мінімальне значення вже дорівнює 0. Математичні співвідношення мають наступний вигляд:

$$С (К) = (К1+1)*(К2+1)*(К3+1)*(К4+1)*(К5+1) – 1, \quad (5)$$

$$С (Ц) = (Ц1+1)*(Ц2+1)*(Ц3+1)*(Ц4+1) – 1, \quad (6)$$

$$С (Д) = (Д1+1)*(Д2+1)*(Д3+1)*(Д4+1) – 1, \quad (7)$$

де С (К) – повна низка СПЗІ для базової послуги безпеки конфіденційності К; К1 – кількість рівнів профільних послуг виду КД (0…4); К2 – кількість рівнів профільних послуг виду КА (0…4); К3 – кількість рівнів профільних послуг виду КО (0…1); К4 – кількість рівнів профільних послуг виду КК (0…3); К5 – кількість рівнів профільних послуг виду КВ (0…4); С (Ц) - повна низка СПЗІ для базової послуги безпеки цілісності Ц; Ц1 – кількість рівнів профільних послуг виду ЦД (0…3); Ц2 – кількість рівнів профільних послуг виду ЦА (0…4); Ц3 – кількість рівнів профільних послуг виду ЦО (0…2); Ц4 – кількість рівнів профільних послуг виду ЦВ (0…3); С (Д) – повна низка СПЗІ для базової послуги безпеки доступності Д; Д1 – кількість рівнів профільних послуг виду ДР (0…3); Д2 – кількість рівнів профільних послуг виду ДС (0…3); Д3 – кількість рівнів профільних послуг виду ДЗ (0…3); Д4 – кількість рівнів профільних послуг виду ДВ (0…3).

Розрахунки за формулами (5) – (7) показують, що повна низка СПЗІ для базових послуг безпеки приймає наступні значення:

$$С (К) = ((4+1)*(4+1)*(1+1)*(3+1)*(4+1)) – 1 = 1000 – 1 = 999; \quad (8)$$

$$С (Ц) = ((4+1)*(4+1)*(2+1)*(3+1)) – 1 = 300 – 1 = 299; \quad (9)$$

$$С (Д) = ((3+1)*(3+1)*(3+1)*(3+1)) – 1 = 256 – 1 = 255. \quad (10)$$

7.2. По-друге, повний склад профільних послуг безпеки для варіантів СПЗІ підкласів К, Ц, Д, КЦ, КД, ЦД, КЦД має певні особливості. Вони полягають у тім, що апріорі до базової низки СПЗІ послуг безпеки 6Н, 9Н повинні додаватись, крім повної низки усіх варіантів елементарних функціональних послуг ПБ-ЕФ для кожної з профільних послуг К, Ц, Д, КЦ, КД, ЦД, КЦД, їх необхідно-умовні послуги ПБ-УН (див. вигляд меню "Умови" рис. 1 – 2).

7.3. По-третє, повна низка СПЗІ для АС, КС класу 1 та підкласу К, тобто значення показника С (6Н) = 810 комбінацій, має, згідно з п. 7.2 та таблицею рис.1, доповнюватись ще двома комбінаціями СПЗІ: КВ-3 + (НВ-1, НЦ-1, НО-1) та КВ-4 + (НВ-1, НЦ-1, НО-1, НР-1, Г-3). Іншими словами, до повної низки послуг спостереженості 6Н необхідно, начебто, додавати сьому послугу НВ-1 з низки послуг 9Н (6Н + (НВ, НА, НП)). З урахуванням цього для класу 1 та підкласу К визначається, що начебто С (6Н) = 810 + 2 = 812. Надалі ми впевнимося, що це вірно і невірно.

Аналогічно для класу 1 та підкласу Ц необхідно начебто додавати до шістки сьому послугу НВ-1 для послуги ЦВ-3 (рис. 2), тоді С (6Н) = 810 + 1 = 811.

Але ретельний аналіз даних меню "Умови" (рис. 1 – 2) свідчить про наступне.

По-перше, генерація стандартних профілів захищеності інформації (СПЗІ) для АС, КС класу 1 та підкласу К з профільними послугами безпеки КВ-3, КВ-4 має істотну особливість.

Вона полягає в тому, що до базової низки СПЗІ С (6Н) = 810 сполучень з шести послуг спостереженості видів НР, НИ, НК, НО, НЦ, НТ необхідно для сполучень з КВ-3, КВ-4 начебто додавати сьому профільну послугу безпеки НВ-1. Це обумовлено тим, що НВ-1 є умовно-необхідною послугою для реалізації профільних послуг КВ-3, КВ-4 в СПЗІ підкласу К класу 1 АС, КС (табл.. на рис. 1, колонка "Необхідні умови"). Але послуга безпеки спостереженості інформації і ресурсів НВ-1 (помічено "НВ") належить до складу СПЗІ АС, КС класу 1, 2 (НР, НИ, НК, НО, НЦ, НТ, "НВ", НА, НП). Аналогічно це справедливо для профільної послуги ЦВ-3 (табл..на рис. 2, колонка "Необхідні умови").

По-друге, повна низка СПЗІ для шістки послуг завжди є константою С (6Н) = 810.

Ми розглянули порядок формування та математичні співвідношення щодо стандартних профілів захищеності окремо для послуг безпеки Н, К, Ц, Д. Це значно зменшує потрібні обчислювальні ресурси щодо швидкодії та пам'яті. Але це ще не остаточні, а тільки проміжні результати. Остаточну повну низку стандартних профілів захищеності певного класу та підкласу АС треба сформувати саме з проміжних результатів наступним шляхом.

По-перше, формується окремо повна низка СПЗІ для АС класу 1 та всіх підкласів, для чого використовується повна низка комбінацій шістки послуг безпеки Н та повні низки послуг безпеки К, Ц, Д, КЦ, КД, ЦД, КЦД. При такому підході щодо послуг спостереженості Н математичні співвідношення остаточної повної низки СПЗІ для АС класу 1 мають наступний вигляд:

$$C(1.К) = C(6Н)*C(К), \quad (11)$$
$$C(1.Ц) = C(6Н)*C(Ц), \quad (12)$$
$$C(1.Д) = C(6Н)*C(Н) \quad (13)$$
$$C(1.КЦ) = C(6Н)*C(К)*C(Ц), \quad (14)$$
$$C(1.КД) = C(6Н)*C(КД), \quad (15)$$
$$C(1.ЦД) = C(6Н)*C(ЦД), \quad (16)$$
$$C(1.КЦД) = C(6Н)*C(КЦД), \quad (17)$$

де С (1.К) – повна низка СПЗІ для АС класу 1 підкласу К; С (1.Ц) – повна низка СПЗІ для АС класу 1 підкласу Ц; С (1.Д) – повна низка СПЗІ для АС класу 1 підкласу Д; С (1.КЦ) – повна низка СПЗІ для АС класу 1 підкласу КЦ; С (1.КД) – повна низка СПЗІ для АС класу 1 підкласу КД; С (1.КЦД) – повна низка СПЗІ для АС класу 1 підкласу КЦД; С (К) – повна низка СПЗІ для базової послуги безпеки конфіденційності К; С (Ц) –- повна низка СПЗІ для базової послуги безпеки цілісності Ц; С (Д) – повна низка СПЗІ для базової послуги безпеки доступності Д; С (КЦ) – повна низка СПЗІ для базових послуг безпеки К та Ц; С (КД) – повна низка СПЗІ для базових послуг безпеки К та Д; С (ЦД) – повна низка СПЗІ для базових послуг безпеки Ц та Д; С (КЦД) – повна низка СПЗІ для базових послуг безпеки К, Ц та Д.

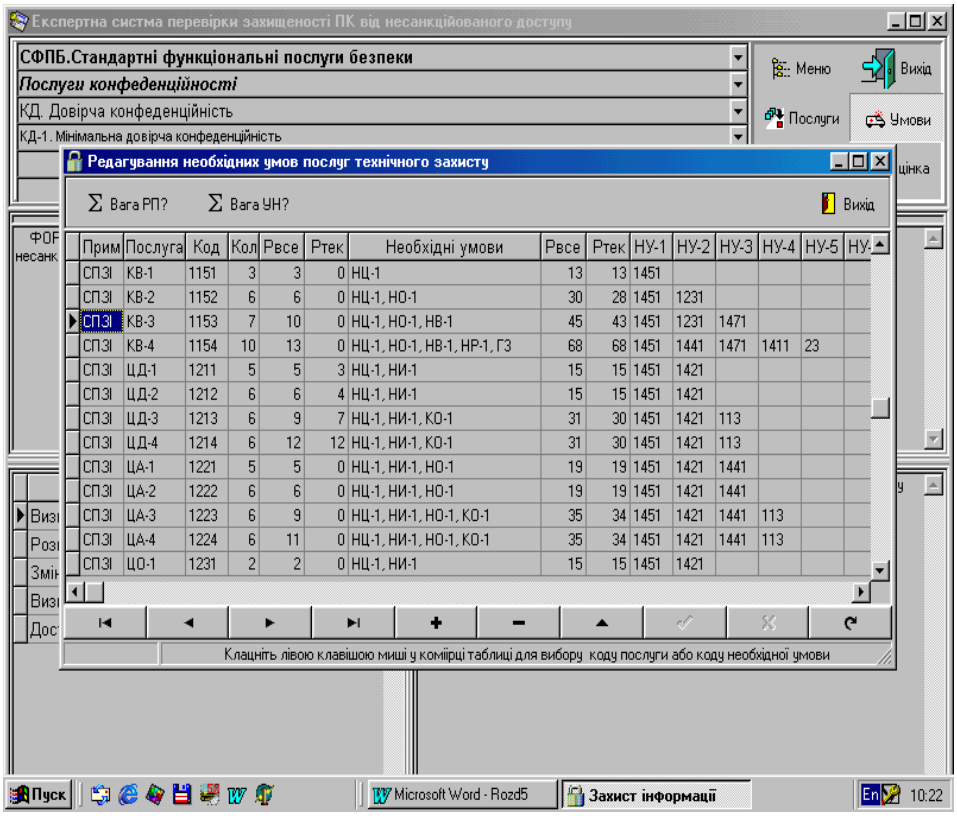

Рисунок 1 – Меню "Умови" експертної системи "Торсіон-1" з маркером на СПЗІ з КВ-3, НВ-1

Розрахунки за формулами (16) – (22) показують, що повна низка СПЗІ для АС класу 1 та всіх підкласів приймає наступні значення:

$$C(1.К) = C(6Н)*C(К) = 810*999 = 809190; \quad (18)$$
$$C(1.Ц) = C(6Н)*C(Ц) = 810*299 = 242190; \quad (19)$$
$$C(1.Д) = C(6Н)*C(Д) = 810*255 = 206550; \quad (20)$$
$$C(1.КЦ) = C(6Н)*C(КЦ) = C(6Н)*C(К)*C(Ц) = 810*999*299 = 241947810; \quad (21)$$
$$C(1.КД) = C(6Н)*C(К)*C(Д) = C(6Н)*C(К)*C(Д) = 810*999*255 = 206343450; \quad (22)$$
$$C(1.ЦД) = C(6Н)*C(ЦД) = C(6Н)*C(Ц)*C(Д) = 810*299*255 = 61758450; \quad (23)$$
$$C(1.КЦД) = C(6Н)*C(К)*C(Ц)*C(Д) = 810*999*299*255 = 61696691550. \quad (24)$$

По-друге, формується окремо повна низка СПЗІ для АС класів 2, 3 та всіх підкласів, для чого використовується повна низка комбінацій дев'ятки послуг безпеки Н та повні низки послуг безпеки К, Ц, Д, КЦ, КД, ЦД, КЦД. Математичні співвідношення остаточної повної низки СПЗІ для АС класів 2, 3 мають наступний вигляд:

$$C(2.К) = C(6Н)*C(К), \quad (25)$$

$$C(2.Ц) = C(6Н)*C(Ц), \quad (26)$$
$$C(2.Д) = C(6Н)*C(Н) \quad (27)$$
$$C(2.КЦ) = C(6Н)*C(К)*C(Ц), \quad (28)$$
$$C(2.КД) = C(6Н)*C(КД), \quad (29)$$
$$C(2.ЦД) = C(6Н)*C(ЦД), \quad (30)$$
$$C(2.КЦД) = C(6Н)*C(КЦД), \quad (31)$$

де C (2.К) – повна низка СПЗІ для АС класів 2, 3 підкласу К; C (2.Ц) – повна низка СПЗІ для АС класів 2, 3 підкласу Ц; C (2.Д) – повна низка СПЗІ для АС класів 2, 3 підкласу Д; C (2.КЦ) – повна низка СПЗІ для АС класів 2, 3 підкласу КЦ; C (2.КД) – повна низка СПЗІ для АС класів 2, 3 підкласу КД; C (2.КЦД) – повна низка СПЗІ для АС класів 2, 3 підкласу КЦД; C (К) – повна низка СПЗІ для базової послуги безпеки конфіденційності К; C (Ц) – повна низка СПЗІ для базової послуги безпеки цілісності Ц; C (Д) – повна низка СПЗІ для базової послуги безпеки доступності Д; C (КЦ) – повна низка СПЗІ для базових послуг безпеки К та Ц; C (КД) – повна низка СПЗІ для базових послуг безпеки К та Д; C (ЦД) – повна низка СПЗІ для базових послуг безпеки Ц та Д; C (КЦД) – повна низка СПЗІ для базових послуг безпеки К, Ц та Д.

Розрахунки за формулами (30) – (36) показують, що повна низка СПЗІ для АС класів 2, 3 та всіх підкласів приймає наступні значення:

$$C(2.К) = C(9Н)*C(К) = 9720*999 = 9710280; \quad (32)$$
$$C(2.Ц) = C(9Н)*C(Ц) = 9720*299 = 2906280; \quad (33)$$
$$C(2.Д) = C(9Н)*C(Д) = 9720*255 = 2478600; \quad (34)$$
$$C(2.КЦ) = C(9Н)*C(КЦ) = C(6Н)*C(К)*C(Ц) = 9720*999*299 = 2903373720; \quad (35)$$
$$C(2.КД) = C(9Н)*C(К)*C(Д) = C(9Н)*C(К)*C(Д) = 9720*999*255 = 2476121400; \quad (36)$$
$$C(2.ЦД) = C(9Н)*C(ЦД) = C(9Н)*C(Ц)*C(Д) = 9720*299*255 = 741101400; \quad (37)$$
$$C(2.КЦД) = C(9Н)*C(К)*C(Ц)*C(Д) = 9720*999*299*255 = 740360298600. \quad (38)$$

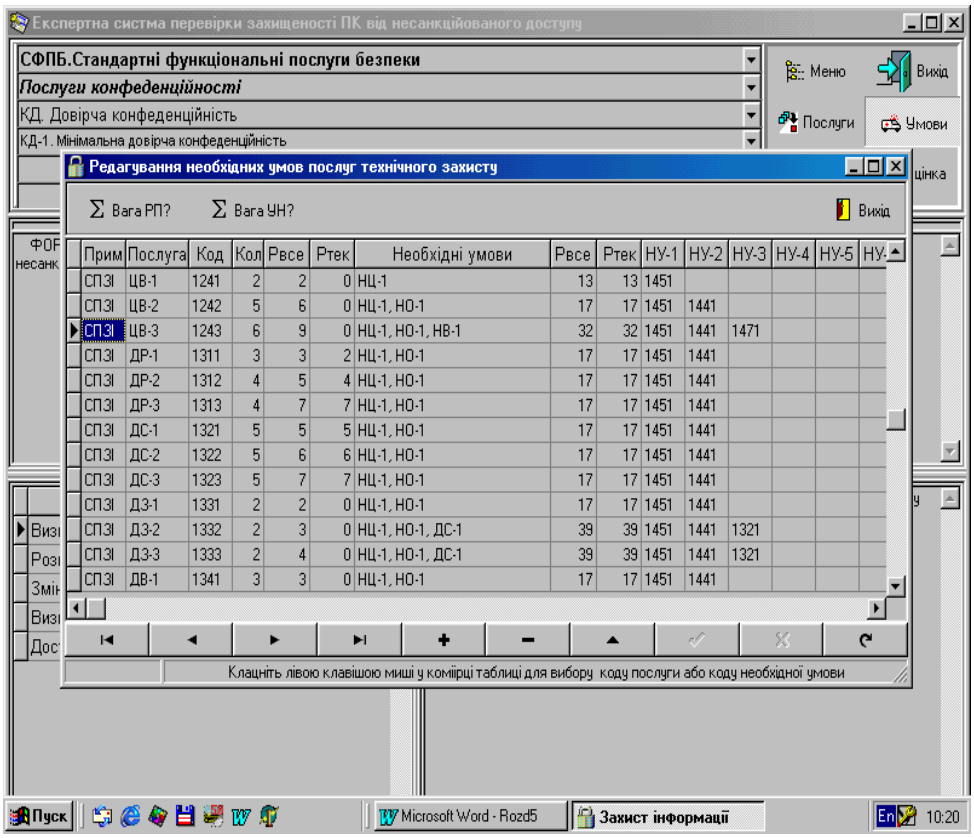

Рисунок 2 – Меню "Умови" експертної системи "Торсіон – 1" з маркером на СПЗІ з ЦВ-3, НВ-1.

Розрахунки повної низки СПЗІ для АС усіх класів та підкласів показують, що для їх формування потрібні занадто великі обчислювальні ресурси щодо швидкодії та пам'яті ПЕОМ, які недоступні сучасним ПЕОМ. Так, максимальне значення повної низки СПЗІ формується для підкласу КЦД АС класу 2, 3 і складає понад 740 мільярдів стандартних профілів захищеності! Перед реальною генерацією такої низки СПЗІ необхідно

ввести певні обмеження щодо їх кількості. Для цього можна використати наступний підхід.

Він полягає в тому, що повна низка СПЗІ генерується тільки за значеннями ризику безпеки R від його максимального до мінімального значення та окремо для кожної послуги безпеки К, Ц, Д, Н. Це дає можливість сформувати низки СПЗІ для кожного підкласу АС класів 1, 2, 3.

Таким чином, на основі викладеного вище щодо постановки задачі та за результатами проведених досліджень [5] можна сформулювати наступні узагальнені правила формування (генерації) стандартних функціональних профілів захищеності інформації в АС (КС).

Правило СПЗІ – 1. Базовою необхідною умовою для формування стандартного профілю захищеності інформації АС (КС) першого класу визначаються шістка послуг безпеки спостереженості інформації і ресурсів видів НР, НИ, НК, НО, НЦ, НТ та всіх їх рівнів. Підвищення рівня послуг безпеки забезпечує підвищення рівня захисту інформації і ресурсів АС, КС.

Правило СПЗІ – 2. Базовою необхідною умовою для формування стандартного профілю захищеності інформації АС (КС) другого, третього класу визначаються дев‘ятка послуг безпеки спостереженості інформації і ресурсів видів НР, НИ, НК, НО, НЦ, НТ, НВ, НА, НП та всіх їх рівнів. Підвищення рівня послуг безпеки забезпечує підвищення рівня захисту інформації і ресурсів АС (КС).

Правило СПЗІ – 3. Повна підготовча низка стандартних профілів захищеності інформації для кожного підкласу К, Ц, Д, КЦ, КД, ЦД, КЦД захищеної АС (КС) першого класу формується сумуванням кожного сполучення – шістки послуг безпеки спостереженості видів НР, НИ, НК, НО, НЦ, НТ і всіх їх рівнів з кожним сполученням послідовно збільшуваних за видами і рівнями одночасно наданих послуг безпеки: конфіденційності К, цілісності Ц, доступності Д, конфіденційності і цілісності КЦ (двійка сполучень), конфіденційності і доступності КД (двійка сполучень), цілісності і доступності ЦД (двійка сполучень), конфіденційності, цілісності і доступності КЦД (трійка сполучень). Підвищення кількості та рівня одночасно наданих послуг безпеки забезпечує підвищення рівня захисту інформації і ресурсів АС (КС).

Правило СПЗІ – 4. Повна остаточна низка стандартних профілів захищеності інформації для кожного підкласу К, Ц, Д, КЦ, КД, ЦД, КЦД захищеної АС (КС) першого, другого і третього класу формується додаванням до кожної профільної послуги безпеки кожного із сполучень, одержаних за правилами СПЗІ – 1, 2,.3, усіх функціональних і гарантійних послуг безпеки, регламентованих в необхідних умовах окремо для кожної із 22-х профільних послуг безпеки виду НР, НИ, НК, НО, НЦ, НТ, НВ, НА, НП, КД, КА, КО, КК, КВ, ЦД, ЦА, ЦО, ЦВ, ДР, ДС, ДЗ, ДВ всіх їх рівнів. Після додавання склад профілю захищеності може бути більше низки із 22-х профільних послуг безпеки, але не перевищувати 27 послуг безпеки включно з Г – 3.

Обмеження: при додаванні профільні послуги із необхідних умов не повинні дублюватись з аналогічними із підготовчої низки, сформованої по правилу СПЗІ-3, тільки по їх рівню, дублювання по виду профільної послуги безпеки допускається.

Правило СПЗІ – 5. Для кожного з підкласів кожного класу АС (КС) формується повна низка ієрархічних стандартних профілів захищеності інформації за правилам СПЗІ – 1, 2, 3, 4, яка може бути різною для кожного класу і підкласу АС (КС). Профілі вважаються ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (конфіденційності, цілісності і доступності). Наростання ступеня захищеності може досягатись як підсиленням певних профільних послуг безпеки, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг.

Правило СПЗІ – 6. Зростання ступеня захищеності інформації для кожного з підкласів кожного класу АС (КС) кількісно оцінюється трьома узагальненими критеріями: рейтингом Е стандартного профілю захищеності інформації, рівнем гарантії Г-1…Г-7 та ризиком R безпеки інформації. Більшість з часткових гарантійних та профільних послуг безпеки узагальнених критеріїв являють собою конкретизацію вимог щодо реалізації комплексу засобів захисту АС (КС) стандартів серії ДСТУ ISO 9000 і для їх тлумачення використовується термінологія з області керування якістю продукції (ДСТУ 3230-95). Повна низка профілів захищеності інформації на замовлення користувачів може упорядковуватись, сортуватись та скорочуватись шляхом групування її за зменшенням ризику безпеки з заданою його дискретністю і точністю.

Правило СПЗІ-7. Базовою компонентою моніторингу стану безпеки інформації в захищеній КС визначається ризик її безпеки. Він має поточне чи належне (задане) значення. Моніторинг здійснюється з метою автоматизованої чи автоматичної реалізації ризику безпеки, не менш належного (заданого) згідно з обраною політикою безпеки.

Моніторинг ризику безпеки здійснюється управлінням прийняття рішення щодо надання певного стандартного профілю захищеності інформації чи їх низки, що визначають і регламентують склад профільних послуг безпеки для реалізації обраної політики безпеки з використанням наступних елементів управління ресурсом захищеної КС (АС) і конфігурацією її апаратно-програмного забезпечення та ядра безпеки обчислювальної системи (комплексу засобів захисту, КЗЗ):

1. *об'єкт комп'ютерної системи* (product object, system object) – елемент ресурсу АС (КС), що знаходиться під керуванням КЗЗ і характеризується певними атрибутами і поводженням;
2. *об'єкт – процес* (process object) – виконувана в даний момент програма, яка повністю характеризується своїм контекстом (поточним станом регістрів обчислювальної системи, адресним простором, повноваженнями тощо);
3. *об'єкт – користувач* (user object) – подання фізичного користувача в АС (КС), що створюється в процесі входження користувача в систему і повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями тощо);
4. *пасивний об'єкт* (passive object) – об'єкт АС (КС), який в конкретному акті доступу виступає як пасивний компонент системи, над яким виконується дія і/або який служить джерелом чи приймальником інформації;
5. *потік інформації* (information flow) – передавання інформації від одного до іншого об'єкта АС (КС);
6. *ідентифікатор об'єкта КС* (object identifier) – унікальний атрибут об'єкта АС (КС), що дозволяє однозначно виділити даний об'єкт серед подібних;
7. *доступ до інформації* (access to information) – вид взаємодії двох об'єктів АС (КС), внаслідок якого створюється потік інформації від одного об'єкта до іншого і/або відбувається зміна стану системи;
8. *правила розмежування доступу; ПРД* (access mediation rules) – частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів;
9. *тип доступу* (access type) – суттєвість доступу до об'єкта, що характеризує зміст здійснюваної взаємодії, а саме: проведені дії, напрям потоків інформації, зміни в стані системи (наприклад, читання, запис, запуск на виконання, видалення, дозапис);
10. *запит на доступ* (access request) – звернення одного об'єкта АС (КС) до іншого з метою отримання певного типу доступу;
11. *санкціонований доступ до інформації* (authorized access to information) – доступ до інформації, що не порушує ПРД;
12. *несанкціонований доступ до інформації; НСД до інформації* (unauthorized access to information) – доступ до інформації, здійснюваний з порушенням ПРД;
13. *захист від несанкціонованого доступу; захист від НСД* (protection from unauthorized access) – запобігання або істотне утруднення несанкціонованого доступу до інформації;
14. *право доступу* (access right) – дозвіл або заборона здійснення певного типу доступу;
15. *повноваження* (privilege) – права користувача або процесу на виконання певних дій, зокрема на одержання певного типу доступу до об'єктів;
16. *керування доступом* (access control) – сукупність заходів з визначення повноважень і прав доступу, контролю за додержанням ПРД;
17. *розмежування доступу* (access mediation) – сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі ПРД можливості надання доступу;
18. *адміністратор безпеки* (security administrator) – адміністратор, відповідальний за дотримання політики безпеки;
19. *порушник* (user violator) – користувач, який здійснює несанкціонований доступ до інформації.

Висновки

1. Визначені підходи і правила щодо оцінки стану безпеки інформації за профілями її захищеності від загроз НСД в комп'ютерних (автоматизованих) системах є актуальними для подальшого удосконалення та реалізації вимог пакету нормативних документів з питань технічного захисту інформації від несанкціонованого доступу Департаменту СТСЗІ СБУ.

2. Для їх практичної реалізації необхідні подальші дослідження з метою розробки та створення (замість низки вже регламентованих 90 базових стандартних профілів захищеності інформації, наведених в НД ТЗІ 2.5-005-99) повного Національного електронного каталогу стандартних профілів захищеності інформації (СПЗІ) в АС (КС) усіх класів і підкласів. Аналогічні каталоги вже існують в провідних західних країнах. Але для цього потрібні занадто великі обчислювальні ресурси щодо пам'яті та високої швидкодії ПЕОМ. Саме тому на першому етапі доцільно створити електронний, а не паперовий каталог, який практично реалізувати неможливо при понад 700 міліардів СПЗІ (36).

3. При формуванні (генерації) повної низки СПЗІ виникає ще одна проблема. Вона полягає в тому, що для формування (генерації) повної низки СПЗІ потрібно $37.3*10^{12}$ байт пам'яті ПЕОМ! Але вихід все ж таки є – формувати (генерувати) повні низки СПЗІ окремо для кожного підкласу АС (КС) та для окремих діапазонів значень ризиків безпеки інформації в АС (КС). Але це вже окрема проблема щодо шляхів зменшення пам'яті ПЕОМ для бази даних електронного каталогу СПЗІ для усіх підкласів та класів АС (КС). Необхідні

нетрадиційні і нові рішення цих проблем.

4. Ще одна проблема виникає щодо тлумачення підкласів як реалізації СПЗІ з підвищеними вимогами для захисту АС (КС) від загроз конфіденційності (підклас К), цілісності Ц (підклас Ц), доступності Д (підклас Д) та їх сполучень КЦ, КД, ЦД, КЦД – у якому співвідношенні, з якою пріоритетністю повинні надаватися послуги безпеки К та інші, послуги безпеки Ц та інші, послуги безпеки Д та інші і так далі. Для цього необхідні нетрадиційні і нові рішення і цієї проблеми.

5. Стандартні профілі захищеності інформації СПЗІ визначають і регламентують не тільки функціональні, але і гарантійні послуги безпеки інформації і ресурсів в захищених АС (КС) певного класу та підкласу. Профіль захисту СПЗІ завжди задається технічним завданням на створення або комплексної системи захисту інформації, або просто певної захищеної АС (КС). Від нього найбільш суттєво залежить забезпечення ризику безпеки інформації та ресурсів АС (КС) – не більше заданого шляхом надання певної низки послуг безпеки К, Ц, Д, Н та їх певних рівнів. Але для вибору цих послуг безпеки та забезпечення ризику безпеки не більше заданого, безумовно, необхідно мати Каталог стандартних профілів захищеності інформації в АС (КС).

Література: ***1.*** *НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".* ***2.*** *НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу".* ***3.*** *А. Е. Ильницкий, В. В. Шорошев. Рекомендации по основам информационной безопасности согласно Единых критериев CCITSE (Common Criteria for Information Technology Security Evaluation). Журнал "Бизнес и безопасность". N 1, 1999.* ***4.*** *Шорошев В. В. Базова модель експертної системи та її використання для прийняття рішення щодо безпеки інформації в КС ОВС України. Науковий вісник НАВСУ, К. 2001.* ***5.*** *Ільніцький А. Ю., Шорошев В. В., Близнюк І. Л. Базова модель експертної системи оцінки безпеки інформації в КС ОВС України (Торсіон-1). Видавництво НАВСУ, К. 2003, с. 316.* ***6.*** *Шорошев В. В., Проскурін В .М., Маєвський Є. Л. Три узагальнених критерії замість сукупності часткових щодо експертної оцінки захищеності інформації від несанкціонованого доступу в автоматизованих (комп'ютерних) системах. Журнал "Зв'язок" № 5, 2003.* ***7.*** *Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 5, 1998. Международные стандарты безопасности компьютерных систем: эволюция развития, проблемы, рекомендации.*

УДК 621.391.82

ДО ПИТАННЯ ЗАХИСТУ СЛУЖБОВИХ ПРИМІЩЕНЬ ВІД ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ

Олександр Тиховод, Борис Хіміченко

Особливе конструкторське бюро "Шторм" при Національному технічному університеті України" КПІ"

Анотація: **Розглянуто дослідження, проведені ОКБ "Шторм" в рамках контролю службових приміщень від витоку мовної інформації акустичним та віброакустичним каналами.**

Summary: **This article deals with researches, were done at OCB "Storm" for check official premises from leaks oral information through acoustic, vibroacoustic channels.**

Ключові слова: **Розбірливість мови, співвідношення сигнал/завада, охоронна зона.**

I Вступ

Як відомо, концепція захисту мовної інформації базується на загальній концепції захисту, згідно з якою акустична інформація є захищеною від витоку контрольованим каналом, якщо у контрольованому діапазоні частот виконується нерівність

$$L_c - L_з + k = N_i , \qquad (1)$$

де L_c – рівень інформативного сигналу, $L_з$ – рівень завад, k – коефіцієнт, який враховує спеціальні методи обробки, N_i – норма категорії захисту.

Існують об`єктивні причини, що призводять до необхідності застосування активних методів захисту. Найголовніша з них є та, що за відсутності ефективно діючої охоронної зони приміщення апріорі є незахищеним від витоку мовної інформації віброакустичниим каналом.