УДК 681. 327:537.53

Миколенко В.В., Олешко Т.І., Хорошко В.О.

ЗАХИСТ ІНФОРМАЦІЇ У ЗАСОБАХ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ВІД ВИТОКУ ЗА РАХУНОК ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ

У останні роки особлива увага приділяється захисту інформації (ЗІ), що оброблюється у засобах обчислювальної техніки. Причому, це відноситься не тільки до великих і малих обчислювальних центрів, локальних обчислювальних мереж, але і до окремих ПЕОМ. Поряд із загальновідомими каналами витоку інформації для захисту ПЕОМ суттєвим є перехоплення побічних електромагнітних випромінювань (ПЕМВ).

При обробці засобами обчислювальної техніки конфіденційної інформації виникаючі ПЕМВ є небезпечними сигналами, і далі ми будемо оперувати цим поняттям.

Ефективність механізму захисту в значному ступені залежить від фіксації наявності та вимірювання параметрів небезпечного сигналу. Це в першу чергу відноситься до небезпечних сигналів побічного електромагнітного випромінювання і сигналі, присутніх при роботі засобів обчислювальної та оргтехніки. Наявність і рівень небезпечних сигналів контролюється при оцінці захищеності об'єкту або при визначенні ступеню радіоелектронного маскування об'єкту.

Небезпечні сигнали видобуваються шляхом прийому та аналізу їх при роботі технічних засобів передачі, обробки, зберігання та відображення інформації, і наводок що виникають у дротах, кабелях та інших токопровідних ланцюгах. При цьому небезпечним вважають сигнал, якщо він містить конфіденційну інформацію і може бути перехоплений зловмисником.

Небезпечні сигнали генеруються електронними пристроями, у тому числі і ПЕОМ, обумовлені протіканням різноманітних видів струмів. Джерелами небезпечних сигналів є елементи, вузли або токопровідні ланцюги технічного засобу з струмами і напругами небезпечних сигналів. Причому, ці пристрої генерують як магнітні, так і електромагнітні поля в широкому частотному спектрі, характер яких визначається призначенням, схемними рішеннями, потужністю пристрою, а також його конструкцією.

Канали витоку інформації можуть виникати унаслідок випромінювання небезпечних сигналів під час роботи ПЕОМ і внаслідок наведення цих сигналів у лініях зв'язку, колах електроживлення і заземлення, інших комунікаціях, що мають вихід за межі контрольованої території. Небезпечні сигнали можуть поширюватися на великі відстані і реєструватися засобами технічних розвідок за межами контрольованої території.

Витік інформації колами заземлення може виникнути за наявності рознесених точок заземлення інформативних кіл у випадку створення в різних точках системи заземлення різниці потенціалів і виникнення за рахунок цього струмів у колах заземлення, при великому значенні опору кола заземлення.

Рівень наводок визначається відстанню між джерелами випромінювання й апаратурою, що підпадає під вплив цих випромінювань, довжиною паралельного пробігу і величиною перехідного затухання ліній, напругою небезпечного сигналу в лінії та рівнем завад.

Застосування спеціальної техніки, призначеної для оцінки параметрів сигналу на фоні довільних завад вимагає повного і достатньо точного знання апріорних даних про характер небезпечного сигналу і завади. Повнота опріорного знання розуміється в сенсі повноти статистичного опису, інакше кажучи, у загальному випадку необхідно знати багатовимірні щільності імовірностей небезпечного сигналу і завади, а також засоби комбінації сигналу та завади, не завжди відомої в реальних ситуаціях.

Небезпечний або корисний розвідувальний сигнал у результаті впливу на нього неадитивних завад або через недостатність апріорних відомостей практично завжди відрізняється від сигналу, що очікується і на який налагоджена спеціальна апаратура. Недостатність або, вірніше кажучи, невизначеність апріорних даних найбільш характерна за наявності штучних завад протидії або радіоелектронного маскування об'єкту [1].

Характер поля змінюється в залежності від відстані до пристрою перехоплення. Якщо ця відстань значно менше довжини хвилі електромагнітного сигналу ($r << \lambda$) поле має явно виражений магнітний або електричний характер, а в дальній зоні ($r >> \lambda$) поле носить явний електромагнітний характер і поширюється у виді плоскої хвилі, енергія якої ділиться порівну між електричною і магнітною складовими. Тому джерела ПЕМВ прийнято підрозділяти на низькочастотні і високочастотні, до яких і відносяться ПЕОМ. Застосування в них імпульсних сигналів прямокутної форми призводить до того, що в спектрі випромінювань є компоненти з частотами до декількох гигагерц. Хоча енергетичний спектр сигналів убуває з ростом частот, але ефективність при цьому збільшується і рівень випромінювань може залишатися постійним.

Важливим чинником є оцінка рівня ПЕМВ, яка провадиться з точки зору відповідності цих рівнів нормам і вимогам [2]: санітарно-гігієнічні норми; норми електромагнітної сумісності; норми і вимоги по ЗІ від витоку через ПЕМВ.

У залежності від того, відповідність яким нормам потрібно встановити, використовуються ті або інші прилади, методи і методики проведення вимірів.

Варто зауважити, що норми на рівні електромагнітних випромінювань із погляду електромагнітної сумісності, а також методики і прилади не можуть бути використані при вирішенні задач ЗІ.

Основними джерелами ПЕМВ є в ПЕОМ дисплей і з`єднувальні кабелі [3]. Якщо методи зменшення випромінювань кабелів відомі, то боротьба з ПЕМВ в дисплеях дуже актуальна проблема.

Якщо на екрані дисплея відображається інформація, що не має повторень, то відеосигнал у першому наближенні можна вважати випадковим, а енергетичний спектр такого сигналу буде мати вигляд:

$$S_x(f) = A\left(\frac{\sin \pi f T_\delta}{\pi f T_\delta}\right)^2,$$

де T_δ - тривалість одного біта відеосигналу, A - амплітуда сигналу, що є функцією числа елементів зображення.

Практично відеосигнал має кінцевий час T_i переходу від одного стану в інший, тому реальний енергетичний спектр описується виразом з урахуванням [1]:

$$S_x(f) = S_x(f)\frac{1}{(\pi f T_i)^2 + 1} = A\left(\frac{\sin \pi f T_\delta}{\pi f T_\delta}\right)^2 \frac{1}{(\pi f T_i)^2 + 1},$$

де останній множник являє собою частотну характеристику ФНЧ із граничною частотою $f_{нч}=1/\pi T_i$. Огинаюча енергетичного спектру практично постійна до частоти $f_0 = 1/\pi T_\delta$, починаючи з якої вона убуває зі швидкістю порядку -20дБ/декаду до $f_{нч}$ [3]. На частотах більш високих, чим $f_{нч}$, швидкість убування складає -40 дБ/декаду.

Проте в ланцюгах дисплея є присутніми не тільки відеосигнали, але і токові імпульси, що повторюються. Отже, енергетичний спектр відеосигналу містить гармоніки,

інтенсивність яких убуває з ростом частоти. Проведені дослідження показали, що саме ПЕМВ дисплея є основним каналом витоку інформації при експлуатації ПЕОМ.

Отже, будь-який сигнал, що входить у ПЕМВ можна характеризувати визначеним набіром параметрів $x_1, x_2, ..., x_n$, кожний із яких приймає значення у відповідних діапазонах $Дx_1, Дx_2, ..., Дxn$. Для наочності можна уявити деякий n-мірний просторовий прямокутний паралелепіпед, ребра якого $Дx_1, Дx_2, ..., Дxn$, і при цьому кожний окремий сигнал у малому паралелепіпеді відбивається точкою з координатами $x_1, x_2, ..., x_n$...

Якщо електронна обстановка в даній точці простору характеризується числом випромінювань N із параметрами, що лежать у зазначених діапазонах, то в паралелепіпеді буде відзначено N точок, кожна з який має свої координати. Отже, множина з N точок заповнює n-мірний прямокутний паралелепіпед; координати кожної точки випадкові; заповнення паралелепіпеда в загальному випадку нерівномірне. Цю нерівномірність варто відбити в моделі. З цією метою приведемо в однозначну відповідність із щільністю заповнення обсягу паралелепіпеда точками n-мірний диференціальний закон розподілу можливості параметрів сигналів $wn\ (x_1, x_2, ..., xn)$ [4].

Для більшості практичних випадків параметри $x_1, x_2, ..., x_n$ незалежні друг від друга. Це пояснюється двома основними причинами: 1) як правило, параметри (частота, напрямок розподілу радіохвиль, поляризація і т.д.) незалежні по своїй фізичній природі, по методу їхніх формувань; 2) діапазони в основному Дхі вважаються вузькими. У цьому випадку зв'язок між параметрами послаблюється. У загальному випадку зв'язок між тривалістю імпульсу і несучою частотою існує, проте про неї нема потреби говорити, якщо зазначені розміри змінюються у вузьких діапазонах. У силу незалежності параметрів вірне співвідношення [3]

$$w_n(x_1, x_2, ..., x_n) = w(x_1)w(x_2)...w(x_n), \qquad (1)$$

де $w(x_i)$ - одномірні ймовірнісні розподіли параметрів.

Справедливість виразу (1) значно полегшує задачу побудови і використання ймовірнісних розподілів.

У поданому n-мірному паралелепіпеді загальний об`єм якого $V=Дxi\cdot Дxi\cdot...Д xi=\prod_{i=1}^{n} Дx_i$, можна виділити деякий відносно малий об`єм $\Delta V'<<V$, що охоплює точку ($x'1$, $x'2$, ..., x 'n), із ребрами, паралельними осям координат. По кожній з осей цей об`єм буде займати відрізок $\Delta X'i$, а самий об`єм $\Delta V'= \Delta X`_1\Delta X`_2...\Delta X'n=\prod_{i=1}^{n}\Delta X`_i$ можна уявити як деяку узагальнену смугу пропускання n-мірного фільтра, що складає з n фільтрів по окремих параметрах із смугою пропускання $\Delta X'i$. Для простоти задамося, що усі фільтри ідеальні в тому смислі, що їхні характеристики вибірковості мають прямокутну форму. Отже, в узагальненому об`ємі (діапазоні) V, заповненому системою випадкових точок, що підпорядковуються розподілу $wn\ (x_1, x_2, ..., x_n)$, за допомогою ідеального n-мірного фільтра виділена узагальнена смуга прозорості $\Delta V'$. Для цієї смуги можна застосувати розподіл Пуассона [4]

$$vk=\frac{1}{k!}\ e\text{-}2zk,$$

де z - середнє число сигналів в об`ємі $\Delta V'1$. У нашому випадку оцінки ПЕМВ:

$$z=N\Delta V'wn\ (x'_1, x'_2, ..., x'_n).$$

У розгорнутому вигляді:

$$vk=\frac{1}{k!}\exp(-N\Delta\, V'wn\,(x'_1, x'_2, \ldots, x'_n))[N\Delta\, V'wn(x'_1, x'_2, \ldots, x'_n)]^k=$$

$$=\frac{1}{k!}\exp[-N\prod_{i=1}^{n}\Delta X`_i\;\; w(x'i)][N\prod_{i=1}^{n}\Delta X`_i\;\; w(x'i)]^k. \quad (2)$$

За допомогою (2) можна записати ряд співвідношень зокрема:

- можливість того, що в об`ємі Δ V' не буде жодного випромінювання

$$v_0=\exp[-N\Delta\, V'wn\,(x'_1, x'_2, \ldots, x'_n)] \quad (3)$$

- можливість того, що в об`ємі Δ V' буде тільки одне випромінювання

$$v_1=\exp[-N\Delta\, V'wn\,(x'_1, x'_2, \ldots, x'_n)][N\Delta\, V'wn\,(x'_1, x'_2, \ldots, x'_n)] \quad (4)$$

- можливість того, що в об`ємі Δ V' буде не більше одного випромінювання (така можливість утворюється шляхом підсумовування (3) і (4))

$$v_{\le 1}=\exp[-N\Delta\, V'wn\,(x'_1, x'_2, \ldots, x'_n)][1+N\Delta\, V'wn\,(x'_1, x'_2, \ldots, x'_n)] \quad (5)$$

З практичної точки зору вираження (3), (4) і (5) мають велике значення. Якщо під шириною узагальненої смуги пропускания $\Delta V'$ розуміють ширину смуги пропускания *n-мірного* фільтра радіоприймального пристрою, то вираз (3) може застосовуватися при оцінці електромагнітної обстановки об'єкта, а вираз (5) - при дослідженні можливості виділення сигналу з деякої сукупності сигналів, поданих системою випадкових точок у n-мірному просторі.

Ці положення дуже важливі при оцінці інформативності ПЕМВ засобів обчислювальної техніки не тільки окремої ПЕОМ, але і обчислювального центру будь-якого розміру.

Для забезпечення ЗІ від витоку через ПЕМВ в ПЕОМ використовуються слідуючі методи і засоби: екранування приміщень й активне радіотехнічне маскування об'єктів. Радіотехнічне маскування об'єктів припускає формування і випромінювання сигналів, що маскують, у безпосередній близькості від зашумлюємого об'єкту. При цьому розрізняють декілька методів такого маскування: енергетичні методи; методи синфазной перешкоди і статистичний метод [2].

При енергетичному маскуванні методом білого шуму випромінюється широкосмуговий шумовий сигнал із постійним енергетичним спектром, що істотно перевищує максимальний рівень випромінювань. Спектрально-енергетичний метод, другий з енергетичних методів маскування, полягає в генеруванні перешкоди, що має енергетичний спектр, обумовлений модулем спектральной щільності інформативних випромінювань ПЕОМ і енергетичним спектром атмосферної перешкоди. Даний метод дозволяє використовувати перешкоди з оптимально обмеженою потужністю для одержання на межі контрольованої зони необхідного співвідношення сигнал-перешкода. У якість показника захищеності в цих методах використовується співвідношення сигнал-перешкода.

У методі синфазної перешкоди в якості сигналу, що маскує, використовуються імпульси випадкової амплітуди, що збігаються за формою і часом існування з інформаційними сигналами. Показником захищеності в цьому методі є гранична повна ймовірність помилки на межі мінімально припустимої контрольованої зони.

Статистичний метод ЗІ полягає в застосуванні ймовірносної структури сигналу, прийнятого зловмисником, шляхом випромінювання спеціальним чином сформованного сигналу, що маскує. У якості контрольованих характеристик сигналу використовуються матриці можливостей зміни станів.

Існування радіотехнічного каналу витоку інформації через ПЕМВ з ПЕОМ не може бути предметом сперечань [3]. Такий канал існує і з ним треба боротися.

Відновлення інформації, що зберігається в ПЕМВ, під силу не тільки професіоналам, що мають у своєму розпорядженні відповідне устаткування, але навіть і спеціалістам, що не мають спеціальної підготовки на достатньо простому устаткуванні.

Для оцінки наявності в ПЕМВ інформаційних сигналів або для оцінки ефективності ЗІ можна скористатися виразами (3), (4) і (5). Проте для оцінки комплексної ефективності застосовуваної системи або методик ЗІ можна скористатися наступною методикою [4]. Вона полягає в оцінці електромагнітної обстановки (ЕМО) у районі захищаємого об'єкту на межі контролюємої зони на наявність у ньому інформаційних сигналів ПЕМВ. Отже, запропонована методика дозволяє виробити вимоги до системи ЗІ, а також оцінити оптимальність їх виконання системою.

Оптимізація функціонування системи передбачає забезпечення максимуму цільової функції системи ЗІ [4, 5] при заданих умовах.

Умови задаються у формі створеної вже на межі контрольованої зони ЕМО. У будь-якому випадку цільова функція Θ рекомендується багатомірною лінійною залежністю:

$$\Theta = (q_1 \ldots q_i \ldots q_n), \qquad q_i = \sum_{i=1}^{m} (p_i p_{ij}),$$

За умови що:

$$\sum_{\substack{i,j=0 \\ i \neq j}}^{m} (p_i c_{ij} p_{ij})_l \leq a_l \qquad (l = 1, 2, 3, \ldots, j_m),$$

$$1 \geq p_{ij} \geq 0, \qquad (i,j = 0, 1, \ldots, m),$$

де m - кількість класів сигналів у ПЕМВ; n - кількість елементів , що випромінюють; l - порядковий номер елементів, що випромінюють; $(p_i\ p_{ij})_l$ - безумовна можливість правильного рішення *по* і-му класі *повідомлення* l-м елементом; $(p_i\ c_{ij}\ p_{ij})_l$ - зважена з *ціною* c_{ij} безумовна можливість помилкового рішення на *користь* і-ого класу *повідомлення* l-м елементом від аргументів, що виражають можливості виконання операцій у мережній моделі:

$$\Theta = \Theta_i(q_1, q_2, \ldots, q_n),$$

де q_i - можливість виконання i-ої операції, n - загальна кількість операцій, рівна числу ребер у моделі.

У свою чергу, деякі частини $n_e \leq n$ операцій залежать від параметрів ПЕМВ і є керованими функціями цих параметрів:

$$q_l = q_k(h_1, h_2, \ldots, h_{nl}),$$

де h_k - k-й параметр ПЕМВ.

Цю залежність для оцінки і забезпечення потрібної електромагнітної обстановки в районі об'єкта на межі контрольованої зони в першому наближенні можна уявити у формі ряду:

$$q_i = q_{i\dot{E}} + \frac{\partial q_i}{\partial h_1}\Delta h_1 + \ldots + \frac{\partial q_i}{\partial h_{nl}}\Delta h_{nl}.$$

Якщо врахувати відповідно до [4], що цільова функція лінійно залежить від можливостей qi (i = 1, 2, ..., n), та її можна записати в такій формі:

$$\dot{E} = \dot{E}_i(h_{10}, \ldots, h_{nl0}) + \frac{\partial \Theta}{\partial h_1}\Delta h_1 + \ldots + \frac{\partial \Theta}{\partial h_{nl}}\Delta h_{nl} \qquad (6)$$

де h_{10}, ..., h_{nl0} –початкові значення параметрів ПЕМВ; Δh_1, ..., Δh_{nl} –збільшення параметрів ПЕМВ стосовно початкових значень.

Тому що функція (6) що диференціюється по параметрах ПЕМВ, то вона може досягати максимуму, якщо неповний диференціал дорівнює нулю (або не існує), що равносильно виконанню системи рівнянь [4], а отже:

$$\begin{cases} \dfrac{\partial \dot{E}}{\partial h_1} = 0 \\ \dfrac{\partial \dot{E}}{\partial h_2} = 0 \\ \text{M} \\ \dfrac{\partial \dot{E}}{\partial h_{n1}} = 0 \end{cases} \qquad (7)$$

Рішення системи рівнянь (7) щодо параметрів ПЕМВ дозволяє знайти значення останніх, що досягають максимуму цільової функції.

Проте досягнення максимуму цільової функції звичайно не є можливим через обмеження областей зміни аргументів *hi*. Обмеження можуть бути обумовлені як фізичною природою так і економічними чинниками. У цих умовах здійснюється оптимізація функціонування системи ЗІ шляхом досягнення цільовою функцією значення не менше заданого:

$$\Theta \geq \Theta_з \qquad (8)$$

Оптимізація провадиться шляхом ранжування параметрів систем ЗІ від ПЕМВ по ознаці найбільшого впливу на цільову функцію

$$\dot{h_i} = \left(\frac{\partial \dot{E}}{\partial h_i} \right)_{\max} :$$

$$\dot{h_i} = \begin{Vmatrix} \dot{h_1} \\ \dot{h_2} \\ \text{M} \\ \dot{h_{n1}} \end{Vmatrix}$$

і послідовному наближенню кожного з параметрів систем ЗІ від ПЕМВ ранжуємого ряду в області його зміни доти поки не буде виконане співвідношення (8).

Ранжування параметрів систем ЗІ від ПЕМВ може бути виконано не тільки по ознаці найбільшого впливу на цільову функцію, але і по інших ознаках. Оптимізація може виконуватися методами лінійного і нелінійного програмування.

При застосуванні систем ЗІ від ПЕМВ оптимізація функціонування досягається правильним використанням застосовуваних засобів і методів захисту, а також контролем випромінювань на межі контрольованої зони. При цьому точне визначення наявності інформаційних сигналів у ПЕМВ провадиться на підставі виражень (3), (4) і (5).

Роботи з технічного захисту інформації в автоматизованих системах і ПЕОМ передбачають:

- категоріювання об'єктів електронно-обчислювальної техніки;
- включення до технічних завдань на монтаж автоматизованих систем і ПЕОМ розділу з технічного захисту інформації;

- монтаж автоматизованих систем і ПЕОМ відповідно до рекомендацій [7] документа;
- обстеження (у тому числі технічний контроль) об'єктів ПЕОМ;
- сертифікація технічного захисту інформації;
- установлення (при необхідності) атестованих засобів захисту;
- технічний контроль за ефективністю вжитих заходів.

Також необхідно призвести організаційні заходи для захисти інформації від перехоплення випромінювань технічних засобів обчислювальної техніки:

1. Навколо ПЕОМ потрібно забезпечити контрольовану територію, за межами якої відношення "небезпечний сигнал/шум" не перевищує встановлених норм при яких неможливий перехвет інформації.

2. У незахищених каналах зв'язку, лініях, проводах та кабелях ПЕОМ і апаратурою що підпадає під вплив випромінювань, що мають вихід за межі контрольованої території, потрібно установити завадозаглушувальні фільтри.

3. Проводь і кабелі потрібно прокладати в екранованих конструкціях.

4. Кабелі ПЕОМ потрібно прокладати окремим пакетом і смердоти не повинні утворювати петлі. Перехрещення кабелів ПЕОМ і допоміжних технічних засобів, що мають вихід за межі контрольованої території, потрібно проводити під прямимо кутом, забезпечуючи відсутність електричного контакту екранувальних оболонок кабелів у місці їх перехрещення.

5. Незадіяні проводь і кабелі потрібно демонтувати або закоротити та заземлити.

6. Бажано щоб система заземлення ПЕОМ не виходила за межі контррольованої території.

7. Не рекомендується використовувати для системи заземлення ПЕОМ природні заземлювачі (металеві трубопроводи, залізобетонні конструкції будинків тощо), які мають вихід за межі контрольованої території.

8. За наявності в ПЕОМ "схемної землі" окреме заземлення для них створювати не потрібно. Шина "схемна земля" повинна бути ізольованою від захисного заземлення та металоконструкцій і не повинна утворювати замкнену петлю.

9. Електроживлення бажано здійснювати екранованим кабелем.

10. Кола електроживлення на ділянці від ПЕОМ до розділових систем чи завадозаглушувальних фільтрів рекомендується прокладати в жорстких екранувальних конструкціях.

11. Не рекомендується здійснювати електроживлення технічних засобів, що мають вихід за межі контрольованої території, від захищених джерел електропостачання.

Найбільш важливішим заходом є сертифікація – яка передбачає що, за допомогою деяких процедур третя сторона дає письмову гарантію, що продукція відповідає заданим вимогам (п.3.5.2. ДСТУ 2462-92 "Сертифікація. Основні поняття"). Третьою стороною є Орган з сертифікації, акредитований у системі УкрСЕПРО, тобто державна організація, незалежна від розробника, виробника, постачальника, споживача, яка має необхідну компетентність у галузі акредистації і, зокрема, має актуалізований фонд нормативні документи та компетентний персонал.

Вимоги до продукцій, а саме ПЕОМ як відомо, задаються державними стандартами та іншими нормативними документами, до складу яких входять і технічні умови (ТУ) на конкретну продукцію, тобто можливе проведення сертифікації продукції і на відповідність вимогам ТУ. ТУ мають право на існування, якщо смердоти конкретизують, доповнюють та (або) посилюють вимоги чинних державних стандартів на дану продукцію, тобто вимоги ТУ не можуть бути нижчими конкретних показників, встановлених державними стандартами.

Таким чином, при надходженні продукції для сертифікації на відповідність ТУ, які не відповідають вимогам чинних державних стандартів на цю продукцію, Орган з сертифікації не має права сертифікувати таку продукцію. Дія таких ТУ повинна бути призупинена з

наступним доопрацюванням їх до усунення невідповідностей, у противному разі, їх державна реєстрацію підлягає скасованню.

При сертифікації однорідної продукції від різних виробників застосовуються одні й ті самі конкретні стандарти, тобто, наприклад, ЕОМ у захищенному виконанні від різних виробників повинні бути сертифіковані на відповідність одним й палимо ж обов'язковим вимогам одних й тихий же нормативних документів.

На підставі п.4.3.2. ДСТУ 3396.0. -96 та п. 4.4. ДСТУ 3410-96 сертифікація засобів ТЗІ, що застосовуються для обробки інформації, охорона якої забезпечується державою відповідно до законодавства, має проводитися неодмінно і на відповідність всім обов'язковим вимогам нормативних документів з технічного захисту інформації, встановленим для цієї продукції.

Орган з сертифікації несе відповідальність за необгрунотовану чи невідповідну видачу сертифікату, сплачуючи в таких випадках до державного бюджету України подвйну вартість виконаних робіт, а при повторному порушенні - Орган з сертифікації винний позбавлятися акредитації.

У процесі сертифікації Орган з сертифікації доручає проведення сертифікаційних випробувань одній з Випробувальних лабораторій, що акредитовані в системі УкрСЕПРО в галузі ТЗІ, але входять до складу інших ніж Орган з сертифікації юридичних осіб.

Слід відмітити, що одним з основних недоліків існуючої системи сертифікації засобів захисту інформації в Україні є монопольність Органа з сертифікації та відмова з його бокові після прийняття рішення за заявкою надавати заявникам можливість зміни Випробувальних лабораторій з економічних причин до укладання з останньою двостороннього договорові. Ця монопольність не дозволяє заявнику провести сертифікацію в іншому Органі з сертифікації, навіть якщо при укладанні договорові Орган з сертифікації вимагає оплати своїх послуг на значно вищому рівні, ніж це передбачає згаданий вище Наказ Держстандарту.

Тепер розглянемо деякі проблеми сертифікації конкретних засобів ТЗІ.

Сертифікати, видані досі в Україні на ЕОМ із захистом інформації (доречі, у сертифікатах термін "ЕОМ у захищеному виконанні" до цих ЕОМ не застосовується, оскільки смердоти, мабуть, і не відповідають вимогам до ЕОМ у захищеному виконанні) засвідчують, що ці ЕОМ відповідають ступеню захищеності від витку інформації лише за рахунок побічних електромагнітних випромінювань, тобто без врахування можливого витку інформації за рахунок наводів. Таке свідчення означає, що в цих ЕОМ зовсім не регламентовано розмір зони 1. Нагадаємо, що під зоною 1 розуміють простір навколо засобу ТЗІ, у межах якого на випадкових антенах наводяться інформаційні сигнали вище припустимого (нормованого) рівня. Тобто згадані сертифікати свідчать про невідповідність цих ЕОМ вимогам технічних розумів на них, бо технічні умови на ЕОМ у захищеному виконанні без виомг до рощміру зони 1, звичайно, не можуть бути зареєстровані.

Таким чином, якщо в сертифікаті відсутнє підтвердження щодо ступеню захищеності інформації в ЕОМ від витку за рахунок наводів, те фактично це засвідчує неможливість використання такої ЕОМ споживачами для обробки інформації, охорона якої забезпечується державою відповідно до законодавства.

Враховуючи конструктивне виконання засобів захисту вищезазначених ЕОМ, викликає сумнів, що вони відповідають і вимогам п.2.4 ДСТУ 29339-92 до розміру зони 2. Нагадаємо, що під зоною 2 розуміють зону (сферу) навколо засобу ТЗІ, у межах якої вважається можливим перехоплення інформації за рахунок побічних електромагнітних випромінювань.

Слід мати на увазі, що ЕОМ, які не відповідають вимогам п.2.4 ДСТУ 23339-92, мають неприпустимо в наш час низьку ефективність захисту. Як правило, при їх захисті використовується метод підбору комплектуючих і, перш за усе, сечасних моніторів з "низьким" рівнем випромінювань, який начебто задовольняє вимоги "для об'єктів II

категорії". Ці монітори часто застосовуються і взагалі без захисту, за рахунок чого більшість ЕОМ потрапляє в особливі умови розташування з усіма витікаючими з цього наслідками. Крім того, таке виконання ЕОМ призводить і до ряду додаткових недоліків. Зокрема, ці ЕОМ зовсім не захищені від виводу їх з ладу або знищення чи спотворення оброблюваної інформації навмисним силовим електромагнітним впливом по ефіру, а підбір комплектуючих призводить до ускладнень при ремонті, що є порушенням ДСТУ 23773-88 [6].

Грамотно спроєктована і застосовувана система ЗІ від ПЕМВ дозволить забезпечити необхідний рівень захисту ПЕОМ або обчислювального центру при відповідному рівні її оцінки. На наш погляд запропоновані методи дозволять підвищити ступінь достовірності одержуваних даних, що допоможе вирішувати поставлені задачі.

Список літератури

1. Олешко Т.І., Хорошко В.О., Юдін О.К. Оцінка параметрів небезпечного сигналу. //Захист інформації, 2001. №1 с.5-10

2. Генне В.И. Защита информации от утечки через побочные электромагнитные излучения цифрового электронного оборудования.//Защита информации. Конфидент. 1998. №2 с.89-95.

3. Маркин А.В. Безопасность излучений и наводок от средств электронно-вычислительной техники: домыслы и реальность. // Зарубежная радиоэлектроника. 1989. №12 с.102-108.

4. Сикорский В.П. Математический аппарат инженера. – К.: Техника, 1975. – 768с.

5. Браиловский Н.Н., Моржов С.В., Хорошко В.А. Особенности защиты информации при управлении воздушным движением. Вістник КМУЦА, 1999, №3 с.

6. Левченко Г.Т., Ільченко М.Ю., Хорошко В.О., Буркацький В.П., Золотухін К.С., Грошев В.М., Циганюк О.Г. Деякі питання сертифікації в галузі технічного захисту інформації. // Бізнес і безпека, 2001. №4, с.40-43

7. Тимчасові рекомендації з технічного захисту інформації в засобах обчислювальної техніки, автоматизованих системах і мережах від витку каналами побічних електромагнітних випромінювань і наводок ТР ЕОТ – 95

Надійшла 29.11.2001

УДК 681.3

Максименко Г.А.

ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ В СИСТЕМАХ АВТОМАТИЧЕСКОГО РАСПОЗНАВАНИЯ СИГНАЛОВ

Обеспечение высокой эффективности современных технических средств обнаружения и распознавания сигналов является весьма актуальной проблемой. Одним из условий успешного решения задач относящихся к данной проблеме, является умение количественно оценивать эффективность технических систем автоматического распознавания сигналов и способов их применения.

Эта оценка сводится к выбору специальных показателей или критериев, могущих служить мерой эффективности соответствующих технических средств. В этой связи одним из первых шагов при решении любой задачи, связанной с количественной оценкой эффективности, является определение вида показателя (показателей), который бы мог