Запропоновано структурну схему та описані функції автоматизованої системи випробувань засобів захисту інформації. Описано математичну модель для оцінювання ефективності функціонування системи інформаційної безпеки

Ключові слова: засоби захисту інформації, інформаційна безпека

Предложена структурная схема и описаны функции автоматизированной системы испытаний средств защиты информации. Описана математическая модель для оценки эффективности функционирования системы информационной безопасности

Ключевые слова: средства защиты информации, информационная безопасность

Block diagram and functions of an automated system for testing of information security are proposed and described. A mathematical model for evaluating the performance of the information security system is described

Keywords: information protection, information security

УДК 004.9:519.2

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ ВИПРОБУВАНЬ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

О.І. Федюшин
Кандидат технічних наук*
Контактный тел.: (057) 733-79-72
E-mail: alexf_08@mail.ru
Л.Б. Макаров
Кандидат технічних наук*
Контактный тел.: (057) 733-79-67
E-mail: lev.makarov@mail.ru
*Кафедра радіоелектроніки і комп'ютерних систем
Українська інженерно-педагогічна академія
вул. Університетська, 16, м. Харків, Україна, 61003

1. Вступ

Сучасний розвиток інформаційних технологій і, зокрема, технологій Internet/Intranet приводить до необхідності *захисту інформації*, що передається в рамках розподіленої корпоративної мережі, яка використовує мережі відкритого доступу. При роботі на своїх власних закритих фізичних каналах доступу ця проблема так гостро не стоїть, оскільки в цю мережу закритий доступ стороннім. Проте виділені канали може собі дозволити далеко не кожна компанія. Тому доводиться задовольнятися тим, що є у розпорядженні компанії. А є, найчастіше, Internet. Тому потрібно винаходити засоби захисту конфіденційних даних, що передаються по фактично незахищеній мережі.

При інтеграції індивідуальних і корпоративних інформаційних систем і ресурсів в єдину інформаційну інфраструктуру визначним чинником є забезпечення належного рівня інформаційної безпеки для кожного суб'єкта, що входить до цього простору. У єдиному інформаційному просторі повинні бути створені всі необхідні передумови для встановлення достовірності користувача (суб'єкта), достовірності змісту і достовірності повідомлення (тобто створені механізми і інструмент аутентифікації). Таким чином, повинна існувати система інформаційної безпеки (ІБ), яка включає необхідний комплекс заходів і технічних рішень по захисту:

– від порушення функціонування інформаційного простору шляхом виключення дії на інформаційні канали і ресурси;

– від несанкціонованого доступу до інформації шляхом виявлення і ліквідації спроб використання ресурсів інформаційного простору, що приводять до порушення його цілісності;

– від руйнування вбудовуваних засобів захисту з можливістю доказу неправомочності дій користувачів і обслуговуючого персоналу;

– від впровадження "вірусів" в програмні продукти і технічні засоби.

У всьому світі зараз прийнято будувати комплексну систему захисту інформації і інформаційних систем у декілька етапів - на основі формування концепції інформаційної безпеки, маючи на увазі в першу чергу взаємозв'язок її основних понять.

Перший етап - інформаційне обстеження підприємства. Саме на цьому етапі визначається, від чого в першу чергу необхідно захищатися компанії. Спочатку будується так звана *модель порушника*, яка описує вірогідну зовнішність зловмисника, тобто його кваліфікацію, наявні засоби для реалізації тих або інших атак, звичайний час дії і тому подібне. На цьому етапі можна отримати відповідь на два питання, які були задані вище: "Навіщо і від кого треба захищатися?" На цьому ж етапі виявляються і аналізуються вразливі місця і можливі шляхи реалізації погроз безпеці, оцінюється вірогідність атак і збиток від їх здійснення.

На наступному етапі розробляються рекомендації по усуненню виявлених погроз, правильному вибору і застосуванню засобів захисту. На цьому етапі може бути рекомендовано не купувати дорогих засобів захисту, а скористатися вже *наявними в розпорядженні*.

Наприклад, у разі, коли в організації є маршрутизатор, можна рекомендувати скористатися вбудованими в нього захисними функціями, а не купувати дорогий міжмережевий екран або Fairwall.

Таким чином досить актуальним і важливим питанням є функціонування та розробка автоматизованих систем випробувань засобів захисту інформації (ЗЗІ) в комп'ютерних системах та мережах. Цій меті присвячена дана стаття.

2. Структура і функції автоматизованої системи

У доступній літературі [1-6,8,9] говориться про необхідність випробувань ЗЗІ але не вказуються шляхи практичної реалізації цього важливого етапу в створенні та експлуатації ЗЗІ. В роботі [9] говориться про необхідність отримання інформації про захищеність автоматизованих систем управління з протоколів випробувань фірм її виробників, але не описані підходи і методики, що дозволяють зробити це.

Тому при розробці автоматизованої системи слід спиратися в першу чергу на існуючі в Україні стандарти в сфері захисту інформаційної безпеки [1-6].

В нашому випадку об'єктами випробувань (ОВ) є ЗЗІ деякого інформаційного ресурсу автоматизованої системи управління(АСУ), які піддаються випробуванням на інформаційну безпеку (ІБ).

Під автоматизованою системою випробувань (АСВ) будемо розуміти людино-машинний організаційно-технічний комплекс, призначений для забезпечення максимально можливого в даних умовах рівняавтоматизації випробувальних робіт по оцінюванню інформаційної безпеки.

На практиці можна виділити два види ЗЗІ: програмні та технічні. До технічних ЗЗІ будем відносити будь-які апаратні та апаратно-програмні комплекси, що дозволяють виключити виток та підміну конфіденційної інформації. Побудова АСВ технічних ЗЗІ багато в чому залежить від типу , і є складною задачею. Далі ми будемо розглядати АСВ програмних ЗЗІ.

До складу розробленої АСВ ЗЗІ входить декілька компонент:

1) Технічне забезпечення (ТЗ) –комплекс технічних засобів, що забезпечують роботу системи і виконання відведених їй функцій.

2) Математичне забезпечення (МЗ)– сукупність математичних моделей та методів, що лежать в основі логічних та обчислювальних процесів і супроводжуючих виконання випробувальних робіт.

3) Програмне забезпечення (ПЗ) – сукупність програм, забезпечуючих цільове використання АСВ ЗЗІ. Програмне забезпечення складається з загального та спеціального.

4) Інформаційне забезпечення (ІЗ) – сукупність вихідних даних випробувань разом в апаратно-програмними засобами управління ними.

5) Лінгвістичне забезпечення (ЛЗ)– сукупність використовуваних формальних мов опису інформації і алгоритмів її обробки в процесі автоматизованих випробувань.

Важливою компонентою АСВ ЗЗІє персонал системи, що включаєадміністратора системита випробовувачів. Структурна схема АСВ ЗЗІ представлена на рис. 1. Розглянемо окремі її компоненти.

Технічне забезпечення включає в себе комп'ютерні стенди, до складу яких входять технічні засоби формування та реалізаціїзасобів нападу на об'єкти інформації, а також обробки результатів випробувань. Структура технічних засобів представлена на рис. 2.

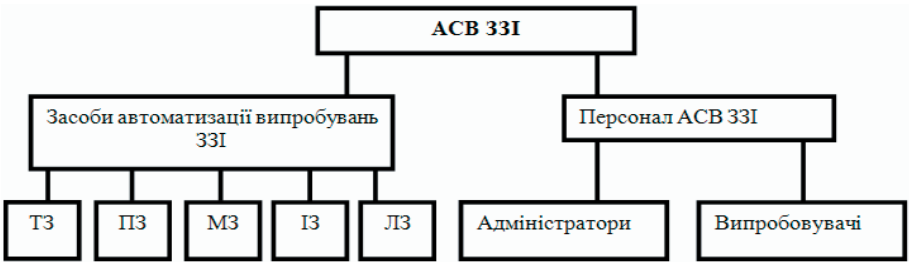

Рис. 1. Структурна схема АСВ ЗЗІ

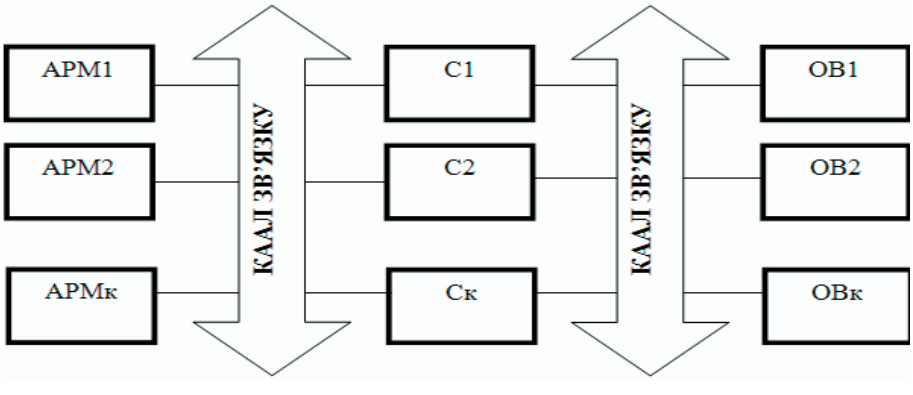

Рис. 2. Структура технічних засобів

Вони включають наступні складові:

АРМ1, АРМ2,...,АРМк –автоматизовані робочі місця випробувачів ЗЗІ; $C_1, C_2, ..., C_K$ -сервериАСВ ЗЗІ; ОВ1, ОВ2, ...,ОВк – об'єкти випробувань.

Розглянемо математичне забезпечення АСВ ЗЗІ. Будемо вважати, що АСВ ЗЗІ працює за схемою незалежних випробувань.

Нехай подія А - це факт виявлення уразливості ЗЗІ, що проходить тестування, при реалізації деякого модуля формування атак (МФА).

Пусть n -кількість МФА, що реалізовані у складі АСВ ЗЗІ для тестування інформаційної безпеки і -го ЗЗІ АСУ, що розглядається.

Припустимо, що в n -дослідах подія A сталась m разів. Передбачається, що кількість появподії A розподілена за біноміальним законом, і імовірність того, що подія A з'явиться m -разів в серії з n -дослідів, має вигляд:

$$P_{m,n} = C_n^m p^m q^{n-m},$$

де p - вірогідність реалізації події A, а $q = 1 - p$.

Після тестування на ІБ i -го ЗЗІ АСУ можна обчислити частоту появи події A, яка дорівнює: $p^* = \frac{m}{n}$.

Побудуємо довірчий інтервал $I_\beta = (p_1, p_2)$, в якому частота p^* події A випадає здовірчою імовірністю β. Для цього потрібно розв'язати систему рівнянь:

$$\sum_{m=k}^{n} C_n^m p^m (1-p)^{n-m} = \frac{\alpha}{2}, \quad (1)$$

$$\sum_{m=0}^{k} C_n^m p^m (1-p)^{n-m} = \frac{\alpha}{2}, \quad (2)$$

де $\alpha = 1 - \beta$ і $k = np^*$ -число появ події A.

Розв'язавши рівняння (1) і (2) відносно p, можна знайти межі довірчого інтервалу p_1 та p_2.

Розглянемо випадок, коли $m = 0$, тобто в n -дослідах подія A зафіксована не була. В такому випадку $p_1 = 0$, а p_2 має вигляд:

$$p_2 = 1 - \sqrt[n]{1-\beta}.$$

Якщо число випробувань є значним $n > 1000$ або $9 < npq < 100$ та $n < 1000$, то можна вважати, що частота події p^* є випадковою величиною, закон розподілу якої є дуже близьким до нормального. Нижче запишемо формули, що дозволяють знайти межі довірчого інтервалу для неї:

$$p_1 = \frac{p^* + \frac{1}{2}\cdot\frac{t_\beta^2}{n} - t_\beta \cdot \sqrt{\frac{p^*(1-p^*)}{n} + \frac{1}{4}\cdot\frac{t_\beta^2}{n^2}}}{1 + \frac{t_\beta^2}{n^2}}; \quad (3)$$

$$p_2 = \frac{p^* + \frac{1}{2}\cdot\frac{t_\beta^2}{n} + t_\beta \cdot \sqrt{\frac{p^*(1-p^*)}{n} + \frac{1}{4}\cdot\frac{t_\beta^2}{n^2}}}{1 + \frac{t_\beta^2}{n^2}};$$

де $t_\beta = \arg\Phi^*\left(\frac{1+\beta}{2}\right)$, а Φ^* -нормальна функція розподілу.

Довірчий інтервал для імовірності p буде мати вигляд $I_\beta = (p_1, p_2)$.

Поставимо задачу визначення мінімального значення правої межі довірчого інтервалу p_2 для заданого значення довірчої імовірності β .Тобто, яка повинна бути точність оцінки імовірності p при максимально можливій цифрі дослідів n, щоб верхня межа довірчого інтервалудля імовірності події A дорівнювала заданому значенню при відсутностівдалих реалізацій події A.

Розв'язокцієї задачі має вигляд:

$$p_2 = 1 - \sqrt[n]{1-\beta}.$$

Побудуємо правила для оцінки результатів випробувань, що є вирішальними.

Припустимо, що (p_{1i}, p_{2i}) - довірчий інтервал для статистичної імовірності $p_i^* = \frac{m_i}{n_i}$ порушення ІБ i -го ЗЗІ АСУ, $i = \overline{1..R}$.

Взаємне розташування заданого значення імовірності P_i та довірчого інтервалу (p_{1i}, p_{2i}) представлено на рис. 3.

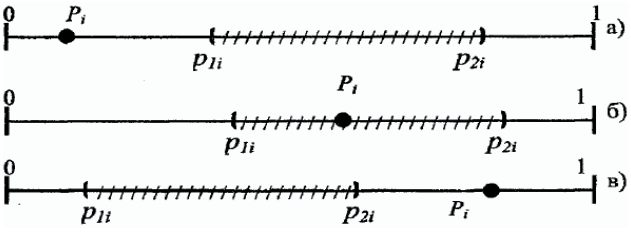

Рис. 3. Значення імовірності P_i

Випадок а) відповідає ситуації, коли значення імовірності порушення ІБ, що розташовується в інтервалі (p_{1i}, p_{2i}), більше допустимого значення цієї імовірності P_i. Таким чином, напрошується висновок про те, що існуючі ЗЗІ, не виконують вимоги по ІБ для i -го елемента.

У випадку б) однозначного висновку щодо стійкості ЗЗІ зробити неможна, тому що значення імовірності порушення ІБ, що розташовується в інтервалі (p_{1i}, p_{2i}), може бути як більше, так і менше допустимого значення цієї імовірності.

Випадок в) відповідає ситуації, колизадана вимога по забезпеченнюІБ виконується.

При цьому чим більше P_i відрізняється відвеличини P_{2i}, тим вище стійкість ЗЗІ до наявних засобів нападу.

Таким чином, маємо наступне правило дляоцінки і-го ЗЗІ АСУ: якщо виконується одне з нерівнянь: $P_i < p_{1i}$ або $p_{1i} \le P_i \le p_{2i}$, то вимоги по ІБ i -го ЗЗІ АСУ не виконуються.

При виконанні умови $P_i > p_{2i}$, i -те ЗЗІ забезпечує ІБ i -го елемента АСУ з довірчою імовірністю, що дорівнює β.

Побудуємо подібні правила (дивіться рис. 4) для випадку відсутності вдалих реалізацій порушення ІБ АСУ, тобто коли $(p_{1i}, p_{2i}) = (0, p_{2i})$.

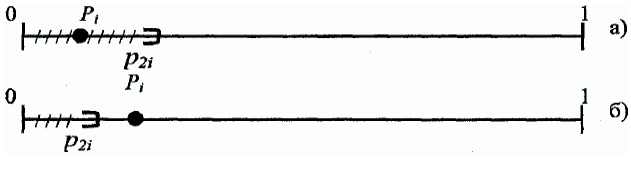

Рис. 4. Випадок відсутності вдалих реалізацій порушення ІБ АСУ

У випадку а) однозначного висновку щодо стійкості ЗЗІ зробити неможна, аджевеличина імовірності порушення ІБ, що розташовується в інтервалі $(0, p_{2i})$, може бути і більше, і менше допустимого значення цієї імовірності P_i.

Випадок б) відповідає ситуації, при якій необхідна вимога дотримання інформаційної безпеки виконується.

Слід зазначити, що якщо запропоновані правила дають негативні або неоднозначні висновки по виконанню вимог ІБ, то потрібно переглянути склад використовуваних ЗЗІ, і повторити випробування до моменту забезпечення вимог по ІБ ЗЗІ АСУ, що розглядається.

Розглянемо математичні методи та алгоритми обробки результатів роботи АСВ ЗЗІ.

Припустимо, що при тестуванні деякого ЗЗІ АСУ S знайдено множину U_S вразливостей. Розглянемо множину F видів компонент інформації, що обробляється в АСУ: конфіденційність (К), цілісність (Ц) та доступність (Д).

Опишемо відношення взаємозв'язку множин F та U_S у вигляді

$$R_S \subseteq U_S \times F, \quad (4)$$

де $F=\{К;Ц;Д\}$. Відношення (4) представляє собою бінарне відношення, і може бути описано булевською матрицею вигляду:

$$C = C\left[i,j\right]_{|u(S)|} \times |F| \quad (5)$$

Величини $M_S = |U_S|$ та $|F|=3$ визначають потужності множин U_S та F, відповідно,і перша з них є змінною.

Приймемо наступні умовні позначення:

$U_S^К$ – множина вразливостей, реалізація яких може призвести до порушення конфіденційності інформації, що циркулює через ЗЗІ, що тестується. $U_S^Ц$ -множина вразливостей, що впливають на цілісність інформації; $U_S^Д$ - множина вразливостей, що впливають на доступність інформації, яка циркулює через ЗЗІ АСУ.

Відповідно тепер, з використанням матриці (5), можно визначити потужності кожної з множин $U_S^К$, $U_S^Ц$;$U_S^Д$:

$$M_S^К = \sum_{i=1}^{Ms} c_{1i}\ ; M_S^Ц = \sum_{i=1}^{Ms} c_{2i}\ ; M_S^Д = \sum_{i=1}^{Ms} c_{3i}\ .$$

Далі визначимо точечні оцінки імовірностей порушення ІБ компонент конфіденційності, цілісності та доступності:

$$p^*_{S|К} = \frac{M_S^К}{n}\ ;\ p^*_{S|Ц} = \frac{M_S^К}{n}\ ;\ p^*_{S|Д|} = \frac{M_Д^К}{n}\ . \quad (6)$$

За аналогією визначемо точечну оцінку імовірності порушення ІБ ЗЗІ,що тестується:

$$p_S^* = \frac{M_S}{n}\ . \quad (7)$$

Далі для кожної з найдених по формулах (6) та (7) імовірностей, побудуємо довірливі інтервали з використанням формул (1), (2) або (3) в залежностівід значення параметра npq та кількості значень параметру n.

Визначимо характеристики захищеності компонент конфіденційності, цілісності, та доступності АСУ, що розглядається та системи в цілому.

Так как порушення хоча б одної деталі з компонент веде до порушення ІБ АСУ, можно сформувати інтегральні оцінки імовірностей порушення ІБ конфіденційності, цілісності, та доступності АСУ.

$$p^*_{Інт|К} = 1-\prod_{i=1}^{n}\left(1-p^*_{i|К}\right)\ ;$$

$$p^*_{Інт|Ц} = 1-\prod_{i=1}^{n}\left(1-p^*_{i|Ц}\right); \quad (8)$$

$$p^*_{Інт|Д} = 1-\prod_{i=1}^{n}\left(1-p^*_{i|Д}\right),$$

де $p^*_{Інт|К}$, $p^*_{Інт|Ц}$, $p^*_{Інт|Д}$-оцінки імовірностей порушення ІБ конфіденційності, цілісності та доступності і -го ЗЗІ.

Визначемо оцінку імовірності порушення ІБ АСУ по аналогії з формулою (8) у вигляді:

$$p^*_{Інт|АСУ} = 1-\left(1-p^*_{Інт|К}\right)\left(1-p^*_{Інт|Ц}\right)\left(1-p^*_{Інт|Д}\right)\cdot \quad (9)$$

По аналогії з пошуком довірчих інтервалів для компонент конфіденціальності, цілісності та доступності ЗЗІ АСУ, побудуємо для кожної з найдених по формулам (8), (9) імовірностей довірчі інтервали.

Використовуючи методику, що описана вище, і сформовані на етапі проектування АСУ вимоги, що перед'являються як до окремих ЗЗІ, так і АСУ, що проходить тестування, можна зробити висновок про достатній або недостатній ступень захищеності системи, що розглядається.

Слід відмити, що комплекс програм організації атак можна організувати з використанням сучасних сканерів вразливостей. В даній роботі пропонується використовувати мережевий сканер Nessus.

Нижче наводяться його основні характеристики та можливості:

1) Модульна архітектура, в якій кожний окремий тест, викладений у вигляді підключаемого модуля.

2) Клієнт-серверна архітектура.

3) Можливість обслуговувати одночасно велику кількість об'єктів

4) Адаптивність тестів, що проводяться. Усі тести координуються між собою, що дозволяє прискорити процес випробувань за рахунок виключення тестів, що ведуть до негативного результату з точки зору можливих вразливостей в ІБ.

5) Багаторежимність функціонування влючає в себе безопасні та небезопаснв режими.

6) Можливість тестування обєктів,оснащених засобами шифрування інформації, що передається з підтримкою протоколів SSL, HTTPS, SMTPS, IMAPS та інші.

3. Приклад обробки результатів випробувань

Розглянемо макетний зразок АСВ ЗЗІ, що побудований на використанні сканера безпеки Nessus та програми обробки результатів. Його структурна схема представлена на рис. 5.

Розглянемо в якості об'єкта випробувань ЗЗІ групу серверів, що працюють під управлінням операційної системи Windows.

З урахуванням можливостей ОС для випробувань було обрано 1627 тестов. Довірча імовірність дорівнює 0,95.

Нехай замовником були сформовані наступні допустимі імовірності порушення ІБ серверів АСУ, і всієї системи в цілому, представлені в табл. 1.

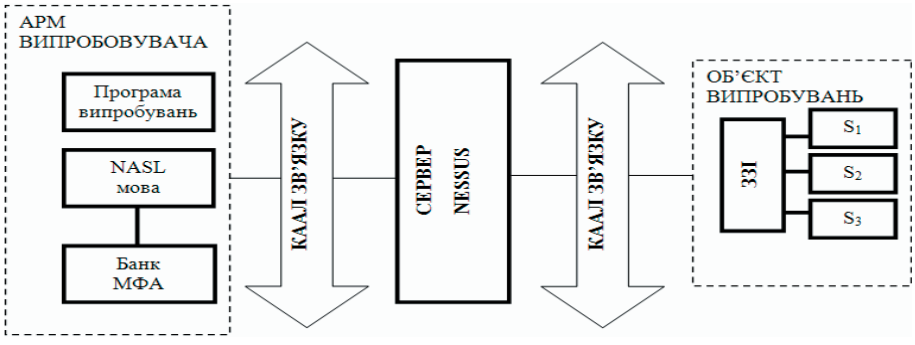

Рис. 5. Макетний зразок АСВ ЗЗІ

Таблиця 1

Допустимі імовірності

$p_{Інт\|АСУ}$	0,1		
$p_{Інт\|К}$	0,05		
$p_{Інт\|Ц}$	0,05		
$p_{Інт\|Д}$	0,05		
Сервер	S_1	S_2	S_3
$p_К$	0,005	0,01	0,01
$p_Ц$	0,005	0,01	0,01
$p_Д$	0,005	0,01	0,01

По завершенні роботи Nessus формує звіт, вивчивши який дослідник формує таблицю, що включає перелік врвзливостей для кожного з серверів, розбиваючи їх по загрозам порушення ІБ (табл. 2).

Таблиця 2

Результати тестування

Сервер	S_1	S_2	S_3
Всього	1	0	1
К	1	0	1
Ц	1	0	1
Д	0	0	0

З використанням методики були знайдені точкові оцінки та довірчі інтервали для вихідних даних табл. 2, які зведені в табл. 3.

Таблиця 3

Довірчі інтервали

Сервер	S_1	S_2	S_3
$p^*_К$	0,0006146281	0	0,0006146281
$I^к_β$	(0,0006136303; 0,0006156276)	(0; 0,018396)	(0,0006136303; 0,0006156276)
$p^*_Ц$	0,0006146281	0	0,0006146281
$I^Ц_β$	(0,0006136303; 0,0006156276)	(0; 0,018396)	(0,0006136303; 0,0006156276)
$p^*_Д$	0	0	0
$I^Д_β$	(0; 0,018396)	(0; 0,018396)	(0; 0,018396)

Визначемо інтегральні точкові оцінки компонент конфіденційності , цілісності, доступності і всієї системи в цілому, використовуючи формули (8), (9).

Результат в табл. 4.

Таблиця 4

Інтегральні точкові оцінки

$p^*_{Інт\|АСУ}$	0,0024563
$I^{АСУ}_{Інт\|β}$	(0,0024508146; 0,0024617976)
$p^*_{Інт\|К}$	0,0012289
$I^К_{Інт\|β}$	(0,0012265939; 0,0012312104)
$p^*_{Інт\|Ц}$	0,0012289
$I^Ц_{Інт\|β}$	(0,0012265939; 0,0012312104)
$p^*_{Інт\|Д}$	0
$I^Д_{Інт\|β}$	(0; 0,0018396)

Порівнявши вимоги по ІБ, представлені в табл. 1, і довірчі інтервали, отримані в табл. 3 і 4, з використанням розроблених правил, можна зробити висновок, що ЗЗІ на протестованих серверах, і в цілому система відповідають вимогам замовника.

Таким чином, в результаті випробувань отримано підтвердження необхідного рівня інформаційної безпеки ЗЗІ серверів системи, що розглядалась.

Література

1. НД ТЗІ 2.5-005 -99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
2. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 5.07.1994 року № 80/94-ВР.
3. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
4. ТР ЕОТ – 95. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінюваньнаводок.
5. НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності.Створення комплексу технічного захисту інформації. Передпроектні роботи.
6. Про внесення змін до Закону України „Про захист інформації в автоматизованихсистемах". Закон від 31.05.2005 року № 2594-IV.

7. Корченко А.Г.,Построение систем защиты информации на нечетких множествах. Теория и практические решения [Текст] / Корченко А.Г. – К. : "МК-Пресс", 2006. – 320с. (ил. Монография).
8. Петров А.А. Методы защиты информации в сетях общего пользования. [Текст] / Петров А.А. //Вісник СНУ ім. В.Даля. – 20-08. - №126. – С. 81-86.
9. Чекатков А.А., Хорошко В.А. Методы и сред ства защиты информации. – К.: Изд-во Юниор, 2003. – 504 с.
10. Термінологічний довідник з питань технічного захисту інформації [Текст] / Коженевський С.Р., Кузнєцов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

УДК 621.396.96:551.508.855

МЕТОДЫ ФИЛЬТРАЦИИ ЗЕМНОЙ ПОМЕХИ В РЛС ВЕРТИКАЛЬНОГО ЗОНДИРОВАНИЯ АТМОСФЕРЫ

А.И. Литвин-Попович
Кандидат технических наук, ассистент*
Контактный тел.: 068-432-93-36
E-mail: andrey_res@ukr.net

С.В. Юдин
Аспирант*
Контактный тел.: (057) 764-48-22, 066-745-80-04
E-mail: udin@ukr.net
*Кафедра радиоэлектронных систем
Харьковский национальный университет радиоэлектроники
пр. Ленина, 14, г. Харьков, Украина, 61166

Розглянуто методи зниження погрішностей, викликаних пасивними перешкодами, в системах радіолокацій вертикального зондування атмосфери. Розглянуті методи дозволяють понизити систематичні погрішності оцінювання динамічних параметрів атмосфери, що проілюстровано результатами імітаційного моделювання

Ключові слова: земна перешкода, вертикальне зондування атмосфери

Рассмотрены методы снижения погрешностей, вызванных пассивными помехами, в радиолокационных системах вертикального зондирования атмосферы. Рассмотренные методы позволяют снизить систематические погрешности оценивания динамических параметров атмосферы, что проиллюстрировано результатами имитационного моделирования

Ключевые слова: земная помеха, вертикальное зондирование атмосферы

Methods for ground clutter suppression in signal processing systems of radar wind profilers have been discussed. Comparative analysis of different methods is provided, effectiveness of an estimation correction method is illustrated

Keywords: ground clutter, radar wind profilers

1. Введение

Метод радиолокационного измерения скорости ветра основан на регистрации сигналов, рассеянных неоднородностями коэффициента диэлектрической проницаемости атмосферы [1,2]. Измерение параметров рассеянных сигналов позволяет оценить динамические параметры атмосферы, в частности направление и скорость ветра. Оценивание параметров рассеянного сигнала (параметризация) производится чаще всего по его спектральной плотности мощности (СПМ).

СПМ рассеянного сигнала содержит составляющую, обусловленную рассеянием излученного зондирующего импульса от движущихся с преобладающим ветром турбулентных неоднородностей коэффициента преломления атмосферы, а также компоненты, обусловленные шумами и помехами. Среди помех, регистрируемых приемным устройством РЛС ВЗ, наибольшее влияние на величину погрешностей измерений оказывает земная помеха (ЗП). ЗП представляет собой отражения зондирующих сигналов от земной поверхности и местных предметов, регистрируемые по боковым лепесткам диаграммы направленности антенны РЛС. Эффективная площадь рассеяния (ЭПР) наземных объектов, значительно больше ЭПР атмосферных неоднородностей. В результате мощность ЗП на входе приемника РЛС превосходит мощность полезного сигнала на 20...40 дБ. Особенно это проявляется на малых высотах зондирования. Мощность ЗП обратно пропорциональна четвертой степени расстояния до отражающих объектов, в то время как мощность сигнала, отраженного от атмосферных неоднородностей меняется