ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.056.8

А.О. Петров, кандидат технічних наук,
О.В. Рибальський, доктор технічних наук, професор,
О.О. Скопа,
В.О. Хорошко, доктор технічних наук, професор

ВИКОРИСТАННЯ СИГНАЛОПОДІБНИХ ЗАВАД У СИСТЕМАХ АКТИВНОГО ЗАХИСТУ ІНФОРМАЦІЇ

У статті докладно описано методи використання сигналоподібних завад у системах активного захисту інформації.
Ключові слова: *завади, сигналоподібні завади, система активного захисту.*

В статье подробно описаны методы использования сигналообразных помех в системах активной защиты информации.
Ключевые слова: *помехи, сигналоподобные помехи, системы активной защиты.*

Methods of a signal like information security in the systems of an active information security are described in details.
Keywords: *hindrances, signal like information security, systems of an active information security.*

Прицільні завади мають переваги перед гауссовими за цілим рядом технічних характеристик. Для дослідження перспективи застосування прицільних завад у системах активного захисту мереж розглянемо два різновиди сигналоподібних завад: статистично незалежну від сигналу та заваду, яка має детермінований зв'язок із сигналом.

Сигналоподібна завада, статистично незалежна від інформативного сигналу, може бути отримана на основі завад, що максимально маскують сигнал, і докладно описана в статті [1]. Ця завада зменшує мінімальний середній ризик приймання сигналів на фоні завади й відноситься до оптимальних завад у тому розумінні, що повністю маскує сигнал при будь-якому способі обробки прийнятої суміші сигналу й завади.

Подальший розвиток проблема дослідження маскуючих властивостей оптимальних і похідних від них завад одержала в [2], у якій докладно розглядаються можливі моделі оптимальних завад для різних способів представлення мовних сигналів, переданих методом дельта-модуляції, досліджуються оптимальні алгоритми приймання цих сигналів і проводиться аналіз якості маскування. У роботі доведено перевагу пропонованих завад стосовно гауссових за величиною потужності завади, необхідної для досягнення заданої величини середнього ризику. Загальні міркування щодо використання оптимальних завад для захисту комп'ютерних систем також є й в [3].

Дослідження завад збільшення потужності для досягнення заданої величини ризику доцільно виконати за допомогою щільності розподілу ймовірності потужності оптимальної завади.

З огляду на [4], представимо щільність розподілу ймовірності потужності оптимальної завади у виді згортка двох щільностей ймовірностей:

$$W_{y0}(\overline{y}) = (1-\lambda)\cdot\sum_{m=0}^{\infty}\lambda^m\cdot W_S^{(m)}(\overline{y})*v(\overline{y}), \qquad (1)$$

де $W_{y0}(\overline{y})$ – багатомірна щільність ймовірності завади; $W_S(\overline{y})$ – багатомірна щільність ймовірності сигналу; $\lambda = \frac{P_1}{1-P_1} < 1, P_1$ – апріорна ймовірність наявності сигналу; * – оператор згортки; $W_S^{(m)}(\overline{y}) = W_S(\overline{y})*W_S(\overline{y})*...*W_S(\overline{y})$ – згортка щільностей ймовірностей; $v(\overline{y})$ – довільна щільність ймовірності.

Таким чином, оптимальна завада являє собою суму двох випадкових незалежних процесів, про що свідчить наявність згортки в (1):

$$y_0(t) = y_1(t) + y_2(t), \qquad (2)$$

де $y_1(t)$ – завада з багатомірною щільністю, що стоїть ліворуч від оператора згортки;

$y_2(t)$ – довільний процес, вибір якого може бути здійснений з метою одержання мінімальної енергії завади.

На сигналі подібний характер завади вказує на наявність багатомірної щільності розподілу сигналу $W_S(\overline{y})$ виразу (1).

Структура завади може бути конкретизована з урахуванням моделі сигналу, для якого вона створюється. При виборі моделі небезпечного сигналу в процесі спеціальних досліджень, як правило, передбачається, що в точці приймання небезпечний сигнал може бути відомий технічному засобу розвідки (ТЗР) повністю, тобто є детермінованим, що забезпечує певний запас захищеності стосовно реальної ситуації. Такий підхід слід уважати виправданим, оскільки в сучасних корпоративних системах, як правило, використовується імпортна комп'ютерна техніка, а, отже, технічна розвідка має можливість одержати її зразки й технічну документацію.

Детермінованому небезпечному сигналу, як показано в [5], відповідає оптимальна завада, описувана квазідетермінованим випадковим процесом з багатомірною щільністю ймовірності:

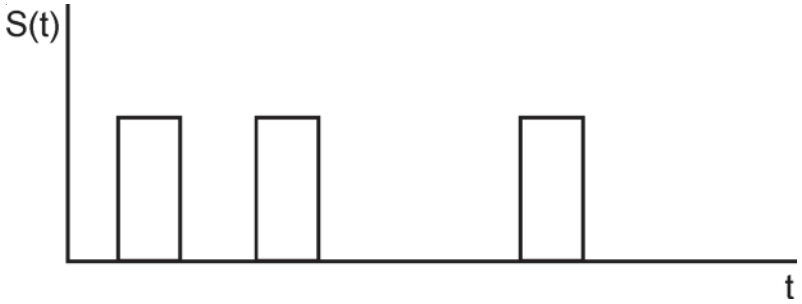
$$W_{y0}(\overline{y}) = (1-\frac{1}{\lambda})\cdot\sum_{m=0}^{\infty}\left(\frac{1}{\lambda}\right)^m\cdot(\overline{y}+m\cdot\overline{S}_0),\ \lambda>1; \qquad (3)$$

$$W_{y0}(\bar{y}) = (1-\frac{1}{\lambda})\cdot\sum_{m=0}^{\infty}\lambda^m\cdot\delta\cdot(\bar{y}-m\cdot\bar{S}_0),\ \lambda<1, \qquad (4)$$

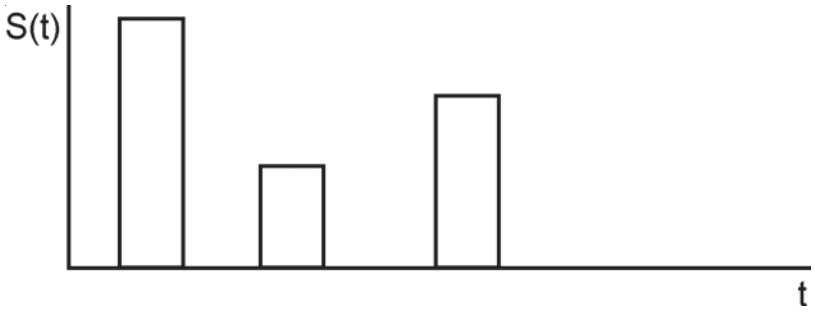
де S_0 – вектор сигналу.

Фізично реалізована завада такого типу має кінцеве число рівнів квантування (m) і може розглядатися для послідовного коду як амплітудно-модульована за випадковим законом послідовності імпульсів, що точно збігаються за всіма параметрами з інформаційними.

На рис. 1 наведено приклад небезпечного сигналу в послідовному коді й відповідна йому реалізація завади. Таким чином, розглянута завада має параметри, що повністю збігаються з параметрами сигналу, але несе неправильну інформацію про значення інформаційного параметра. Через це завади даного класу будемо називати прицільними за параметрами, або просто прицільними завадами.



а) інформативний сигнал



б) прицільна завада

Рис. 1. Часові діаграми інформативного сигналу, представленого в послідовному коді, і прицільної завади

Розглянемо тепер системи активного захисту (САЗ), де використовуються прицільні завади (ПЗ) з погляду можливості опису їх за допомогою сформульованих раніше основних технічних характеристик (ТХ).

Методику розрахунків середньої ймовірності характеризуючої помилки, що маскує здатність ідеалізованої прицільної завади, наведено в [6]:

$$P_{ОШ} = P_1\cdot\frac{1-\lambda^m}{1-\lambda^{m+1}},\ \lambda<1; \qquad (5)$$

$$P_{ОШ} = P_1 \cdot \frac{\lambda^m - 1}{\lambda^{m+1} - 1},\ \lambda > 1; \qquad (6)$$

$$P_{ОШ} = 0.5 \cdot \left(1 - \frac{1}{m+1}\right),\ \lambda = 1. \qquad (7)$$

Результати розрахунків показують, що вже при значенні параметра m=15, відповідно до нормативного документа [7], виконуються норми для об'єктів першої категорії. При цьому істотним є те, що можливе одержання однієї й тієї ж імовірності помилки приймання розряду машинного коду при меншій (приблизно у два рази) потужності завади порівняно з гауссовою. Завдяки застосуванню багатоканальних генераторів прицільних завад потужність їх випромінювання може бути зменшена ще в кілька разів.

Таким чином, для прицільної завади принципово можливо забезпечити високе значення маскувальної здатності при менших енергетичних витратах, що впливають на такі технічні характеристика, як ЕМС і прихованість.

Водночас у рамках ідеалізованої моделі прицільної завади й сигналу маскувальна здатність значно знижується завдяки тому, що на підставі оцінки відповідного параметра вхідної суміші в ТЗР прицільна завада може бути повністю скомпенсована. Ця обставина істотно стримувала розвиток САЗ, які використовують прицільні завади.

Причиною подібної ситуації є те, що при розгляді ідеалізованої завади не враховується такий важливий фактор, який сприяє підвищенню маскувальної здатності і захищеності стосовно методів компенсації завад як наявність гауссового компонента в адитивній суміші сигналу й завад. Інтенсивність цього компонента досить велика, оскільки оцінка захищеності відповідно до [7] проводиться в умовах, коли відношення сигнал/шум менше або близьке до одиниці.

У роботі [8] на прикладі розгляду структури й завадостійкості асимптотично оптимального приймача при подібній математичній моделі каналу показано, що за наявності навіть слабкого шуму величина помилки зростає через неточність оцінки параметрів імпульсів завади в каналі компенсації.

Таким чином, урахування гауссового компонента може істотно поліпшити маскувальну здатність прицільних завад і їхню захищеність стосовно методів компенсації. Ускладнення моделі каналу в цьому випадку призводить до того, що вона перестає відповідати моделі, прийнятої в [6, 9], і результати, отримані в цих роботах, не можуть бути використані. З іншого боку, у повному обсязі не можуть бути використані й результати [8], отримані для асимптотично оптимального приймання детермінованого сигналу, оскільки вони є слушними при відношенні сигнал/шум набагато більше одиниці, а нас цікавить діапазон, коли ця величина менша або близька до одиниці. Отже, завдання оцінки маскувальної здатності та захищеності стосовно методів компенсації завад має бути вирішене по-іншому.

Вирішення цього завдання передбачає синтез оптимального алгоритму обробки перехопленої суміші сигналу й завади для того, щоб представити потенційні можливості ТЗР, а потім аналіз синтезованого алгоритму для одержання кількісних оцінок захищеності, на основі яких формулюються вимоги до параметрів завади.

Найбільш характерною для технічних засобів корпоративної мережі є паралельна обробка інформації й використання паралельних кодів. Однак формули розрахунків середньої ймовірності помилки (5) – (7) можна застосувати тільки для сигналів послідовного коду.

При прийманні паралельного коду має місце завдання розрізнення сигналів, що приводить до використання багатоканальних схем, аналіз яких, як відомо, значно складніший, ніж одноканальних граничних схем, характерних для послідовного двійкового коду.

Маскувальні властивості прицільних завад для сигналів паралельного коду доцільно оцінювати при ідеальній моделі завади, урахування ж її реальних характеристик можна зробити приблизно з використанням результатів, отриманих для послідовного коду.

Отже, для кількісної маскувальної оцінки здатності прицільних завад стосовно паралельних і послідовних кодів з основою більше двох має бути розроблений алгоритм, що дозволяє робити обчислення середньої ймовірності помилки.

У цілому, одержання кількісних оцінок маскувальної здатності і захищеності стосовно методів компенсації завад є основою для формування кількісних вимог до параметрів САЗ і способів її побудови.

Розглянемо зв'язані показники САЗ, що використовують такі прицільні завади, як прихованість і електромагнітна сумісність (ЕМС).

Маскування сигналів послідовних і паралельних кодів прицільною завадою призводить до того, що сумарне випромінювання завади й сигналу стає практично таким, що не відрізняється від випромінювання чисто паралельного коду, досить розповсюдженого в корпоративних мережах. Еквівалентна розрядність цього паралельного коду може бути встановлена після проведення досліджень маскувальної здатності прицільних завад стосовно основних типів кодів. Однак зважаючи на те, що захищеність паралельних кодів зростає зі збільшенням розрядності, можна припустити, що еквівалентна розрядність, наявна в сумарному випромінюванні, є практично постійною величиною.

Таким чином, подібність випромінювання прицільної завади й небезпечного сигналу, представленого в паралельному коді, забезпечує високу прихованість САЗ, що використовують прицільні завади. Крім того, кожна прицільна завада адаптована під свій небезпечний сигнал завдяки кореляції з ним, у той час як гауссова завада, як правило, забезпечує захист одразу декількох небезпечних сигналів, що призводить до випромінювання значної надлишкової потужності завади, погіршує прихованість і показники ЕМС. Якщо говорити про такий показник, як відносні енергетичні витрати на одержання заданої середньої ймовірності помилки, то, згідно з [9], вони можуть бути зменшені в кілька разів стосовно САЗ із гауссовими завадами. За даними, наведеними в [10], ступінь поліпшення може бути оцінений й кількісно, але тільки стосовно послідовного коду, оскільки оцінити маскуючу здатність прицільних завад стосовно паралельного коду дуже складно.

Другим різновидом сигналоподібних завад, деякою мірою протилежних прицільним, є так звані імітуючі завади. Суть способу захисту, заснованого на застосуванні цих завад, полягає в тому, що в технічних системах корпоративних мереж додатково встановлюють пристрої, випромінювання яких є аналогічним випромінюванню ланцюгів, де циркулюють небезпечні сигнали, причому сумарне випромінювання повинне мати постійну інтенсивність і параметри, незалежно

від оброблюваної інформації. На рис. 2 пунктиром показана можлива інтерпретація імітуючої завади стосовно сигналу в послідовному коді.

Іншою можливою інтерпретацією сигналоподібної завади, статистично пов'язаної із сигналом, може бути компенсуюча завада, яка протифазна сигналу й впливає на нього таким чином, що сумарне випромінювання дорівнює нулю. Математичні моделі цих завад досить подібні, тому подальший розгляд будемо виконувати для імітуючої завади. Імітуюча завада проста в реалізації, але має й ряд істотних недоліків, що знижують її практичну цінність. По-перше, висока маскувальна здатність цієї завади досягається при повному її збігу за всіма параметрах з інформативним сигналом. А якщо ні, то при відсутності гауссової компоненти відбувається повна селекція завади. По-друге, оскільки завада жорстко пов'язана з інформативним сигналом, сам генератор завади так само стає джерелом інформативного сигналу й має створюватися з урахуванням спеціальних вимог. Ці обставини обмежують галузь застосування САЗ використовуваних імітуючих завад.

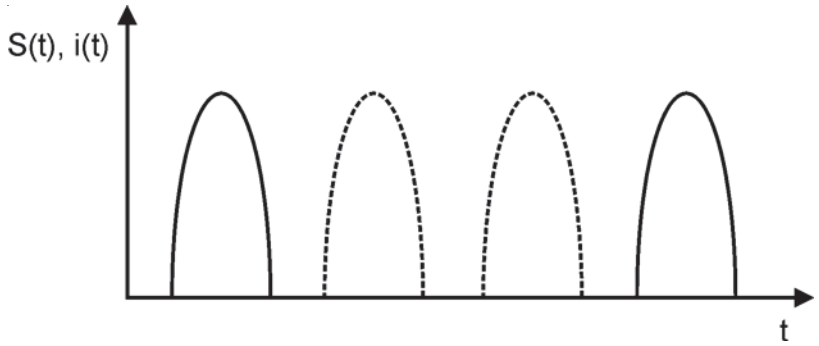


Рис. 2. Часові діаграми інформативного сигналу, представленого в послідовному коді імітуючої завади

Строге порівняння за всіма ТХ імітуючих завад із САЗ прицільних завад, що використовуються, не видається можливим, тому що наявні результати досліджень є недостатніми для остаточних висновків про здатність, що маскує, і захищеності стосовно методів селекції й компенсації завад, а також по ряду інших ТХ.

Таким чином, проведено якісну оцінку можливостей САЗ, що використовують сигналоподібні завади, показано перспективність їх застосування для захисту в мережах, в яких обробляється та циркулює інформація з обмеженим доступом. САЗ, засновані на застосуванні прицільних або завад, що імітують, мають високу здатність, маскувальну прихованість і надійність, а також високі показники ЕМС, які можуть перевершувати аналогічні показники САЗ, що використовують гауссові завади. Оцінка вимагає додаткових досліджень, пов'язаних із побудовою формальної моделі й визначення ефективності САЗ, що використовують сигналоподібні завади.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Хмелевский И.В.* Анализ эффективности использования аддитивных помех для маскировки передачи речи методом дельта-модуляции : дисс. канд. тех. наук / И.В. Хмелевский. – Свердловск, 1989. – 182 с.

2. *Павловский Е.В.* Модель приемника перехвата импульсных сигналов ЭВМ / Е.В. Павловский // Вопросы специальной радиоэлектроники. Серия телемеханика и системы управления, 1978. – Вып. 12. – С. 74–82.

3. *Гуткин Л.С.* Теория оптимальных методов радиоприема при флуктуационных помехах: / Л.С. Гуткин. – М. : Сов. радио, 1972. – 448 с.

4. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005-99.

5. Нормы эффективности защиты АСУ и ЭВМ от утечки информации за счет ПЭМИН. – М. : МОП, 1977. – 35 с.

6. *Павловский Е.В.* Модель приемника перехвата импульсных сигналов ЭВМ / Е.В. Павловский // Вопросы специальной радиоэлектроники. Серия телемеханика и системы управления, 1978. – вып. 12. – С. 74–82.

7. *Котоусов А.С.* Различение детерминированных сигналов в квазидерминиррованном потоке импульсов / А.С. Котоусов // Проблемы передачи информации, 1976. – Т. 12. – Вып. 1. – С. 41–47.

8. *Левин Б.Р.* Теоретические основы статистической радиотехники: в 3-х тт. – Т. 1. / Б.Р. Левин. – М. : Сов. Радио, 1974. – 392 с.

9. *Конторович В.Я.* Оптимальный прием сигналов дискретных сообщений на фоне аддитивных помех / В.Я. Конторович, В.Е. Ляндерс // Известия вузов. Серия Радиоэлектроника, 1973. – Т. 16. – № 3. – с. 49–53.

10. Защита от радиопомех / Под ред. М.В. Максимова. – М. : Сов. радио, 1967. – 496 с.

Отримано 2.03.2012