УДК 623.618.2

Ю.В. Стасєв, О.О. Мелешенко, І.О. Ткаченко

Харківський університет Повітряних Сил імені Івана Кожедуба, Харків

УМОВИ РЕАЛІЗАЦІЇ ДИНАМІЧНОГО РЕЖИМУ ФУНКЦІОНУВАННЯ ЗАХИСТУ СИСТЕМИ ЗВ'ЯЗКУ ТА УПРАВЛІННЯ

В роботі розглянута можливість забезпечення активного завадо- та імітозахисту у системах і засобах зв'язку, захисту їх від засобів радіоелектронної розвідки й радіоелектронної боротьби. Встановлено, що для вирішення поставлених завдань застосовується реалізація динамічного режиму функціонування. Доведено теореми недешифрованості динамічного режиму функціонування і визначено необхідні та достатні умови для шляхів його досягнення.

Ключові слова: *радіоелектронна протидія, динамічний режим функціонування, ентропія розкриття, сигнально-кодові конструкції, система зв'язку.*

Вступ

Постановка проблеми у загальному вигляді. Забезпечення активного завадозахисту та імітозахисту у системах і засобах зв'язку та здійснення захисту їх від засобів радіоелектронної розвідки й радіоелектронної боротьби евентуального супротивника можливо при реалізації динамічного режиму функціонування.

Для оцінки ефективності динамічного режиму функціонування використовується міра невизначеності відносно використання в системах і засобах зв'язку ансамблю сигнально-кодових конструкцій та їх конкретного вигляду, що назвемо ентропією розкриття.

Мета статті – розробка достатніх та необхідних умов динамічного режиму функціонування захисту системи зв'язку та управління.

Аналіз останніх досягнень і публікацій. Проведені дослідження [1] показали, що розв'язання проблеми підвищення якості функціонування системи зв'язку можливе за рахунок:

– застосування змішаної стратегії поведінки системи зв'язку, що полягає у випадковому виборі алгоритму функціонування системи та використовуваних сигнально-кодових конструкцій (зменшення ймовірності постановки оптимальної перешкоди);

– вибору структури і параметрів системи зв'язку, що збільшують часткові показники якості її функціонування;

– збільшення ймовірності розпізнавання діючої стратегії радіоелектронного подавлення і класу завад та зміни алгоритму функціонування системи зв'язку.

Забезпечувати виконання цих умов, як показали дослідження [2 – 4], можливо при реалізації динамічного режиму функціонування цифрової системи зв'язку.

Постановка задачі та викладення матеріалів дослідження

Нехай, з погляду супротивника, будь-який сигнал S_i є відображенням j-го значення U_j, то з незалежною появою сигнально-кодових конструкцій ентропія розкриття n елементів повідомлення буде визначатися виразом

$$H = \sum_{j=1}^{n} H_j , \qquad (1)$$

де H_j – часткова ентропія розкриття j-го повідомлення.

Ентропія розкриття j-го повідомлення являє собою математичне сподівання кількості інформації в одному повідомленні множини $\{M\}$, що реалізує динамічний режим функціонування.

Визначимо умови недешифровності множини $\{M\}$. Для цього доведемо такі теореми.

Теорема 1. Нехай інформаційній множині $\{U\} = \{u_1, u_2, ..., u_z\}$ за правилом перетворюючої множини $\{M\}$ ставиться у відповідність сигнально-кодова конструкція з множини $\{S\} = \{S_1, S_2, ..., S_Q\}$. Тоді ентропія $H_j(U_j, S_i)$ розкриття j-го повідомлення буде набувати максимального значення з незалежною появою сигнально-кодових конструкцій $\{S\}$ і повідомлень.

Доведення. Спільну ентропію сукупності S й U можна зобразити у вигляді

$$H(U,S) = -\sum_{j=1}^{z}\sum_{i=1}^{Q} p(U_j, S_i)\log_2(U_j, S_i) , \qquad (2)$$

де $p(U_j, S_i)$ – імовірність спільної появи повідомлення U_j й сигналу S_i.

Визначимо максимум спільної ентропії $H(U,S)$:

$$H(U,S) = H(U) + H(U/S). \quad (3)$$

Відомо, що $H(U,S)$ приймає максимальне значення, якщо $H(U)$ й $H(U/S)$ максимальні.

У [5, 6, 7] показано, що $H(U)$ приймає максимальне значення при стратегічно незалежних повідомленнях.

Знайдемо максимум $H(U/S)$:

$$H(U,S) = -\sum_{j=1}^{z}\sum_{i=1}^{Q} p(U_j, S_i)\log_2(U_j/S_i). \quad (4)$$

Для умовної ентропії $H(U/S)$ справедлива така нерівність:

$$H(U/S) \le H(U). \quad (5)$$

Отже,

$$H(U,S) = -\sum_{j=1}^{z}\sum_{i=1}^{Q} p(U_j, S_i)\log_2(U_j/S_i) \le \le -\sum_{j=1}^{z} p(U_j)\log p(U_j). \quad (6)$$

У виразі (7) рівність виконується за умови

$$p(U_j/S_i) = p(U_j).$$

Виконання цієї умови можливе при статистичній незалежності U_j й S_i.

Тоді

$$p(U_j, S_i) = p(U_j)p(S_i), \quad (8)$$

тобто одержимо

$$H(U,S) = -\sum_{j=1}^{z}\sum_{i=1}^{Q} p(U_j)p(S_i)\log_2 p(U_j). \quad (9)$$

З огляду на те, що $\sum_{i=1}^{Q} p(S_i) = 1$, маємо

$$H = (U/S) = -\sum_{j=1}^{z} p(U)\log_2 p(U_j) = H(U). \quad (10)$$

Отже, при статистично незалежних множинах $\{U\}$ і $\{S\}$ ентропія розкриття максимальна.

Теорема 2. Нехай інформаційній множині

$$\{U\} = \{u_1, u_2, \ldots, u_z\}$$

за правилом перетворюючої множини ставиться у відповідність сигнально-кодова конструкція з множини $\{S\} = \{S_1, S_2, \ldots, S_Q\}$.

Тоді ентропія H_j розкриття j-го повідомлення буде набувати максимального значення з незалежною появою сигнально-кодових конструкцій з множини $\{S\}$.

Доведення. Нехай інформаційній множині $\{U\}$ за законом перетворюючої множини $\{M\}$ ставиться у відповідність сигнально-кодова конструкція з множини $\{S\}$ з імовірністю $p\{S_i\}$. Імовірність появи сигнально-кодової конструкції S_i залежить від появи $(S_{i-1}, S_{i-2}, \ldots, S_{i-n})$.

Тоді, як виходить з [4], справедлива така нерівність:

$$H_j(S_i/S_{i-1}, S_{i-2}, \ldots) \le H_j(S_i). \quad (11)$$

Теорема 3. Умовна ентропія джерела, що задає динамічний режим функціонування, після перехоплення повідомлення $H(M/U)$ буде набувати максимального значення з незалежною появою сигнально-кодових конструкцій з множини $\{S\}$ від інформаційної множини $\{U\}$.

Доведення. Визначимо $H(M/U)$ відповідно до [5, 6, 7]:

$$H(M/U) = \sum_{k=1}^{z}\sum_{i=1}^{Q} p(S_i)\, p(U_k/S_i)\log\frac{1}{p(U_k/S_i)}. \quad (12)$$

Дійсно, якщо евентуальний супротивник при перехопленні k сигнально-кодових конструкцій ($k = \overline{1, z}$) не може уточнити наявні в нього апріорні ймовірності на основі обчислення апостеріорних імовірностей

$$p(U_k/S_i) = p(U_j)p(S_i/U_j); \quad p(S_l/U_j) = \frac{p(S_i)\, p(U_j/S_i)\, p(S_i)}{p(U_j)}, \quad (13)$$

то

$$p(U_j/S_i) = p(U_j); \quad p(S_i/S_iU_j) = p(S_i). \quad (14)$$

Таким чином, завдання розкриття закону зміни керуючої множини зводиться до методів статистичного випробування всіх можливих варіантів, а умовна ентропія

$$H(\mu/U) = H(\mu) = \sum_{k=1}^{z} p(S_k)\log\frac{1}{p(S_k)}. \quad (15)$$

Отже, умовна ентропія $H(\mu/U)$ джерела, яка задає динамічний режим функціонування, набуває значення з незалежною появою сигнально-кодових конструкцій з множини $\{S\}$ від інформаційної множини $\{U\}$, що й було потрібно довести.

Отже, з теореми 3 випливають два найважливіших визначення.

Визначення 1. Якщо умовна ентропія джерела, що задає динамічний режим функціонування, максимальна, то кількість інформації про перетворюючу множину після прийому Q сигнально-кодових конструкцій визначається виразом

$$I(U,M) = H(M) - H(M/U) \quad (16)$$

і дорівнює нулю.

Визначення 2. Якщо умовна ентропія джерела, що задає динамічний режим функціонування, максимальна, то надмірність, що міститься в інформації про перетворюючу множину, обумовлена таким виразом:

$$D = \frac{H(M) - H(M/U)}{H(M)} \qquad (17)$$

і дорівнює нулю.

Теореми 1 – 3 визначають необхідні й достатні умови теоретичної недешифровності закону перетворюючої множини.

На підставі доведених теорем 1 – 3, а також визначень 1, 2 сформулюємо умови реалізації режиму функціонування.

1. Імовірність передачі сигнально-кодової конструкції не повинна залежати від переданих інформаційних символів і від передачі попередніх сигнально-кодових конструкцій.

2. Розмір ансамблю використовуваних сигнально-кодових конструкцій має задовольняти вимогам з іміто- і криптостійкості.

3. Надмірність, яка міститься в інформації про множення, що задає динамічний режим функціонування на фізичному рівні, повинна прямувати до нуля.

4. Складність і стійкість множини, що задає динамічний режим функціонування на фізичному рівні, повинні вибиратися залежно від використовуваного протоколу й вимог до імітозахисту системи.

5. Стійкість множини, що задає динамічний режим функціонування, не повинна порушуватися навіть у випадку, коли евентуальному супротивнику відомий метод реалізації динамічного режиму. Стійкість має залежати тільки від кількості ключів.

6. Виконання процедур перетворення має бути формальним. Ці процедури не повинні залежати від довжини повідомлення.

Висновки і напрямки подальших досліджень

Таким чином, необхідні й достатні умови визначають шляхи досягнення теоретичної недешифрованості динамічного режиму функціонування, а їх реалізація в системі зв'язку дозволяє забезпечити активний завадозахист та імітозахист і, т внаслідок цього, забезпечити ефективний захист систем і засобів зв'язку від засобів радіоелектронної розвідки й радіоелектронної боротьби евентуального супротивника.

Список літератури

1. Теорія сигнально-кодових конструкцій: монографія / М.І. Науменко, Ю.В. Стасєв, О.О. Кузнецов, С.П. Євсеєв. – Х.: ХУ ПС, 2008. – 541 с.

2. Горбенко И.Д. Сигнально-теоретические вопросы синтеза производных систем сигналов для радиоканалов, функционирующих в динамическом режиме "бегущий код" / И.Д. Горбенко, Е.Ф. Глазин, Ю.В. Стасев. – М.: 71 НТК ВА им. Ф.Э. Дзержинского, 1985. – С. 68.

3. Горбенко И.Д. Производные системы сигналов и их свойства / И.Д. Горбенко, Ю.В. Стасев. – К.: Радиотехника. – 1989. – №9. – С. 26-27.

4. Ирвин Дж. Передача данных в сетях и инженерный подход / Дж. Ирвин, Д. Харль. – СПб.: Питер, 2002. – 405 с.

5. Вентцель Е.С. Теория вероятностей и ее инженерные приложения / Е.С. Вентцель, Л.А. Овчаров. – М.: Наука, 1988. – 480 с.

6. Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – М., 2002. – 480 с.

7. Сорока Л.С. Основы теории минимально-избыточных сигналов. Математические методы и средства обработки / Л.С. Сорока. – Х.:МОУ, ОНИИ ВС, 2005. – 280 с.

Надійшла до редколегії 30.11.2015

Рецензент: д-р техн. наук, проф. В.В. Бараннік, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

УСЛОВИЯ РЕАЛИЗАЦИИ ДИНАМИЧЕСКОГО РЕЖИМА ФУНКЦИОНИРОВАНИЯ ЗАЩИТЫ СИСТЕМЫ СВЯЗИ И УПРАВЛЕНИЯ

Ю.В. Стасев, О.О. Мелешенко, И.А. Ткаченко

В работе рассмотрена возможность обеспечения активного помехо- и имитозащиты в системах и средствах связи, защиты их от средств радиоэлектронной разведки и радиоэлектронной борьбы. Установлено, что для решения поставленных задач применяется реализация динамического режима функционирования. Доказаны теоремы недешифруемости динамического режима функционирования и определены необходимые и достаточные условия для путей его достижения.

Ключевые слова: *радиоэлектронное противодействие, динамический режим функционирования, энтропия раскрытия, сигнально-кодовые конструкции, система связи.*

TERMS IMPLEMENT DYNAMIC MODE OF OPERATION OF THE COMMUNICATION SYSTEM OF PROTECTION AND CONTROL

Yu.V. Stasev, O.O. Meleshenko, I.A. Tkachenko

Possibility of providing of active noise immunity is in process considered in the systems and communication means, defence them from facilities of radio electronic secret service and radio electronic fight. It is set that for the decision of the put tasks realization of the dynamic mode of functioning is used. The theorems of indecipherability of the dynamic mode of functioning are well-proven and necessary and sufficient terms are certain for the ways of his achievement.

Keywords: *radio electronic counteraction, dynamic mode of functioning, opening entropy, alarm-code constructions, communication network.*