УДК 621.391

В.И. Грабчак[1], И.В. Пасько[1], С.Е. Лахтин[2], Р.В. Королев[3]

[1]*Военный институт РВ и А Сумского государственного университета, Сумы*
[2]*Институт корпоративных информационных технологий, Курск*
[3]*Харьковский университет Воздушных Сил им. И. Кожедуба*

АНАЛИЗ МАТЕМАТИЧЕСКОЙ МОДЕЛИ И СТРУКТУРНОЙ СХЕМЫ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ

Анализируется математическая модель и структурная схема систем передачи данных в телекоммуникационных системах и сетях, обосновываются критерии и показатели оценки эффективности их функционирования.

математическая модель и структурная схема системы передачи данных, своевременность, достоверность, помехоустойчивость, скрытность

Введение

Постановка проблемы в общем виде и анализ литературы. Одним из первоочередных направлений в решения социально-экономических задач развития страны является построение современных высокоэффективных телекоммуникационных систем и сетей [1]. Их общей тенденцией является значительное усложнение аппаратурного состава и увеличение интенсивности потоков разнородной информации, циркулирующей между отдельными элементами [2, 3]. Вместе с тем существенно возросли требования к надежности и эффективности функционирования телекоммуникационных систем и сетей в процессе их целевого применения [2, 4].

Современные тенденции развития техники автоматизации и связи направлены на разработку и внедрение высокотехнологических систем передачи данных и построения на их основе современных телекоммуникационных систем и сетей нового поколения, которые обеспечивают высокую скорость обработки и передачи информации с требуемыми критериями и показателями эффективности их функционирования.

Целью статьи является анализ математической модели и структурной схемы систем передачи данных в телекоммуникационных системах и сетях, обоснование критериев и показателей оценки эффективности их функционирования.

Основная часть

Математическая модель и структурная схема системы передачи данных. Основной подсистемой телекоммуникационных систем предназначенной для обеспечения управления качественным обменом сообщений (информацией управления) является система передачи данных [5]. Рассмотрим математическую модель и структурную схему системы передачи данных, формализуем процессы обработки и передачи информации.

Структурная схема системы передачи данных телекоммуникационных систем в общем виде представлена на рис. 1. Она состоит из следующих элементов: 1) источник сообщений; 2) аппаратура кодирования источника сообщений; 3) аппаратура специального преобразования данных (шифрования); 4) аппаратура канального (помехоустойчивого) кодирования; 5) передатчик сообщений, который преобразует по некоторому правилу информационные сообщения в сигналы, соответствующие характеристикам данного канала; 6) канал – среда, которая используется для передачи сигнала от источника к приемнику; 7) аппаратура перехвата противником передаваемых сообщений; 8) аппаратура обработки и анализа перехваченных противником сообщений; 9) аппаратура передачи ложных сообщений и постановки помех противника; 10) приемник, выполняющий операцию, обратную по отношению к операции, производимой передатчиком; 11) аппаратура декодирования, выполняющая операции, обратные канальному кодированию (декодер помехоустойчивого кода); 12) аппаратура специального преобразования (расшифрования); 13) аппаратура декодирования получателя сообщения; 14) получатель сообщения – это объект, для которого предназначено сообщение; 15) аппаратура формирования ключевых данных.

Математическая модель системы передачи данных описывается следующей совокупностью операторов: $\{W_I\}$ – оператор формирования информационных сообщений; $\{W_M\}$ – оператор преобразования информационных сообщений в информационные блоки данных (оператор кодирования источника); $\{W_E\}$ – оператор преобразования информационных блоков данных в криптограммы (оператор шифрования данных); $\{W_C\}$ – оператор преобразования криптограмм в кодовые слова (оператор помехоустойчивого кодирования); $\{W_S\}$ – оператор преобразования кодовых слов в последовательность сигналов (оператор формирования сигналов); $\{W_Z\}$ – оператор взаимодействия передаваемых сигналов с

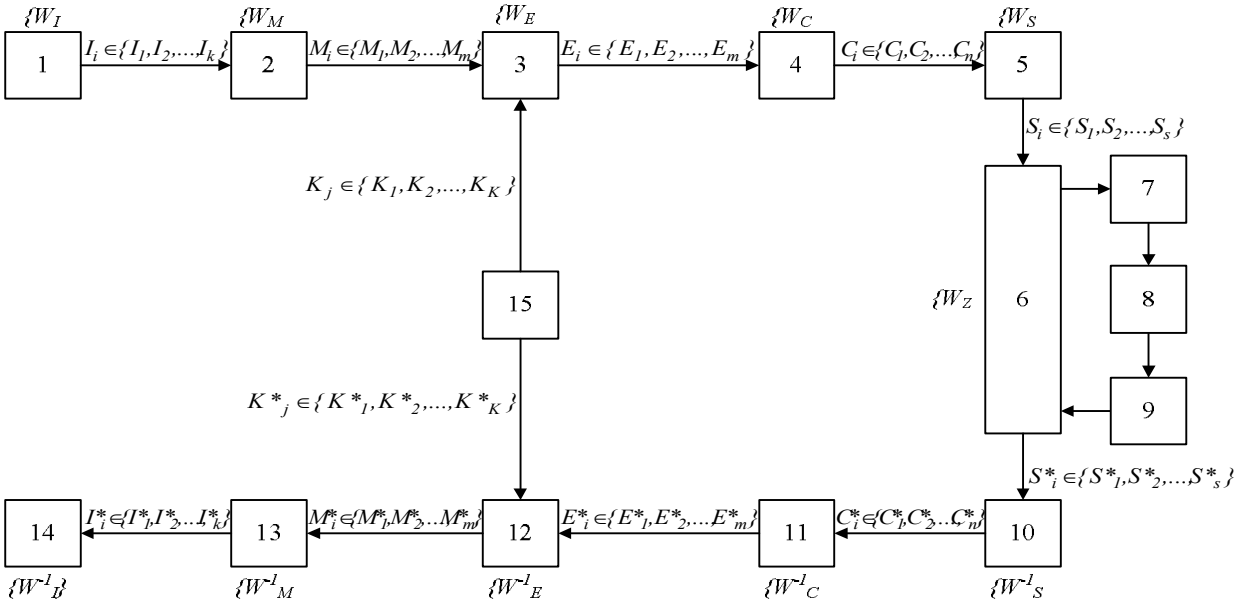

Рис. 1. Математическая модель системы передачи данных

преднамеренными и непреднамеренными помехами в канале связи; $\{W^{-1}_Z\}$ – оператор взаимодействия полученных сигналов с пространством сообщений на входе узла получателя информации; $\{W^{-1}_S\}$ – оператор преобразования последовательности сигналов в кодовое слово (оператор обработки сигналов); $\{W^{-1}_C\}$ – оператор преобразования кодовых слов в криптограммы (оператор декодирования помехоустойчивого кода); $\{W^{-1}_E\}$ – оператор преобразования криптограмм в информационные блоки данных (оператор расшифрования данных); $\{W^{-1}_M\}$ – оператор преобразования информационных блоков данных в информационные сообщения (оператор декодирования получателя информации); $\{W^{-1}_I\}$ – оператор обработки полученных сообщений.

Источник сообщений (1) порождает поток сообщений из множества $I = \{I_1, I_2, \ldots, I_k\}$. Процедуру формирования сообщений зафиксируем в виде формального оператора $\{W_I\}$. Каждое сообщение I_i представляется конкретной реализацией некоторого случайного процесса, описывающего работу источника сообщений. Каждому сообщению $I_i \in \{I_1, I_2, \ldots, I_k\}$ соответствует вероятность $P(I_i)$. Распределение вероятностей случайного процесса задается совокупным распределением вероятностей случайных величин, т.е. множеством априорных вероятностей $P_I = \{P(I_1), P(I_2), ..., P(I_k)\}$, причем $\sum_{i=1}^{k} P(I_i) = 1$.

Каждое сообщение $I_i \in \{I_1, I_2, \ldots, I_k\}$ несет информацию, численно равную мере неопределенности (энтропии) конкретной реализации случайного процесса, описывающего работу источника сообщений, т.е. запишем $H(I_i) = -P(I_i) \cdot \log(P(I_i))$, где основание логарифма задает единицу измерения количества информации. Для простоты положим основание равное двум, что соответствует двоичному (битовому) исчислению количества информации.

Таким образом, источник информации представляется как случайный процесс, конкретная реализация которого представляется в виде некоторого сообщения $I_i \in \{I_1, I_2, \ldots, I_k\}$. Если в единицу времени источник формирует одно сообщение из множества I, тогда мера информации порождаемое источником за ту же единицу времени задается функцией вида:

$$H(I) = -\sum_{i=1}^{k} P(I_i) \cdot \log(P(I_i)),$$

т.е. энтропией множества вероятностей $P_I = \{P(I_1), P(I_2), ..., P(I_k)\}$.

Максимальное значение энтропии источника достигается при равновероятном появлении сообщений из множества $I_i \in \{I_1, I_2, \ldots, I_k\}$. Тогда $\forall P_i = \frac{1}{k}$ и имеем $H_{max}(I) = \log(k)$. Отношение энтропии источника к максимальному значению, которого могла бы достичь энтропия при тех же символах, называют относительной энтропией источника. Это величина максимального сжатия, которое можно достичь при том же алфавите символов. Единица минус относительная энтропия есть избыточность δ:

$$\delta = 1 - \frac{H(I)}{H_{max}(I)} = 1 - \frac{-\sum_{i=1}^{k} P(I_i) \cdot \log(P(I_i))}{\log(k)}.$$

Аппаратура кодирования источника информации (2) представляет сообщения $I_i \in \{I_1, I_2, \ldots, I_k\}$, порожденные источником (1), в удобном для дальнейшей обработке виде и служит, прежде всего, для сжатия передаваемых данных, т.е. для устранения избыточности δ. Другими словами, аппаратура кодирования источника информации (2) реализует отображения множества сообщений $\{I_1, I_2, \ldots, I_k\}$ в множество информационных блоков данных $\{M_1, M_2, \ldots, M_m\}$ так, чтобы все вероятности $P(M_i)$ из множества вероятностей $P_M = \{P(M_1), P(M_2), \ldots, P(M_m)\}$ были, по возможности, равны. В этом (теоретическом) случае энтропия

$$H(M) = -\sum_{i=1}^{m} P(M_i) \cdot \log(P(M_i))$$

максимальна и, очевидно, равна максимальной энтропии источника. В общем случае

$$H(I) \geq H(M) \geq H_{max}(I), \ \log(k) \geq \log(m).$$

Аппаратура специального преобразования данных (шифрования) (3) реализует отображение множества информационных блоков $\{M_1, M_2, \ldots, M_m\}$ в множество шифрограмм (криптограмм) $\{E_1, E_2, \ldots, E_m\}$.

Зафиксируем множество отображений $\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_k\}$, где $\varphi_i: M \to E, \ i = \overline{1,k}$.

Всего имеется K вариантов отображений, каждое из которых параметризируется ключом прямого отображения (шифрования) $K_j \in \{K_1, K_2, \ldots, K_K\}$ из множества соответствующих ключей. Ключевые данные формирует аппаратура формирования ключевых данных (15), работа которой описывается некоторым случайным процессом.

Аппаратура канального (помехоустойчивого) кодирования (4) реализует отображение множества криптограмм $\{E_1, E_2, \ldots, E_m\}$ во множество кодовых слов $\{C_1, C_2, \ldots, C_n\}$. Целью помехоустойчивого кодирования является внесение по определенному алгоритму в передаваемые данные избыточности. На приемной стороне, анализируя принятые кодовые слова с возможной ошибкой $C^*_i \in \{C^*_1, C^*_2, \ldots, C^*_n\}$ и их соответствие внесенной избыточности, аппаратура канального (помехоустойчивого) декодирования (11) уменьшает действие возникших при передаче сообщений ошибок.

Передатчик сообщений (5) преобразует по некоторому правилу информационные сообщения в сигналы, соответствующие характеристикам данного канала. Другими словами, передатчик (5) реализует отображение множества кодовых слов $\{C_1, C_2, \ldots, C_n\}$ во множество сигналов $\{S_1, S_2, \ldots, S_s\}$.

В процессе передачи сигнала $S_i \in \{S_1, S_2, \ldots, S_s\}$ по каналу связи (6) на него воздействует аппаратура перехвата (7), обработки и анализа перехваченных противником сообщений (8), а так же аппаратура передачи ложных сообщений и постановки помех противника (9). Приемник (10) принимает смесь сигнала и помехи $S^*_i \in \{S^*_1, S^*_2, \ldots, S^*_s\}$ и выполняет преобразования, обратные передатчику. После выполнения канального декодирования, расшифрования и декодирования источника принятое сообщение отправляется получателю информации. Аппаратура обратного преобразования (10), (11), (12), (13) и (14) выполняет функции, реализующие обратные отображения: множества сигналов $\{S^*_1, S^*_2, \ldots, S^*_s\}$ во множество кодовых слов $\{C^*_1, C^*_2, \ldots, C^*_n\}$, множества кодовых слов $\{C^*_1, C^*_2, \ldots, C^*_n\}$ во множество криптограмм $\{E^*_1, E^*_2, \ldots, E^*_m\}$, множество криптограмм $\{E^*_1, E^*_2, \ldots, E^*_m\}$ в множество информационных блоков $\{M^*_1, M^*_2, \ldots, M^*_m\}$, множество информационных блоков $\{M^*_1, M^*_2, \ldots, M^*_m\}$ в множество сообщений $\{I^*_1, I^*_2, \ldots, I^*_k\}$. Каждое отображение задается соответствующими энтропийными и вероятностными характеристиками.

В соответствии с общими положениями теории надежности и эффективности технических систем, под эффективностью функционирования понимается степень соответствия полученных результатов функционирования технической системы требуемым [6]. Анализ математической модели и структурной схемы системы передачи данных показывает, что требуемым результатом функционирования системы передачи данных является обеспечение своевременности, достоверности, помехоустойчивости и скрытности передачи данных. Оценка того, насколько полно реализована своевременность, достоверность, помехоустойчивость и скрытность передачи информации осуществляется с помощью отдельных показателей, отражающих степень выполнения системой передачи данных, функциональной задачи.

Критерии и показатели оценки эффективности функционирования системы передачи данных. Исследуем основные показатели эффективности системы передачи данных, обоснуем критерии и показатели их оценки.

Своевременность – свойство связи, характеризующее ее способность обеспечивать доведение сообщений до получателя за время, не превышающее требуемое [7].

Требуемое время доведения сообщения определяется категорией срочности, которая зависит от важности сообщений. Основным критерием оценки своевременности является вероятность доведения информации до получателя за время, не превышающее требуемое:

$$P_{дов} = \lim_{n_o \to \infty} \frac{n_1}{n_0},$$

где n_0 – общее число переданных сообщений; n_1 – число сообщений, доведенных до получателя за время T, не превышающее требуемое; T – реальное время доведения сообщения до получателя.

Для повышения своевременности связи необходимо увеличить показатель n_1. Это можно достигнуть, путем уменьшения времени T, которое характеризует оперативность связи. Оно включает следующие составляющие:

$$T = T_п + T_{прд} + T_д,$$

где $T_п$ – время подготовки сообщения к передаче; $T_{прд}$ – время передачи сообщения; $T_д$ – время доставки сообщения до получателя.

Время подготовки сообщения к передаче включает в себя:

$$T_п = t_р + t_о + t_д + t_в,$$

где $t_р$ – время принятия решения на организацию связи; $t_о$ – время оформления сообщения; $t_д$ – время доставки сообщения к передающему устройству; $t_в$ – время ввода сообщения в передающее устройство.

Время $t_р$ определяется временными затратами, сопровождающими процесс смены направлений передачи или каналов связи. Чем больше автоматизирован этот процесс и чем выше квалификация технического персонала, тем меньше $t_р$ и выше своевременность связи.

Времена $t_о$, $t_д$, $t_в$ в значительной степени зависят от вида связи, используемой для передачи сообщений. Для их уменьшения необходима автоматизация процессов оформления сообщений и доставки их к передающему устройству, а также повышение классности специалистов, работающих на этих устройствах.

Время передачи сообщения зависит от скорости передачи информации:

$$T_{прд} = J/V,$$

где J – количество информации, передаваемых по каналу связи, бит; V – скорость передачи информации по каналу связи, бит/с.

Для повышения своевременности связи необходимо уменьшить время $T_{прд}$, что может достигаться:

– улучшением технических характеристик каналов связи, т.е. увеличением их пропускной способности;

– сокращением количества информации, подлежащей передаче по каналам связи.

Время доставки сообщения до получателя включает в себя:

$$T_д = t_с + t_{дс} + t_{дп},$$

где $t_с$ – время считывания информации с приемного устройства; $t_{дс}$ – время документирования сообщений; $t_{дп}$ – время доставки документированного сообщения до получателя.

Времена $t_с$, $t_{дс}$, $t_{дп}$ зависят от вида организованной связи и степени автоматизации процесса приема сообщений.

Достоверность – свойство связи, характеризующее ее способность обеспечивать точное воспроизведение передаваемых сообщений в пунктах приема [7].

Общим показателем оценки достоверности связи является вероятность правильного приема $P_{п.п}$. На практике чаще используют обратную величину $P_{ош} = 1 - P_{п.п}$, как показатель потери достоверности связи.

Они определяются таким образом:

$$P_{п.п} = \lim_{n_0 \to \infty} \frac{n_1}{n_0}; \; P_{ош} = \lim_{n_0 \to \infty} \frac{n_2}{n_0},$$

где n_0 – общее число переданных элементов сообщения; n_1 – число правильно принятых элементов сообщения; n_2 – число искаженных при передаче элементов сообщения.

Для повышения достоверности связи необходимо совершенствовать технические средства, предназначенные для преобразования и передачи сигналов, использовать специальные помехоустойчивые коды.

Помехоустойчивость – свойство связи, характеризующее ее способность обеспечивать передачу сообщений с заданной достоверностью в условиях взаимодействия помех всех видов [7].

Количественной мерой помехоустойчивости является минимальное соотношение энергии сигнала к спектральной плотности мощности шума, необходимое для обеспечения требуемой вероятности правильного приема. Этот показатель позволяет при фиксированном уровне достоверности оценить (сравнить между собой) энергетическую эффективность системы передачи данных.

Другими словами, задача повышения помехоустойчивости передачи дискретных сообщений формализовано представляется в виде задачи минимизации соотношения энергии сигнала к спектральной плотности мощности шума при фиксированном показателе потери достоверности – вероятности ошибочного приема сообщения.

Скрытность – свойство связи, характеризующее ее способность противостоять раскрытию противником факта передачи, места передачи и содержания передаваемой информации [7].

Основными показателями оценки скрытности связи является коэффициент засекречивания, коэффициент скрытности связи и безопасное время.

Коэффициент засекречивания определяется как

$$K_з = \frac{N_з}{N_o},$$

где $N_з$ – число закрытых каналов связи; N_o – общее число каналов связи.

Под закрытым каналом связи понимают канал, оснащенный аппаратурой специального преобразования данных.

Коэффициент скрытности связи характеризует относительную долю информации, которая не может быть разведана противником за требуемое время. Численно он определяется из выражения

$$K_г = \frac{J_o - J_p}{J_o},$$

где J_o – общее количество информации; J_p – количество информации, которая может быть разведана противником.

Безопасное время $T_Б$, характеризует время безопасной работы рассматриваемой аппаратуры специального преобразования данных при условии применения противником различных методов криптоанализа.

Безопасное время определяется по критерию минимального риска:

$$T_Б = \min\left\{T_{Б_1}, T_{Б_2}, ..., T_{Б_L}\right\}, \qquad (1)$$

где $T_{Б_i}$ – время безопасной работы рассматриваемой аппаратуры специального преобразования данных при условии применения противником i-го ($i = \overline{1, L}$) метода криптоанализа; L – число известных методов криптоанализа для рассматриваемого криптоалгоритма.

В соответствии с основными положениями теории сложности время, затрачиваемое алгоритмом, как функция размера задачи, называется временной сложностью этого алгоритма S_{B_i} [8].

Тогда соответствующий показатель безопасного времени $T_{Б_i}$ запишется в виде:

$$T_{Б_i} = \frac{S_{B_i}}{\gamma \cdot \Psi}, \qquad (2)$$

где $\gamma = 31622400$ – числовой коэффициент для пересчета секунд в годы; Ψ – производительность вычислительной системы, доступная криптоаналитику (противнику).

Тогда с учетом (2) выражение (1) перепишется в виде:

$$T_Б = \min\left\{\frac{S_{B_1}}{\gamma \cdot \Psi}, \frac{S_{B_2}}{\gamma \cdot \Psi}, ..., \frac{S_{B_L}}{\gamma \cdot \Psi}\right\},$$

что эквивалентно следующей записи:

$$T_Б = \frac{S_{B_{min}}}{\gamma \cdot \Psi},$$

где $S_{B_{min}}$ – временная сложность алгоритма, реализующего наилучший известный метод криптоанализа, $S_{B_{min}} = \min\left\{S_{B_1}, S_{B_2}, ..., S_{B_L}\right\}$.

Для повышения скрытности применяются специальные меры по кодированию, шифрованию и по обеспечению скрытности функционирования системы связи.

Выводы

Проведенный анализ математической модели и структурной схемы системы передачи данных показывает, что требуемым результатом функционирования системы передачи данных является обеспечение своевременности, достоверности, помехоустойчивости и скрытности передачи данных. Оценка того, насколько полно результаты функционирования системы передачи данных соответствуют требуемой своевременности, достоверности, помехоустойчивости и скрытности осуществляется с помощью отдельных показателей. Обоснованные аналитические выражения, позволяют определить степень выполнения системой передачи данных, функциональной задачи.

Список литературы

1. Концепция Национальной программы информатизации одобренной Законом Украины «Про Концепцію Національної програми інформатизації» от 4 февраля 1998 г. № 75/98-ВР.

2. Береза А.М. Основи створення інформаційних систем. – К., 2001. – 214 с.

3. Пономаренко В.С. Проектування інформаційних систем: Навч. посіб. для ВНЗ. – К.:ВЦ Академія, 2002. – 496 с.

4. Пятибратов А.П. Вычислительные системы, сети и телекоммуникации. – М., 2003. – 512 с.

5. Ломовицкий В.В. Основи построения систем и сетей передачи информации: Учебное пособие для вузов. – М.: ГЛТ, 2005. – 382 с.

6. Надежность и эффективность в технике: Справочник. В 10 т. / Ред. совет: В.С. Авдуевский и др. – М.: Машиностроение, 1988. – Т. 3. – 328 с.

7. ДСТУ В 3265 – 95. Зв'язок військовий. Терміни та визначення. – К.:УкрНДІССІ, 1995. – 23 с.

8. Бернард Скляр. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.

Поступила в редколлегию 11.04.2007

Рецензент: д-р физ.-мат. наук, проф. С.В. Смеляков, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.