УДК 681.3

ПОМЕХОУСТОЙЧИВАЯ ПЕРЕДАЧА ДАННЫХ ПО РАДИОКАНАЛУ В ТЕЛЕМЕТРИЧЕСКОЙ СИСТЕМЕ

Шилко К.Н., магистрант; Паскробка Г.С., магистрант

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белошицкий А. П. – канд. техн. наук

Аннотация. Доклад посвящен проблеме повышения защищенности телеметрической информации от несанкционированного доступа и помех структурно-алгоритмическими методами. Рассматриваются особенности, возникающие при передаче телеметрической информации по радиоканалу. Для устранения возникающих искажений предлагается использовать избыточность.

Ключевые слова. Помехоустойчивое кодирование, телеметрическая система, шифрование.

В системах передачи телеметрический информации между летательным или иным объектом и наземным приемным пунктом важное значение имеет помехозащищенность и информационная защита данных при передаче их по радиоканалу.

При разработке способов передачи телеметрической информации по радиоканалу необходимо учитывать следующие факторы передачи сигнала [1]: распространение, дальность и покрытие.

Распространение: Путь и способ, который радиоволна проходит от ее источника (передатчик) до места назначения (приемник). Путь распространения различается в зависимости от частоты радиосигнала. Также он зависит от частоты преломления или отражения радиосигнала от объектов или при прохождении через слои ионосферы.

Дальность: расстояние, на котором качество радиосвязи является достаточным для решения конкретной задачи.

Покрытие: доступность радиосигнала на ожидаемой дальности, когда сигнал не блокирован техногенными или природными преградами.

Эти факторы необходимо учитывать при выборе диапазона частот телеметрической системы, ее технической реализации, методов и способов передачи и обработки информации.

Обобщенная структурная схема телеметрической системы представлена на рисунке 1. Блоки сбора и передачи данных расположены на объекте телеметрии, а блоки приема и обработки данных – у получателя.

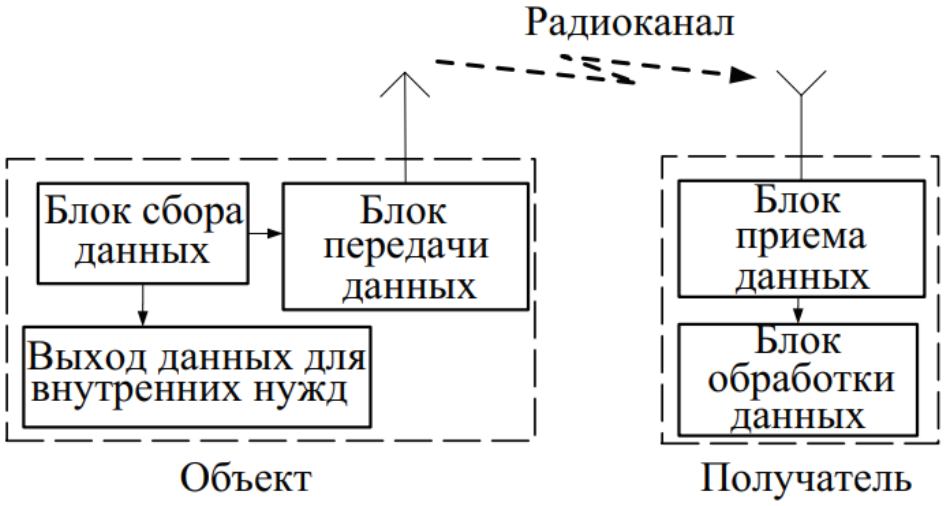

Рисунок 1 – Обобщенная структурная схема телеметрической системы

В системах цифровой передачи данных информации при прохождении сигнала по каналу передачи данных (рисунок 2) сигнал подвергается различным изменениям (искажениям) под действием шумов [1,2]. Это ведет за собой нарушение целостности передаваемой информации и может привести к сбоям в работе.

Рисунок 2 – Обобщенная структурная схема канала передачи данных телеметрической системы

Для контроля целостности данных предлагается использовать циклические избыточные коды (CRC). Алгоритм CRC базируется на свойствах деления с остатком двоичных многочленов, то есть многочленов над конечным полем $GF(2)$. Значение CRC является по сути остатком от деления многочлена, соответствующего входным данным, на некий фиксированный порождающий многочлен. Количество различных многочленов степени, меньшей N, равно 2^N, что совпадает с числом всех двоичных последовательностей длины N. Значение контрольной суммы в алгоритме с порождающим многочленом $G(x)$ степени N определяется как битовая последовательность длины N, представляющая многочлен $R(x)$, получившийся в остатке при делении многочлена $R(x)$, представляющего входной поток бит, на многочлен $G(x)$:

$$R(x) = P(x) * x^n \bmod G(x) \quad (1)$$

Где $R(x)$ – многочлен, представляющий значение CRC, $P(x)$ – многочлен, коэффициенты которого представляют входные данные, $G(x)$ – порождающий многочлен, N – степень порождающего многочлена.

Для защиты данных от несанкционированного доступа предлагается использовать шифр AES128. AES – блочный шифр с длиной блоков равной 128 битам, и шифр поддерживает ключи длиной N_k, равной 128, 192 или 256 бит.

В начале зашифровывания input копируется в массив State по правилу $state[r,c] = input[r+4c]$, для $0 \le r \le 4$ и $0 \le c \le Nb$. После этого к State применяется процедура AddRoundKey(), и затем State проходит через процедуру трансформации (раунд) 10, 12, или 14 раз (в зависимости от длины ключа), при этом надо учесть, что последний раунд несколько отличается от предыдущих. В итоге, после завершения последнего раунда трансформации, State копируется в output по правилу $output[r+4c] = state[r,c]$.

В помехоустойчивом кодировании широко применяется код Рида – Соломона. При использовании этого кода на выходе кодера образуется избыточное сообщение для дальнейшей передачи. В кодах Рида-Соломона сообщение представляется в виде набора символов некоторого алфавита. При построении кода Рида-Соломона задается пара чисел N, K, где N – общее количество символов, а K – «полезное» количество символов, остальные $N-K$ символов представляют собой избыточный код, предназначенный для восстановления ошибок. Структура данных в этом случае имеет вид, представленный на рисунке 3.

Рисунок 3 – Структурная схема пакета данных

Такой код будет иметь так называемое «расстояние Хэмминга» D = N–K+1; Расстояние Хэмминга является параметром кода и определяется как минимальное число различий между двумя различными кодовыми словами. В соответствии с теорией кодирования, код, имеющий расстояние Хемминга D = 2t+1, позволяет восстанавливать t ошибок данных при передаче по радиоканалу в телеметрической системе.

Для оценки достоверности передачи с использованием помехоустойчивого кодирования и без него использовалась среда имитационного моделирования MATLAB. Установлено, что применение кодирования позволяет повысить достоверность при передаче информации через канал передачи данных. Преимуществами использования выбранных кодов являются: простота реализации, кодирование и декодирование потоков данных непрерывно во времени, возможность обнаруживать и частично восстанавливать практически уничтоженную информацию.

Список использованных источников:

1. Рихтер С.Г. Кодирование и передача речи в цифровых системах подвижной радиосвязи. – М.: Горячая линия – Телеком, 2018. – 302 с.

2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

UDC 681.3

INTERFERENCE DATA TRANSMISSION ON A RADIO CHANNEL IN A TELEMETRIC SYSTEM

Shilko K.N., Master Student; Paskrobka G.S., Master Student

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Beloshitskiy A.P.– PhD

Annotation. The report is devoted to the problem of increasing the security of telemetric information from unauthorized access and interference by structural and algorithmic methods. The features that arise during the transmission of telemetric information over a radio channel are considered. To eliminate the arising distortions, it is proposed to use redundancy.

Keywords. Anti-jamming coding, telemetry system, encryption.