Литература:

1. *Хокинс Д., Блейксли С.* Об интеллекте. – Москва-Санкт-Петербург-Киев: Издательский дом «Вильямс», 2007. – 313 с.

2. *Пенроуз Р.* Новый ум короля. О компьютерах, мышлении и законах физики. – Москва: Едиториал УРСС, 2003. – 600 с.

3. *Белда И.* Разум, машины и математика. – Москва: Де Агостини, 2014. – 400 с.

4. *Рассел С., Норвиг П.* Искусственный интеллект. Современный подход. – Москва-Санкт-Петербург-Киев: Издательский дом «Вильямс», 2016. – 1408 с.

5. *Баррат Д.* Последнее изобретение человечества. – Москва: Альпина нон-фикшн, 2015. – 292 с.

6. *Бостром Н.* Искусственный интеллект. Этапы. Угрозы. Стратегии. – Москва: ООО «Манн, Иванов и Фербер», 2016. – 368 с.

7. *Домингос П.* Верховный алгоритм. – Москва: ООО «Манн, Иванов и Фербер», 2015. – 352 с.

8. *Форд М.* Роботы наступают. – Москва: Альпина нон-фикшн, 2016. – 416 с.

9. *Василенко М.Н., Трохов В.Г., Василенко П.А., Пронин В.П.* К вопросу цифровизации ведения технической документации // Железнодорожный транспорт. – 2020. – № 10. – С. 56-62.

Сидоренко А.А., Тедеев Ю.Р.

Повышение информационной безопасности каналов управления путем применения корректирующих кодов

Аннотация: Актуальной задачей является обеспечение информационной безопасности каналов управления. Наиболее уязвимым для внешних воздействий является радиоканал управления. Применение корректирующих кодов положительно влияет на все аспекты информационной безопасности. Наиболее целесообразно применение помехоустойчивых кодов, адаптивных к состоянию канала передачи команд управления.

Ключевые слова: информационная безопасность, корректирующие коды, каскадные коды, турбокоды

Информационная безопасность состоит в защите конфиденциальности, целостности и доступности информации [1]. В качестве одного из методов обеспечения информационной безопасности каналов управления может быть использовано помехоустойчивое кодирование.

Применение корректирующих (помехоустойчивых) кодов, с использованием которых кодируется передаваемая по каналу управления информация, положительно влияет на все перечисленные составляющие информационной безопасности: конфиденциальность, целостность и доступность информации. На выходе процедуры кодирования получается закодированный сигнал, обладающий структурной избыточностью, необходимой для реализации возможности исправления ошибок.

Кодирование информации кодом, параметры которого удалось сохранить в тайне от стороны, осуществляющей несанкционированный доступ, повышают конфиденциальность передаваемой информации. При этом следует учесть тот факт, что кодирование информации корректирующим кодом преследует цель повышения устойчивости к возникающим в процессе передачи ошибкам, и не является полноценной криптозащитой.

Способность корректирующих кодов исправлять ошибки повышает целостность передаваемой информации, что, в свою очередь, обеспечивает доступность информации легальному пользователю (устройству).

Осуществление управления с использованием радиоканала затрудняется тем, что в радиоканале передаваемые сигналы подвержены искажениям и затуханию из-за негативного воздействия многочисленных факторов. В этом случае применение корректирующих кодов наиболее целесообразно.

Семейство корректирующих кодов достаточно разнообразно. Коды различаются длинной сообщения, степенью вводимой избыточности, методами кодирования-декодирования, способностью исправлять одиночные и групповые ошибки [2]. Параметры кода определяются множеством факторов, например, длинной передаваемого сообщения (управляющей команды),

характеристиками канала передачи информации, допустимой вероятностью битовой ошибки в принятой управляющей команде.

История корректирующих кодов длится уже три четверти века. Со временем, для улучшения корректирующей способности коды начали соединять в разнообразные комбинации. Было выяснено, что даже для варианта соединения двух относительно простых кодов в комбинацию, можно получить код с весьма высокой корректирующей способностью [3-4]. К комбинированным кодам принято относить турбокоды, каскадные коды, коды произведения, гибридные коды, сигнально-кодовые конструкции [5]. Комбинирование кодов более значительно повышает конфиденциальность информации, так как осуществляя несанкционированный доступ, необходимо знать параметры уже нескольких кодов.

Совместно с комбинированием кодов часто применяют перемежение бит по определенному алгоритму, реализуемое с целью рассредоточения пакетов ошибок, осуществляя на приемной стороне обратную процедуру. Перемежение бит способно значительно повысить конфиденциальность информации.

Одними из самых распространенных комбинированных кодов являются последовательные каскадные коды (далее – ПКК). В ПКК кодирование осуществляется в два уровня [6]. Входные данные сначала кодируются внешним кодом, а затем внутренним. Декодирование происходит в обратном порядке. За преимущества, получаемые от применения помехоустойчивого кодирования, приходится «расплачиваться» ростом избыточности. Для случая применения каскадного кода рост избыточности особенно значителен.

Качество канала связи может изменяться под воздействием разнообразных факторов. Большой нестабильностью обладает качество КВ и УКВ радиосвязи, особенно подвижной [7-8]. Корректирующая способность кода выбирается исходя из необходимости обеспечения допустимой вероятности ошибки в принятом сообщении (управляющей команде) при наихудшем прогнозируемом состоянии канала передачи данных. При этом, в случае благоприятного состояния канала передачи данных из-за неоправданной избыточности расходуется дополнительно ресурс по энергетике и по времени доставки сообщения, что создает

проблему. Рассмотрим один из вариантов решения данной проблемы применительно к последовательному каскадному коду.

Предлагается модифицированный метод последовательного кодирования, позволяющий регулировать избыточность и корректирующую способность ПКК, изменяя долю кодовых бит внешнего кода, кодируемых внутренним кодом [9]. Для удобства назовем такой ПКК гибким ПКК (далее – ГПКК). Наиболее простым методом регулировки избыточности является перфорация кодовой последовательности, но такой метод сложно применим при использовании блочных кодов. ГПКК может быть реализован при каскадном соединении любых кодов. Упрощенная структурная передачи данных с применением ГПКК изображена на рисунке 1.

В настоящее время особую важность приобретают вопросы организации управления с использованием радиоканала при работе средств радиоэлектронного подавления (РЭП). Вследствие воздействия РЭП в канале передачи значительно возрастает вероятность битовой ошибки. При высокой вероятности возникновения ошибки наиболее эффективными среди помехоустойчивых кодов считаются турбокоды, применяемые в разнообразных стандартах: CDMA-2000, INTELSAT, IEEE 802.16, WiMax, DVB-RCS, UMTS, 3GPP LTE, TIA-1008, DMR.

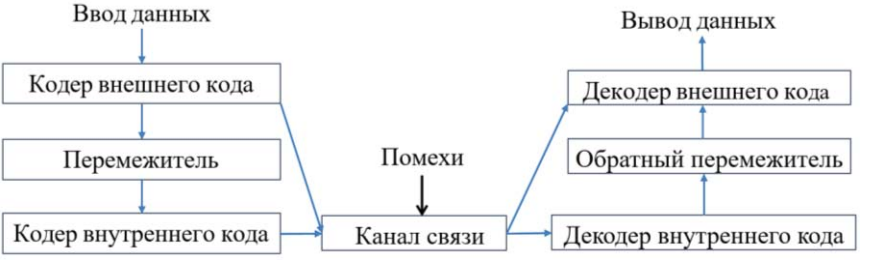

Рисунок 1 – Структурная передачи данных с применением ГПКК

Турбокод является развитием системы каскадного кодирования путем применения итеративного декодирования. Рассмотрим принципы построения турбокодов, изложенные в многочисленных источниках [4, 10-11]. Как видно из структурной схемы N – размерного кодера турбокода (рисунок 2), на выходе кодера

турбокода поток передаваемых данных состоит из последовательности информационных бит и N последовательностей проверочных бит. На входе декодера из принятой последовательности формируется N кодовых слов. Декодер турбокода реализует итеративное декодирование, в ходе которого осуществляется передача мягкого решения с выхода одного декодера на вход другого с повторением данной процедуры до тех пор, пока не будет достигнута необходимая точность принятия решения.

Каждый информационный бит принятого кодового слова турбокода участвует в формировании N слов на входе декодера. Исходя из отмеченных особенностей и проведенных исследований [12], можно сделать вывод о высокой чувствительности декодера турбокода к достоверности значений информационных бит кодового слова. Негативной стороной такой чувствительности является высокая вероятность ошибки декодирования при наличии ошибок в информационных битах кодового слова. Предлагается осуществлять дополнительное кодирование информационных бит кодового слова турбокода, что повысит их достоверность и благоприятно отразится на корректирующей способности кода. Будем называть такой турбокод – турбокодом с дополнительным кодированием информационных бит. Недостатком дополнительного кодирования всего блока информационных бит является значительный рост избыточности. Возникающую избыточность можно снизить, дополнительно кодируя только часть информационных бит.

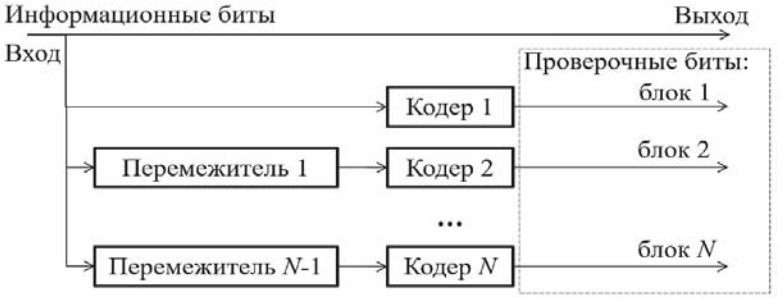

Рисунок 2 – Структурная схема N – размерного кодера турбокода

Современные люди окружены устройствами, использующими в своей работе алгоритмы помехоустойчивого кодирования. Технологии помехоустойчивого кодирования стали обязательным элементом систем хранения и передачи данных. Современные кодеры и декодеры реализуются на практике применением как аппаратных методов на базе микропроцессоров фирм Xilinx, AHA, Analog Devices, так и программных.

Наиболее гибким является применение программных кодеров-декодеров. Совместить программную реализацию с аппаратной в настоящее время стало как никогда просто. Для этого, например, можно использовать микрокомпьютеры Raspberry Pi или микроконтроллеры на базе платформы Arduino, на вычислительных мощностях которых будут функционировать кодер и декодер корректирующего кода. Микрокомпьютер Raspberry Pi использует язык программирования Python, а язык контроллера Arduino синтаксически достаточно схож с C++. Радиоканал при этом может быть организован на основе одного из программируемых модулей беспроводной передачи данных, например: NRF24L01, TEA576-7FM, MBee, HC-12.

Литература:

1. ГОСТ Р 1.0-2004. Практические правила управления информационной безопасностью.

2. *Голиков А.М.* Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика: учеб. пособие для вузов. – СПб.: Лань, 2022. – 452 с.

3. *Матвеев Б.В.* Основы корректирующего кодирования. Теория и лабораторный практикум: учеб. пособие. – СПб.: Лань, 2014. – 192 с.

4. *Аджемов А.С., Санников В.Г.* Общая теория связи: учебник для вузов. – М.: Горячая линия-Телеком, 2023. – 624 с.

5. *Варгузин В.А., Цикин И.А.* Методы повышения энергетической и спектральной эффективности цифровой радиосвязи. – СПб.: БХВ-Петербург, 2013. – 352 с.

6. *Форни Д.* Каскадные коды. – М.: Мир, 1970. – 207 с.

7. *Карболин В.А., Носов В.И.* Исследование влияния скорости передачи и частоты дискретизации импульсной характеристики на

помехоустойчивость КСШП-системы радиосвязи // Вестник СибГУТИ. – 2018. – № 2. – С. 71-83.

8. *Перфилов О.Ю.* Радиопомехи: учебн. пособие для вузов. – М.: Горячая линия-Телеком, 2016. – 110 с.

9. *Sidorenko A.A.* Overview of the International Conference on Applied Physics, Information Technologies and Engineering – APITECH-V-2023 // Journal of Physics: Conference Series. – 2024. – Vol. 2697(1). – P. 012038 (1-7).

10. *Красносельский И.Н.* Турбокоды: принципы и перспективы // Электросвязь. – 2001. – № 1. – С. 17-20.

11. *Паньшо С.П., Югай В.В.* Турбокодирование // Успехи современной радиоэлектроники. – 2004. – № 2. – С. 3-16.

12. *Sidorenko A.A.* Overview of the International Conference on Applied Physics, Information Technologies and Engineering – APITECH III 2021 // Journal of Physics: Conference Series. – 2021. – Vol. 2094(1). – P. 032061(1-9).