УДК 004.056.2
DOI 10.21685/2072-3059-2020-3-4

Ю. Ю. Синицын, А. Б. Сизоненко

ВОССТАНОВЛЕНИЕ СИНХРОНИЗАЦИИ ПРИ РАСШИФРОВАНИИ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ МОДИФИЦИРОВАННОГО АЛГОРИТМА ДЕКОДИРОВАНИЯ ПО ВИТЕРБИ

Аннотация.

Актуальность и цели. Современные системы передачи данных, использующие криптографические методы защиты информации, требуют обеспечения высоких показателей надежности и качества передачи информации. Объектом исследования являются защищенные системы передачи данных. Предметом исследования являются различные способы исправления ошибок в канале связи. Цель исследования – разработка алгоритма восстановления синхронизации шифра и гаммы при расшифровании с использованием свойств сверточных кодов после передачи сообщения по каналу связи с помехами.

Материалы и методы. Исследование проводилось с использованием среды Matlab, модели декодера сверточных кодов по алгоритму Витерби.

Результаты. Разработаны алгоритм и структурная схема устройства, реализующего восстановление синхронизации шифра и гаммы при расшифровании сообщения после прохождения канала связи с помехами.

Выводы. Влияние искажения типа потеря бита на переданное по каналу связи с помехами сообщение способно привести к рассинхронизации шифра и гаммы при расшифровании сообщения. Анализ процесса декодирования сообщения по алгоритму Витерби даст возможность обнаружения и устранения данного типа помех.

Ключевые слова: защищенные системы передачи данных, сверточные коды, алгоритм Витерби, синхронизация зашифрованного сообщения и гаммы.

Yu. Yu. Sinitsyn, A. B. Sizonenko

SYNCHRONIZATION RECOVERY WHEN DECODING MESSAGES USING A MODIFIED VITERBI DECODING ALGORITHM

Abstract.

Background. Modern data transmission systems using cryptographic methods of information protection require high reliability and quality of information transmission. The object of research is protected data transmission systems. The subject of research is various ways to correct errors in the communication channel. The purpose of this work is to develop an algorithm for restoring the synchronization of the cipher and gamma when decrypting, after transmitting a message over a communication channel with interference, using the properties of convolutional codes.

Materials and methods. The study was conducted using the Matlab environment. Models of convolutional code decoder using the Viterbi algorithm.

Results. An algorithm and a block diagram of a device that implements the restoration of synchronization of the cipher and gamma when decrypting a message, after passing a communication channel with interference, have been developed.

Conclusions. The effect of distortion such as bit loss on a message transmitted over a communication channel with interference can lead to desynchronization of the cipher and gamma when decrypting the message. Analysis of the message decoding process using the Viterbi algorithm will make it possible to detect and eliminate this type of interference.

Keywords: secure data transmission systems, convolutional codes, Viterbi algorithm, encrypted message and gamma synchronization.

Введение

Для защищенных систем передачи данных одной из наиболее приоритетных задач является обеспечение высоких показателей надежности и качества передачи информации. Для этого система должна обладать требуемой помехоустойчивостью, которая характеризует способность системы сохранять заданные количественные и качественные показатели, несмотря на наличие помех в канале связи.

В защищенных системах передачи данных между источником информации и приемником информации возникает символьная синхронизации. При воздействии помех на передаваемое сообщение возможно изменение одного или группы символов, удаление или добавление лишних символов [1].

Изменение зашифрованных данных приведет к искажению данных при расшифровании. Для обнаружения и исправления ошибок, вызванных помехами в канале связи, используют корректирующие коды. Корректирующие коды не способны исправлять искажения кодовой последовательности с потерянным или добавленным битом. Модификация алгоритмов декодирования корректирующих кодов позволяет устранить такие виды искажений. Это приведет к восстановлению синхронизации при расшифровании сообщений в защищенных системах передачи данных.

Анализируя процесс декодирования по Витерби при нарастании значений метрик путей, можно определить характер искажений кодовой последовательности и попытаться восстановить потерянные или удалить добавленные биты.

Проблемы синхронизации в защищенных системах передачи данных

В защищенных системах передачи данных изменение одного или группы символов приведет к невозможности расшифровать данные символы, а потеря либо добавление символов при передаче приведет к рассинхронизации зашифрованного сообщения и гаммы, в результате чего расшифрование сообщения с места потери или добавления символов станет невозможным (рис. 1) [2].

Одним из способов уменьшения влияния помех на искажение зашифрованного сообщения является применение помехоустойчивого кодирования. Сверточные коды широко применяют среди кодов, исправляющих ошибки. Сверточные коды сегодня используются как отдельно, так и в совокупности

с блочными кодами. Например: код Рида – Соломона образует каскадные коды при последовательном кодировании и турбокоды – при параллельном кодировании данных.

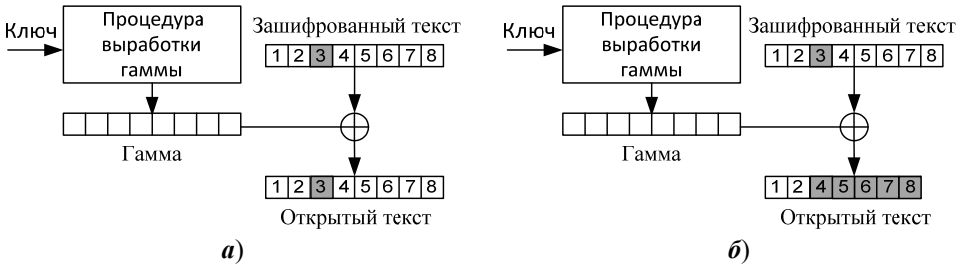

Рис. 1. Влияние помех на зашифрованное сообщение:
а – изменение символа; ***б*** – потеря символа

Схема защищенной системы передачи данных, использующей в качестве корректирующего кода сверточный код, представлена на рис. 2.

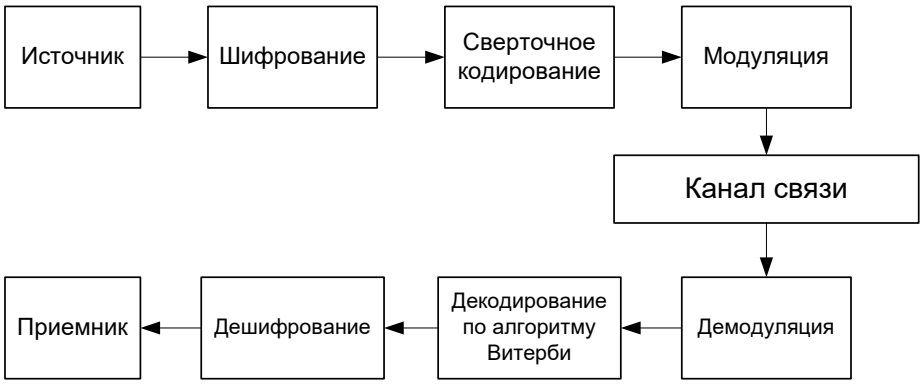

Рис. 2. Схема защищенной системы передачи данных

Одним из методов декодирования сверточных кодов является алгоритм Витерби [3]. Данный метод осуществляет поиск наиболее подходящего списка состояний, которые имеют наибольшую вероятность произошедших событий.

Алгоритм Витерби основан на методе максимального правдоподобия. На каждом такте декодирования для каждой ветви решетки кода вычисляется метрика – число, характеризующее степень отличия бит, генерируемых данной ветвью от принятого кодового слова.

Ошибка по каждой ветви служит метрикой d_H расстояния Хэмминга и соответствует числу отличающихся от требуемых принятых символов.

Суммарная метрика $d_{\sum H}$ по каждому из возможных путей определяется как метрика путей.

Алгоритм Витерби выбирает путь с наименьшей суммарной метрикой и отбрасывает те пути, которые превышают некоторую пороговую величину в данный момент времени [4].

Анализ влияния искажений на декодирование кодовой последовательности

Рассмотрим работу декодера на примере сверточного кода с порождающими полиномами $G_1(x)=1+x+x^2$, $G_2(x)=1+x^2$ и скоростью кодирования $k/n = 1/2$, где k – количество входных бит данных; n – количество выходных бит данных.

Закодируем сверточным кодером с вышеуказанными характеристиками последовательность из двадцати символов $m = 11011011001101110100$. Закодированная последовательность выглядит следующим образом:

$$U = 11\text{-}01\text{-}01\text{-}00\text{-}01\text{-}01\text{-}00\text{-}01\text{-}01\text{-}11\text{-}11\text{-}01\text{-}01\text{-}00\text{-}01\text{-}10\text{-}01\text{-}00\text{-}10\text{-}11.$$

Корректирующая способность выбранного кода позволяет исправить две подряд ошибки бит. При воздействии тройной ошибки декодер неверно декодирует один бит исходной последовательности.

Рассмотрим два случая воздействия пакета из восьми ошибок на переданную кодовую последовательность и потери одного бита переданной последовательности.

На рис. 3 показан процесс декодирования по алгоритму Витерби при воздействии на переданную кодовую последовательность пакета ошибок из восьми бит. Из канала связи получена следующая последовательность:

$$Z = 11\text{-}01\text{-}01\text{-}00\text{-}10\text{-}\mathbf{10\text{-}11\text{-}01\text{-}10}\text{-}11\text{-}11\text{-}01\text{-}01\text{-}00\text{-}01\text{-}10\text{-}01\text{-}00\text{-}10\text{-}11$$

(ошибки выделены полужирным шрифтом).

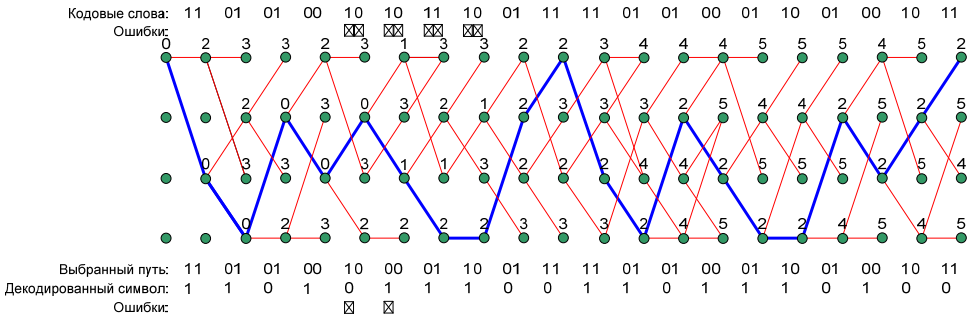

Рис. 3. Процесс декодирования кодовой последовательности, искаженной пакетом из восьми ошибок

При работе декодер неверно декодирует пятый и шестой бит исходной последовательности. После окончания влияния помехи на последовательность все последующие биты исходной последовательности декодер декодирует верно. Процесса нарастания метрик путей не наблюдается.

Рассмотрим работу декодера при воздействии искажения потери символа на переданную кодовую последовательность. В данном примере при передаче данных был потерян девятый бит. Из канала связи получена последовательность

$$Z_1 = 11\text{-}01\text{-}01\text{-}00\text{-}10\text{-}10\text{-}00\text{-}10\text{-}11\text{-}11\text{-}10\text{-}10\text{-}10\text{-}00\text{-}11\text{-}00\text{-}10\text{-}01\text{-}01\text{-}10$$

(последним символом добавлен 0 для завершения процесса декодирования).

При работе декодера мы наблюдаем неверное декодирование десяти бит исходной последовательности начиная с места потери бита. Из-за потери одного бита кодовой последовательности в кодовых словах начиная с места потери происходит сдвиг бит данных. Происходит нарастание количества ошибок при декодировании. При работе декодера мы наблюдаем нарастание значений метрик путей.

При работе декодера с принятой кодовой последовательностью без ошибок максимальное значение метрики пути наблюдалось три (рис. 2, 3). При декодировании принятой кодовой последовательности с пакетом из восьми ошибок максимальное значение метрики пути наблюдалось пять (рис. 3), и после окончания влияния помехи увеличение значений метрик путей не наблюдалось. При декодировании принятой кодовой последовательности с одной ошибкой потери символа наблюдается рост метрик путей от начала влияния помехи до последнего кодового слова принятой кодовой последовательности (рис. 4).

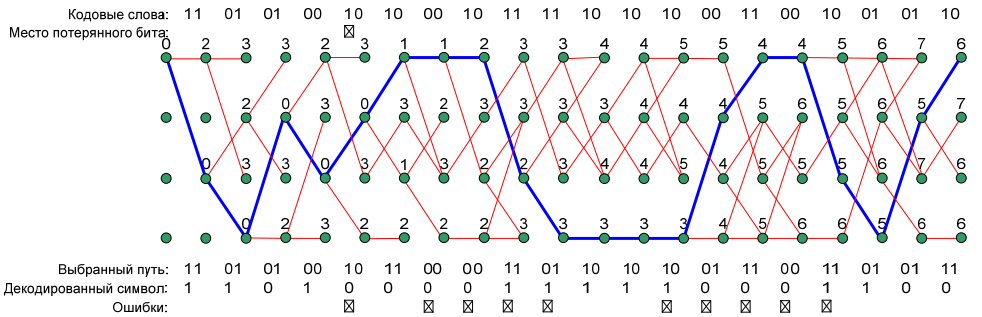

Рис. 4. Процесс декодирования последовательности с ошибкой потери бита

Алгоритм декодирования сверточных кодов для восстановления рассинхронизации при расшифровании сообщения

В предлагаемом алгоритме при получении данных от демодулятора счетчик бит данных производит расчет принятых бит и отправляет полученное значение на устройство управления (УУ) (рис. 5).

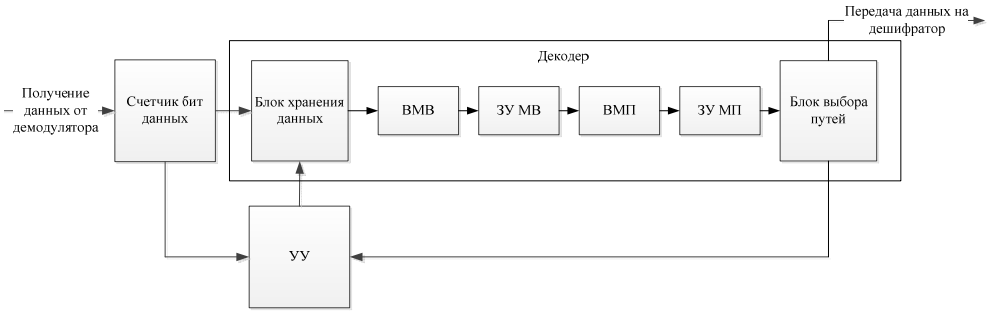

Рис. 5. Структурная схема алгоритма декодирования для устранения рассинхронизации при расшифровании сообщения

В устройстве управления происходит сравнение количества принятых бит со значением стандарта размера фрагмента при передаче данных. В соот-

ветствии с результатами сравнения устройство управления принимает решение об алгоритме декодирования. Предложено использовать два алгоритма декодирования. При совпадении количества принятых бит со значением стандарта размера фрагмента данных необходимо использовать алгоритм декодирования с инверсией бит данных (без добавления бит). При несовпадении количества принятых бит со значением стандарта размера фрагмента данных – использовать алгоритм декодирования с добавлением бит данных (рис. 6).

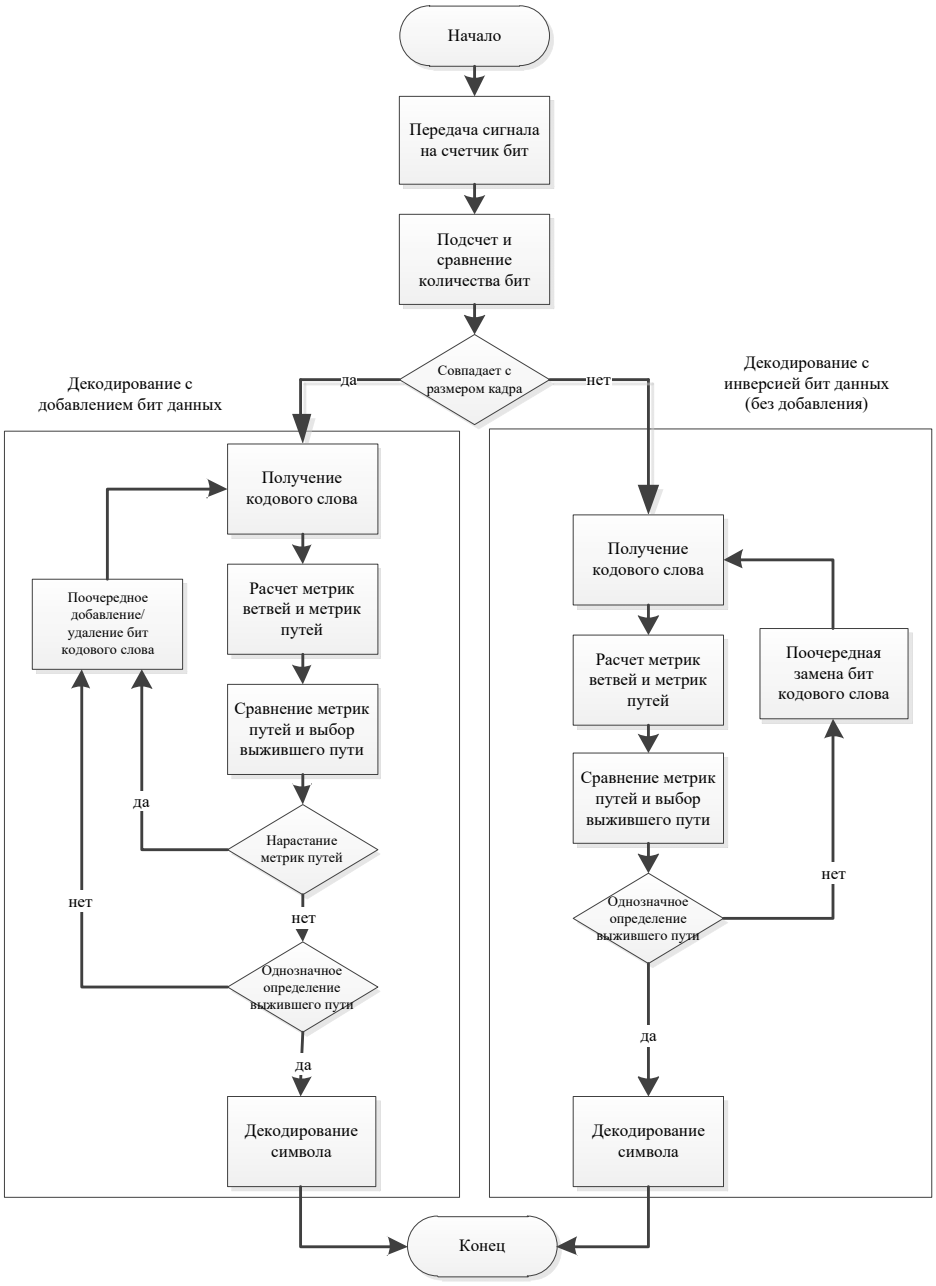

Рис. 6. Блок-схема алгоритма декодирования для устранения рассинхронизации при расшифровании сообщения

После прохождения счетчика бит данных кодовая последовательность направляется в декодер. Принятая последовательность хранится в блоке хранения данных и декодируется по алгоритму Витерби. Блок ВМВ декодера вычисляет метрики ветвей и передает данные о значении метрик в запоминающее устройство метрик ветвей ЗУ МВ. Запоминающее устройство метрик ветвей передает значение метрик в блок вычисления метрик путей ВМП. Хранение данных метрик путей осуществляется в запоминающем устройстве метрик путей ЗУ МП. Данные из запоминающего устройства метрик путей передаются и анализируются в блоке выбора путей. При нарастании метрик путей и невозможности однозначного выбора пути блок выбора путей отправляет сигнал в устройство управления УУ (рис. 5). Устройство управления останавливает процесс декодирования и возвращает процесс декодирования на кодовое слово, с которого не удается однозначно декодировать бит исходной последовательности.

В этом месте в зависимости от принятого алгоритма декодирования (рис. 6) устройство управления принимает решение об инверсии, удалении или добавлении бит данных в кодовом слове. После изменения бит данных производится новый расчет метрик ветвей и сравнение метрик путей. Если нарастание метрик путей прекратилось и неоднозначность декодирования разрешилась, декодирование продолжается в обычном режиме.

Декодированные биты исходной последовательности данных передаются на дешифратор, где в соответствии с ключом и режимом шифрования происходит процесс расшифрования сообщения.

Декодирование представленным алгоритмом позволит улучшить корректирующую способность декодера сверточных кодов. Это позволит устранить рассинхронизацию зашифрованного сообщения и гаммы, вызванную инверсией, потерей, добавлением бит данных, при передаче сообщения по каналу связи с помехами.

Заключение

Уменьшить влияние помех на зашифрованное сообщение, передаваемое по каналу связи, возможно, используя свойства сверточных кодов. Представленный алгоритм позволяет уменьшить влияние ошибок на передаваемое сообщение, это дает возможность устранить рассинхронизацию зашифрованного сообщения и гаммы и улучшить качество передачи сообщений по каналам связи защищенных систем передачи данных.

Алгоритм, представленный в данной статье, возможно применять как для декодирования по алгоритму Витерби с жестким решением, так и для декодирования по алгоритму Витерби с мягким решением.

Данный алгоритм можно также использовать для каскадных кодов и турбокодов, которые в качестве внутреннего кода используют сверточные коды.

Библиографический список

1. **Сизоненко, А. Б.** Использование свойств сверточных кодов для устранения рассинхронизации при расшифровании сообщений, зашифрованных синхронными поточными шифрами / А. Б. Сизоненко // Информационные системы и технологии. – 2013. – № 1. – С. 41–46.

2. **Синицын, Ю. Ю.** Анализ влияния помех в канале связи на процесс расшифрования сообщений, зашифрованных в различных режимах / Ю. Ю. Синицын, А. Б. Сизоненко, А. В. Колованов // Информационные системы и технологии – 2020 : сб. материалов XXVI Междунар. науч.-техн. конф. – Нижний Новгород : Нижегород. гос. техн. ун-т им. Р. Е. Алексеева, 2020. – С. 637–642.
3. **Никитин, Г. И.** Сверточные коды : учеб. пособие / Г. И. Никитин. – Санкт-Петербург : СПбГУАП, 2001. – 80 с.
4. **Скляр, Б.** Цифровая связь. Теоретические основы и практическое применение : пер. с англ. / Б. Скляр. – Изд. 2-е, испр. – Москва : Вильямс, 2004. – 1104 с.

References

1. Sizonenko A. B. *Informatsionnye sistemy i tekhnologii* [Information systems and technologies]. 2013, no. 1, pp. 41–46. [In Russian]
2. Sinitsyn Yu. Yu., Sizonenko A. B., Kolovanov A. V. *Informatsionnye sistemy i tekhnologii – 2020: sb. materialov XXVI Mezhdunar. nauch.-tekhn. konf*. [Information systems and technologies – 2020: proceedings of XXVI International scientific and practical conference]. Nizhniy Novgorod: Nizhegorod. gos. tekhn. un-t im. R. E. Alekseeva, 2020, pp. 637–642. [In Russian]
3. Nikitin G. I. *Svertochnye kody: ucheb. posobie* [Convolutional codes: teaching aid]. Saint-Petersburg: SPbGUAP, 2001, 80 p. [In Russian]
4. Sklyar B. *Tsifrovaya svyaz'. Teoreticheskie osnovy i prakticheskoe primenenie* [Digital communication. Theoretical foundations and practical application]. 2nd ed. rev.: transl. from Engl. Moscow: Vil'yams, 2004, 1104 p. [In Russian]

Синицын Юрий Юрьевич
адъюнкт, Краснодарское высшее военное училище (Россия, г. Краснодар, ул. Красина, 4)

E-mail: Sinia90@mail.ru

Sinitsyn Yuriy Yur'evich
Postgraduate student, Krasnodar Higher Military School (4 Krasina street, Krasnodar, Russia)

Сизоненко Александр Борисович
доктор технических наук, начальник кафедры защиты от несанкционированного доступа, Краснодарское высшее военное училище (Россия, г. Краснодар, ул. Красина, 4)

E-mail: siz_al@mail.ru

Sizonenko Aleksandr Borisovich
Doctor of engineering sciences, head of the sub-department of protection against unauthorized access, Krasnodar Higher Military School (4 Krasina street, Krasnodar, Russia)

Образец цитирования:

Синицын, Ю. Ю. Восстановление синхронизации при расшифровании сообщений с использованием модифицированного алгоритма декодирования по Витерби / Ю. Ю. Синицын, А. Б. Сизоненко // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2020. – № 3 (55). – С. 36–43. – DOI 10.21685/2072-3059-2020-3-4.