Информационные процессы, Том 25, № 2, 2025, стр. 169–174.

ПЕРЕДАЧА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Метод превращения стандартной цифровой конвенциальной системы радиосвязи в систему, защищённую от нелегального абонента

В. В. Зяблов[*], В. Г. Потапов[*], В. Р. Сидоренко[**]

[*] *ФГБУН «Институт проблем передачи информации им. А.А. Харкевича», Российская академия наук, Москва, Россия*

[**] *«Технический университет г.Мюнхен», Мюнхен, ФРГ*

Поступила в редколлегию 03.07.2025 г. Принята 25.07.2025 г.

Аннотация—Предлагается простой метод превращения стандартной цифровой беспроводной конвенцльной системы связи в систему радиосвязи, в которой нелегальный абонент, зная используемые метод помехоустойчивого кодирования и вид модуляции, не может прочитать передаваемое сообщение.

КЛЮЧЕВЫЕ СЛОВА: радиосвязь, скремлирование, несанкционированный доступ, теория информации.

DOI: 10.53921/18195822_2025_25_2_169

1. ВВЕДЕНИЕ

Беспроводная связь, включая беспроводные сети, стала широко распространенной в обществе. Улучшения в беспроводной связи жизненно важны для повышения ее надежности. Во многих протоколах связи данные шифруются перед передачей. Это делается не только для того, чтобы сделать данные на передатчике относительно случайными и предотвратить модуляцию длинных последовательностей единиц или нулей, которые часто встречаются во входных данных, но и для того, чтобы защитить передаваемую информацию от несанкционированного доступа. В работах [2,3] мы рассматривали коммуникационную звездообразную сеть с центральной станцией и пользователями. Передача по зашумленным каналам от центральной станции к пользователям и обратно использовалось кодирование с исправлением ошибок. Модифицированная сеть предполагала, что у каждого пользователя есть секретный ключ, также известный центральной станции. В данной работе рассматривается конвенциональная система цифровой радиосвязи. Передача информации по зашумленным каналам между абонентами также использует кодирование с исправлением ошибок. Обычно код с исправлением ошибок открыт для всего мира (он не является секретом). Это позволяет нелегальному пользователю получить несанкционированный доступ к передаваемым данным. Мы предлагаем изменить код и физический протокол передачи так, чтобы защитить радиосеть от ошибок канала и несанкционированного доступа с использованием того же кода. Модифицированная сеть предполагает, что у каждого абонета есть секретный ключ.

2. ПОСТАНОВКА ЗАДАЧИ

Рассмотрим конвенциональную систему цифровой радиосвязи, которая является традиционным вариантом беспроводной связи, реализуемой абонентскими радиостанциями. В таких

системах реализуются следующие виды вызовов: индивидуальный, групповой, передача коротких сообщений. Для простоты изложения рассмотрим конвенциональную систему цифровой симплексной радиосвязи, в которой в каждый момент времени информация передаётся только в одном направлении.

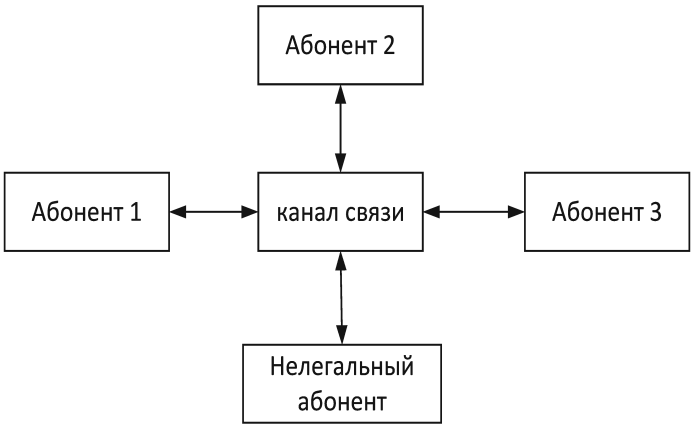

Рис. 1. Конвенциональная система связи

.

Без потери общности, рассмотрим упрощенную блок-схему стандартной цифровой беспроводной прямой линии связи при индивидуальном вызове абонента 1 – абонента 3 (см. Рис. 2).

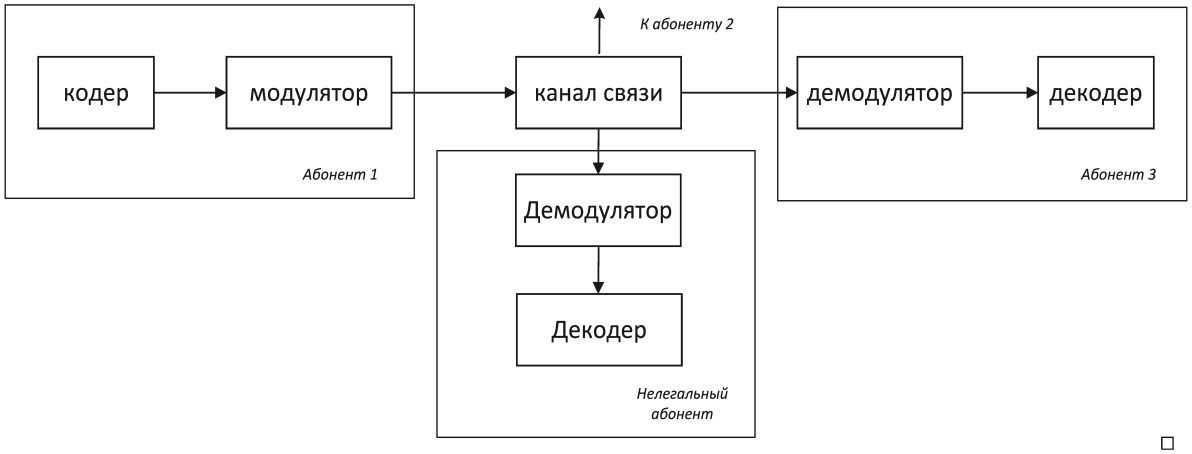

Рис. 2. Упрощенная блок-схема стандартной системы радиосвязи

.

В цифровой линии связи сообщение кодируется некоторым линейным двоичным блочным (n, k, d) кодом $\mathcal{C}$ с проверочной матрицей G , обеспечивающим достаточную надёжность в канале. Точнее, будем рассмотривать двочный симметричный канал без памяти с вероятостью ошибки p. Декодер $\mathcal{D}_t$ кода $\mathcal{C}$ исправляет все вектора ошибок e до веса $t = [(d-1)/2]$. Будем считать, что нелегальному абоненту известна схема помехоустойчивого кодирования, т.е. нелегальный абонент гарантированно может принять и прочитать любое сообщение, передаваемое в стандартной системе радиосвязи. Поставим перед собой задачу, чтобы модифицированная система связи должна использовать декодер $\mathcal{D}_t$ и полностью сохранять корректирующие свой-

ства исходной системы по отношению к ошибкам в канале. Однако не позволять нелегальному абоненту читать сообщения.

3. МОДИФИКАЦИЯ СИСТЕМЫ

Рассмотрим, как можно небольшим усложнением аппаратуры связи, особенно если она реализована по технологии SDR, лишить нелегального абонента возможности прочитать переданное сообщение. Для этого преобразуем блок-схему системы связи Рис. 1 в схему с цифровым скремблированием, которое обеспечивает обратимое преобразование передаваемого цифрового потока без изменения скорости передачи (см. Рис. 3). Точнее добавим «генератор специальной ошибки» на передающей стороне, который бы без обратного преобразования на приемной стороне гарантированно переводил бы передаваемое кодовое слово $c_i \in \mathcal{C}$ в другое кодовое слово $\tilde{c}_i \neq c_i$, где $\tilde{c}_i \in \tilde{\mathcal{C}}$.

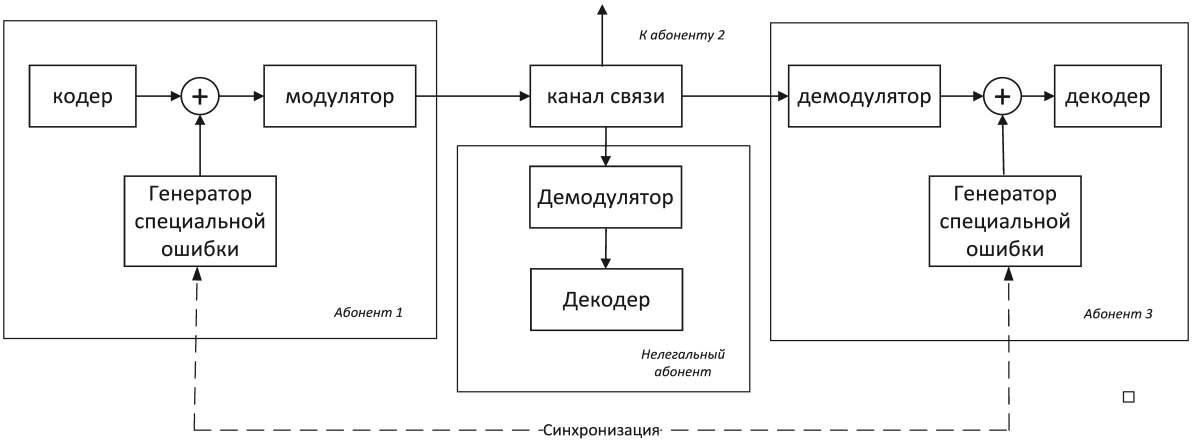

Рис. 3. Модифицированная блок-схема системы связи

.

Прежде всего рассмотрим, что представляет собой новый элемент аппаратуры связи (генератор специальной ошибки). Оба этих устройства как на передающей, так и на приемных сторонах построены совершенно одинаково (см. Рис.4). Они включают в себя начальное двоичное случайное слово e_0 длины n с числом единиц в слове $\frac{n}{2}$. Текущую ошибку e_i - также слово длины n с числом единиц в слове $\frac{n}{2}$. Матрицу перестановок P размера $n \times n$. Все блоки в системе работают синхронно с тактовой частотой передачи кодовых слов.

На каждом такте на передающем и приемном концах линии связи к передаваемому и приемному кодовому слову добавляется одна и та же текущая ошибка e_i. На первом такте текущая ошибка совпадает с начальным двоичным словом e_0. На каждом следующем такте новая текущая ошибка определяется как ошибка предыдущего такта, умноженная на матрицу перестановок P, т.е. $e_i = e_{i-1}P$.

Будем считать, что нелегальному абоненту известна схема модификации системы радиосвязи, однако ему неизвестны: информационное слово u, двоичное слово e_0 и матрица перестановок P.

Рассмотрим, как выглядят передаваемые и принимаемые кодовые слова в блок-схеме Рис. 3 на передающей и приемной сторонах.

На передающей стороне на входе модулятора имеем:

$$\hat{c_i} = c_iP + e_i = u_iGP + e_i = u_iGP + e_{i-1}P = (u_iG + e_{i-1})P, \tag{1}$$

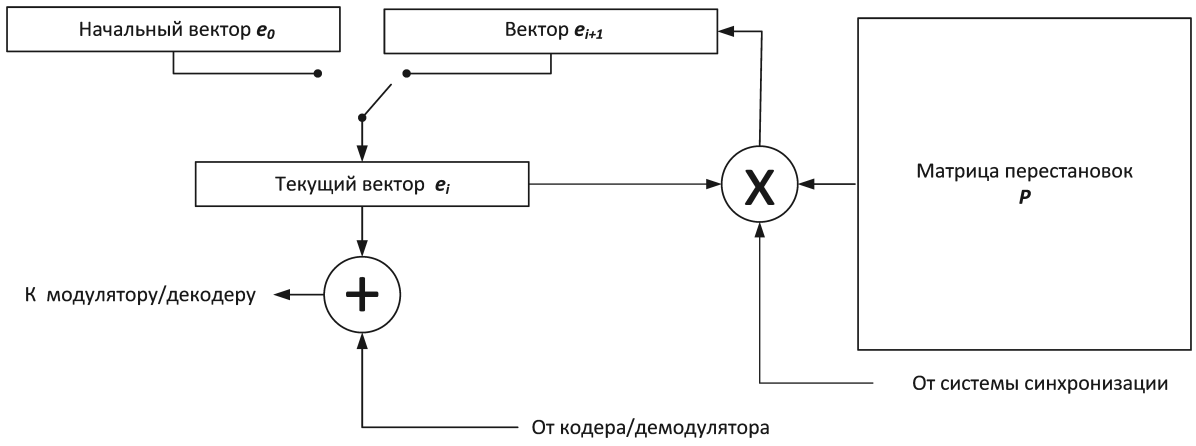

Рис. 4. Схема генератора специальной ошибки

.

где u_i - передаваемое информационное слово, а e_i можно рассматривать как кодовые слова из смежного класса по подгруппе 2^k аддитивной группы поля Галуа $\mathrm{GF}(2^n)$. Из выражения (1) видно, что передаваемый код $\tilde{\mathcal{C}}$ как и в [1] имеет порождающую матрицу $\tilde{G} = GP$, т.е. формулу (1) можно переписать как

$$\hat{c_i} = \tilde{c_i} + e_i. \tag{2}$$

На приемной стороне легального абонента на выходе демодулятора получаем:

$$\hat{c_i} + e_{ch} = \tilde{c_i} + e_i + e_{ch},$$

а на входе декодера с учетом (2) и (1):

$$(\hat{c_i} + e_{ch} - e_i)P^{-1} = (\tilde{c_i} + e_i + e_{ch} - e_i)P^{-1} = (\tilde{c_i} + e_{ch})P^{-1} = c_i + e_{ch}P^{-1} \tag{3}$$

где e_{ch}– ошибка, вносимая каналом на стороне легального абонента. Очевидно, что вес Хэмминга $w(e_{ch}P^{-1}) = w(e_{ch})$. Предположим, что вес вектора ошибок канала равен $w(e_{ch}) \leq t$, тогда декодер $\mathcal{D}_t$ исправляет ошибки в векторе $c_i + e_{ch}P^{-1}$ и находит правильное кодовое слово $c_i = u_iG$ и информационный вектор u_i.

На приемной стороне нелегального абонента на выходе демодулятора имеем:

$$\hat{c_i} + e^{'}_{ch}, \tag{4}$$

где $e^{'}_{ch}$- ошибка, вносимая каналом на стороне нелегального абонента.

При декодирования нелегальным абонентом декодером $\mathcal{D}_t$ вектор (4) в общем виде можно представить в виде :

$$\hat{c_i} + e^{'}_{ch} = c_i + c_{e_i} + e_{e_i} + e^{'}_{ch} = \bar{c}_i + \bar{e}_{ch}, \tag{5}$$

т.е. нелегальный пользователь всегда декодирует кодовое слово $\bar{c}_i = c_i + c_{e_i}$, которое является суммой двух кодовых слов передаваемого c_i и кодового слова c_{e_i}из смежного класса, порождаемого вектором e_i, в присутствии вектора ошибок $\bar{e}_{ch} = e_{e_i} + e^{'}_{ch}$.

Справедливость (5) будет предметом детального исследования ниже. Главное, что результатом декодирования нелегального абонента будет *кодовое слово* $\bar{c}_i$, *несовпадающее с переданным* c_i.

4. ДЕТАЛЬНЫЙ АНАЛИЗ ЛИНИИ СВЯЗИ С НЕЛЕГАЛЬНЫМ АБОНЕНТОМ

Как уже отмечалось, линия связи с нелегальным абонентом с точки зрения передачи информации ничем не отличается от линии связи с легальным абонентом за исключением векторов ошибок в канале: e'_{ch} и e_{ch}. Поэтому анализ сводится к исследованию только возможности нелегального абонента получить переданное сообщение c_i. Это анализ начнем с некоторых фундаментальных свойств теории кодирования. Классифицируем все множество ошибок вносимых и исправляемых кодом при декодировании по максимуму правдоподобия.

Всего могут быть внесены в качестве ошибок любое двоичное слово длины n, т.е. их количество равно $N_e = 2^n$. Любой линейный код скорости $R = \frac{k}{n}$ может исправлять $N_{Re} = 2^{(1-R)n}$ ошибочных слов. Следовательно, имеется множество

$$N_{-e} = N_e - N_{Re} = 2^n - 2^{(1-R)n} \tag{6}$$

неисправляемых слов, т.е. очень большое множество.

Рассмотрим результаты декодирования из множеств исправляемых и неисправляемых ошибок:

1. при декодировании кодового слова с ошибками из исправляемого множества ошибок результатом будет переданное слово;
2. при декодировании кодового слова с ошибками из неисправляемого множества ошибок результатом будет кодовое слово, несовпадающее с переданным.

Задача модернизированной системы связи сделать так, чтобы нелегальному абоненту приходило слово из канала с неисправляемым сочетанием ошибок. В этом случае нелегальный абонент будет всегда иметь неправильное слово, т.е. не иметь информации о передаваемых сообщениях.

5. ЗАКЛЮЧЕНИЕ

Покажем, что предложенный метод модификации системы связи решает эту задачу (см. Рис. 3 – 4).

Отметим, что вес исправляемой ошибки в линейном коде как правило существенно менее $\frac{n}{2}$. Поэтому выбираем вес вносимой ошибки e_i равной $\frac{n}{2}$, т.е. всегда будем добавлять неисправимую ошибку. Это означает, что нелегальный абонент получает слово определяемое (5), т.е. в результате декодирования всегда будет иметь кодовое слово, не совпадающее с переданным.

Рассмотрим возможно ли нелегальному абоненту сделать что-то, чтобы получить правильное сообщение. Для этого ему нужно знать вносимое e_i. Однако, как следует из (5), в принятом нелегальным абонентом сообщении e_i отсутствует, а при $e'_{ch} = 0$ есть представление e_i в виде

$$e_i = c_{e_i} + e_{e_i}, \tag{7}$$

где e_{e_i}некоторая исправимая ошибка, а c_{e_i} - некоторое кодовое слово. Ответим на вопрос как много различных c_{e_i} соответствует одному значению e_{e_i}. Всего имеется различных значений e_i, используемых в предлагаемой схеме столько, сколько имеется различных слов N_{ke} веса $\frac{n}{2}$, т.е. N_{ke} имеет порядок $n^{-c}2^n$, где $c \approx 0.8$ и равно

$$N_{ke} = \begin{cases} \frac{1}{2}\binom{\frac{n}{2}}{n} & \text{, если } n \text{ - четное} \\ \\ \frac{n-1}{2n}\binom{\frac{n+1}{2}}{n} & \text{, если } n \text{ - нечетное.} \end{cases}$$

С другой стороны, число различных исправляемых e_{e_i} равно $N_{Re} = 2^{(1-R)n}$. Таким образом, число кодовых слов, соответствующих одному значению e_{e_i} имеет порядок N_{ke}, т.е. экспоненциально большое число, следовательно необходимо выбрать кодовое слово из экспоненциально большого числа слов и при этом неясен критерий выбора. К тому же, если $e'_{ch} \neq 0$, то поиск c_{e_i} принципиально невозможен.

СПИСОК ЛИТЕРАТУРЫ

1. R.J. McEliece, A public-key cryptosystem based on algebraic coding theory // DSN Progress Report, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, pp 114-116, 1978.
2. Zyablov V., Potapov V., Sidorenko V., A network with data protection from both channel errors and unauthorized access using one code // The 2024 Munich Workshop on Coding and Cryptography (MWCC), 2024 , April 8-10
3. V.V. Zyablov, V.G. Potapov, V.R. Sidorenko, Data protection in a network from both channel errors and unauthorized access using one code // Информационные процесссы, Том 24, 2, 2024, С: 136-139

A method for converting a digital conventional radio communication system into a system protected from an illegal subscriber

V. V. Zyablov, V. G. Potapov, V. R. Sidorenko

A simple method is proposed for converting a standard digital wireless conventional communication system into a radio communication system in which an illegal subscriber, knowing the error-correcting coding method and modulation type used, cannot read the transmitted message.

KEYWORDS: radio communication, scrambling, unauthorized access, information theory.