



сотрудника из каталога при его увольнении автоматически запретит доступ его учетной записи к общим объектам и т. п.

Использование таких сетей в высших учебных заведениях позволит внедрить электронный студенческий билет и зачетную книжку – пластиковую карту с фотографией студента, на магнитной полосе которой будет записана информация о прослушанных курсах, экзаменационных отметках, ежедневных опозданиях и взятых в библиотеке книгах. Подобные пластиковые карты можно ввести и для преподавателей: они могут являться ключами к аудиториям, защищенным компьютерам, по ним можно получать льготу при путешествиях, посещениях музеев федерального значения и т. д.

Безусловно все это возможно только в случае принятия соответствующих нормативно-правовых актов и должного финансирования проводимых работ. Проект организации ЛВС с открытой инфраструктурой является базовым и ставит своей

целью не только организацию учебного процесса, но и возможность показать жизнеспособность данных систем на практике. В этом проекте предпочтение продуктам Microsoft было отдано по следующим причинам:

разрабатывать собственную систему накладно, к тому же это приводит к несовпадению форматов выходных данных в разных системах;

добиться схожих результатов можно также при помощи бесплатных операционных систем и платформ, но это было бы нецелесообразно, поскольку Удмуртский университет является академическим партнером Microsoft.

В этой связи нельзя не отметить работу Microsoft в области упрощения инструментария настройки и лояльную политику по отношению к вузам в части цен на программные продукты. Гибкость, масштабируемость, безопасность, контролируемость, адекватность – неоспоримые преимущества ЛВС на базе продуктов Microsoft перед аналогами.

СПИСОК ЛИТЕРАТУРЫ

1. Блэк Ю. Сети ЭВМ: протоколы, стандарты, интерфейсы. М.: Мир, 1990. 510 с.
2. Макин Дж., Маклин Й. Внедрение, управление и поддержка сетевой инфраструктуры Microsoft Windows Server 2003. М.: Русск. редакция, 2004. 594 с.
3. Брэгг Р. Безопасность сети на основе Microsoft Windows Server 2003. М.: Русск. редакция, 2005. 632 с.

4. Рэтлиф Б., Баллард Дж., Microsoft ISA Server 2004. М.: Русск. редакция, 2006. 382 с.
5. Непейвода Н. Н. Сообщество открытого софта как реализация принципов анархизма // Тр. Первой конференции свободного программного обеспечения в высшей школе. Переславль Залесский, 2006. С. 19, 20.

Хромов В. В., Есипов А. В.

ОЦЕНКА ВЕРОЯТНОСТНО-ВРЕМЕННЫХ ХАРАКТЕРИСТИК КЛАССА АЛГОРИТМОВ ПЕРЕДАЧИ ДАННЫХ ПО КАНАЛУ С НЕЗАВИСИМЫМИ ОШИБКАМИ

В настоящее время для передачи информации в каналах низкого качества активно применяются протоколы, предусматривающие синхронный прием повторений канального кадра с последующим мажоритарным исправлением искаженных символов. Информация, подлежащая передаче – шифроблоки системы шифрования с закрытым ключом. Сообщение состоит из N таких блоков, значение N может варьироваться от одного блока до нескольких десятков. Протокол обеспечивает высокую помехоустойчивость, однако остается открытым вопрос о его надежности. Угрозу создает возможность того, что информация, подвергшаяся

в канале искажению, может быть признана истинной. В работе предлагается методика расчета вероятностно-временных характеристик приема и оценка информационной безопасности протокола через вероятность ложного приема.

Алгоритм передачи данных. Одним из важнейших этапов выбора протокола передачи является определение способа кадровой синхронизации. Известны три способа кадрирования [3]: знаковое, битовое кадрирование с флагом и кадрирование с указанием длины кадра в поле заголовка. Каждый из этих способов имеет свои достоинства и недостатки. В решаемой нами задаче предлагается

следующий оригинальный метод синхронизации. Синхронизация устанавливается по слову обмена (СО), состоящему из 16 разрядов. Первые 7 разрядов определяют количество блоков в сообщении, следующие 4 определяют номер повторения сообщения, последние 5 – проверочные.

Максимально в сеансе одно сообщение может быть повторено 15 раз.

4 проверочных разряда заполняются остатком циклического кодирования предыдущих разрядов полиномом $x^4 + x + 1$. Проверочный разряд 16 содержит проверку на нечетность предыдущих 15-ти разрядов.

Для повышения достоверности и вероятности приема СО повторяется три раза, что позволяет на приеме произвести мажоритарное исправление искаженных символов.

Слово обмена формируется на каждом повторении сообщения.

В начале первого блока данных находятся 8 служебных битов, за ними идут 120 информационных битов. В последние 16 разрядов заносится остаток от циклического кодирования предыдущих 128 разрядов полиномом $x^{16} + x^{12} + x^5 + 1$. Длина первого блока данных, таким образом, составляет 144 разряда, длина последующих, не содержащих 8 служебных битов – 136 разрядов.

Алгоритм приема данных состоит в следующем:

1. Поиск СО путем проверки последовательности из 48 бит, поступающих из канала, на выполнение условий: число исправлений на 16 позициях должно быть не более 6; в блоке из 16 бит содержится нечетное число единиц; блок из 15 бит без остатка делится на полином $x^4 + x + 1$.

Если не выполняется хотя бы одно условие, поиск СО продолжается после отбрасывания самого старого бита и добавления нового. Прием СО определяет управляющую информацию: положение следующего СО и границы блоков.

2. Проверка информационных блоков на наличие ошибок делением на полином $x^{16} + x^{12} + x^5 + 1$. Деление без остатка означает правильный прием блока, а для одноблочного сообщения выносится решение о приеме данных, принятая информация пересылается на следующий уровень протокольного обмена данными.

Если сообщение многоблочное, то анализируются на делимость все блоки сообщения, в случае приема всех блоков выносится решение о приеме сообщения.

3. Если есть непринятые блоки, то осуществляется переход в режим накопления и последующего мажоритарного исправления ошибок в забракованных блоках.

4. При трех подряд браковках блока производится мажоритарное исправление ошибок (голосованием 2 из 3-х) и проверяется, удалось ли исправление ошибок, по делимости исправленного блока на полином 16-ой степени.

5. В случае неприема анализируется по пунктам 2, 3, 4 четвертый блок и, если исправления не произошло, то производятся все оставшиеся голосования 2 из 3-х.

6. При накоплении пяти блоков и отсутствии приема голосования продолжают, включая вариант 3 из 5-ти. И далее, вплоть до приема пятнадцатого блока, с голосованиями вплоть до 7 из 13-ти.

Для решения поставленной задачи – расчета вероятности ложного приема сообщения – предлагается рассматривать процесс приема как марковскую цепь. Возможные состояния цепи следующие:

0 – начало передачи;

1 – правильный прием блока и синхросылки;

2 – ложный прием блока;

3 – неприем блока, прием синхросылки;

4 – правильный прием очередного повтора;

5 – ложный прием очередного повтора;

6 – неприем очередного повтора.

Математическая модель процесса приема одноблочного сообщения приведена на рис.1. Вероятность правильного и ложного приема при обработке i ($i = 1 \dots 15$) повторений находится возведением матрицы переходных вероятностей в степень, равную i . Правильному приему для одноблочного сообщения соответствуют состояния 1 и 4, ложному приему – состояния 2 и 5 на рисунке 1.

Вероятности на первом шаге приема:

несинхронизация – $P_{00} = 1 - (q^3 + 3pq^2)^{16}$,

правильный прием сообщения –

$$P_{01} = (q^3 + 3pq^2)^{16} q^{144},$$

ложный прием сообщения –

$$P_{02} = (q^3 + 3pq^2)^{16} \left(\frac{1}{2^{16}} \cdot \left(1 - \sum_{i=0}^3 C_{144}^i p^i q^{144-i} \right) \right),$$

неприем сообщения –

$$P_{03} = 1 - P_{00} - P_{01} - P_{02}.$$

Вероятности правильного, ложного приема и неприема сообщения после первого повтора соответственно:

$$P_{34} = q^{144},$$

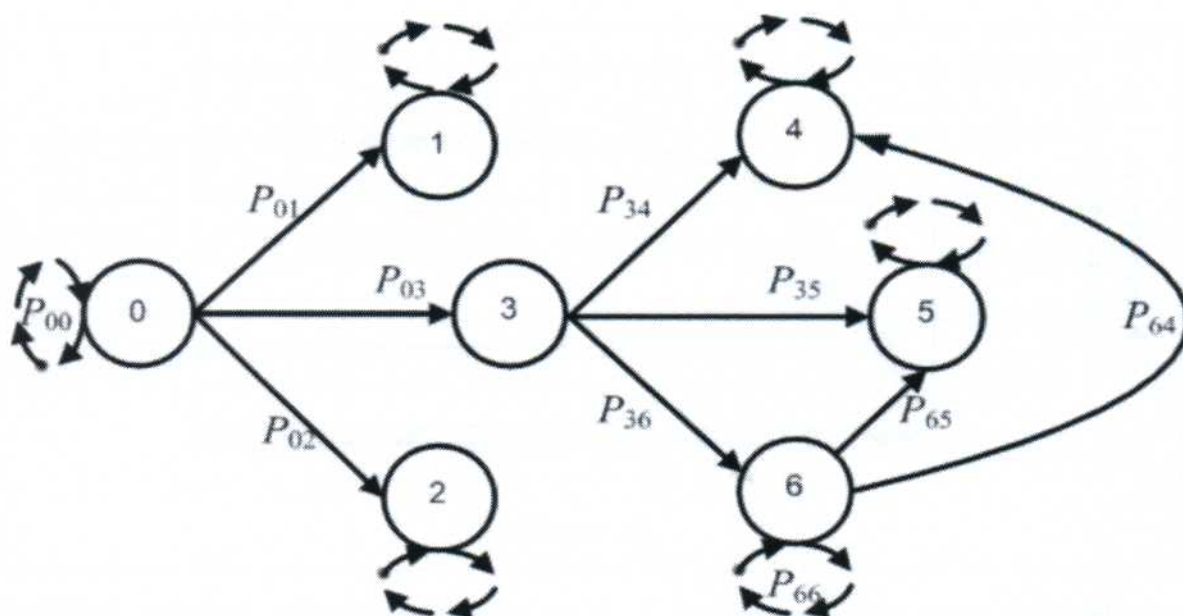


Рис. 1. Граф вероятностей переходов цепи Маркова при передаче одноблочного сообщения

$$P_{35} = P_{FALSE} = \frac{1}{2^{16}} (1 - \sum_{i=0}^3 C_{144}^i p^i q^{144-i}),$$

$$P_{36} = 1 - P_{34} - P_{35}.$$

Вероятность правильного, ложного приема и неприема сообщения после очередного повтора и голосования соответственно:

$$P_{64} = q^{144} + (1 - q^{144} - P_{FALSE})(q^3 + 3pq^2)^{144},$$

$$P_{65} = P_{FALSE} + (1 - q^{144} - P_{FALSE}) \times \\ \times (1 - \sum_{i=0}^3 C_{144}^i (1 - q^3 - 3q^2p)^i (q^3 + 3q^2p)^{144-i}) \frac{1}{2^{16}}$$

$$P_{66} = 1 - P_{64} - P_{65}.$$

Вероятностно-временные характеристики достоверного приема сообщения, рассчитанные по указанной методике, приведены в таблице 1.

Таблица 1

№ повтора	Вероятность ошибки бита					
	0,04	0,03	0,02	0,01	0,005	0,001
1	0,002597	0,011932	0,053496	0,234098	0,485293	0,865784
2	0,005188	0,023722	0,104130	0,413393	0,735077	0,981986
3	0,476792	0,666679	0,853573	0,979075	0,998378	0,999999
4	0,725460	0,888788	0,982537	1	1	1
5	0,855931	0,962880	0,997905	1	1	1
6	0,924387	0,987596	0,999737	1	1	1
7	0,960304	0,995841	0,999955	1	1	1
8	0,979149	0,998591	0,999981	1	1	1
9	0,989037	0,999508	0,999984	1	1	1
10	0,994225	0,999814	0,999985	1	1	1
11	0,996947	0,999917	0,999985	1	1	1
12	0,998375	0,999951	0,999985	1	1	1
13	0,999124	0,999962	0,999985	1	1	1
14	0,999517	0,999966	0,999985	1	1	1
15	0,999724	0,999967	0,999985	1	1	1

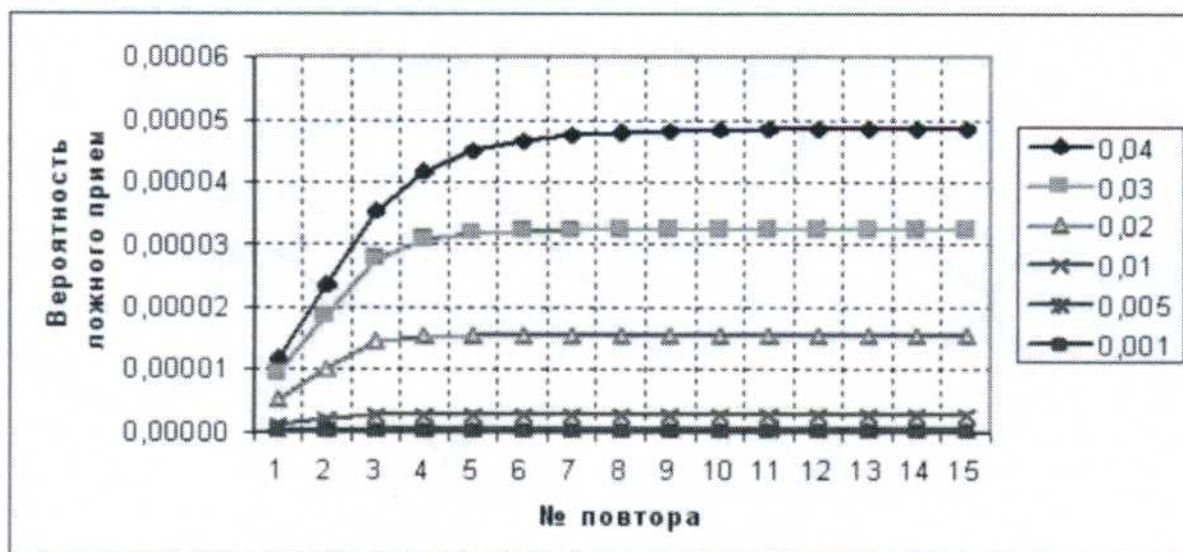


Рис.2. Зависимость вероятности ложного приема от номера повторения сообщения и величины ошибки бита

Таблица 2

№ повтора	Вероятность ошибки бита					
	0,04	0,03	0,02	0,01	0,005	0,001
1	$1,18 \cdot 10^{-5}$	$9,34 \cdot 10^{-6}$	$5,13 \cdot 10^{-5}$	$1,15 \cdot 10^{-6}$	$2,36 \cdot 10^{-7}$	$1,04 \cdot 10^{-8}$
2	$2,36 \cdot 10^{-5}$	$1,86 \cdot 10^{-5}$	$9,98 \cdot 10^{-6}$	$2,02 \cdot 10^{-6}$	$3,57 \cdot 10^{-7}$	$1,18 \cdot 10^{-8}$
3	$3,53 \cdot 10^{-5}$	$2,77 \cdot 10^{-5}$	$1,46 \cdot 10^{-5}$	$2,7 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$
4	$4,16 \cdot 10^{-5}$	$3,08 \cdot 10^{-5}$	$1,53 \cdot 10^{-5}$	$2,72 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$
5	$4,49 \cdot 10^{-5}$	$3,19 \cdot 10^{-5}$	$1,54 \cdot 10^{-5}$	$2,72 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$
6	$4,66 \cdot 10^{-5}$	$3,22 \cdot 10^{-5}$	$1,54 \cdot 10^{-5}$	$2,72 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$
7	$4,75 \cdot 10^{-5}$	$3,23 \cdot 10^{-5}$	$1,54 \cdot 10^{-5}$	$2,72 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$
8	$4,80 \cdot 10^{-5}$	$3,24 \cdot 10^{-5}$	$1,54 \cdot 10^{-5}$	$2,72 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$
9	$4,82 \cdot 10^{-5}$	$3,24 \cdot 10^{-5}$	$1,54 \cdot 10^{-5}$	$2,72 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$
10	$4,84 \cdot 10^{-5}$	$3,24 \cdot 10^{-5}$	$1,54 \cdot 10^{-5}$	$2,72 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$
11	$4,84 \cdot 10^{-5}$	$3,24 \cdot 10^{-5}$	$1,54 \cdot 10^{-5}$	$2,72 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$
12	$4,85 \cdot 10^{-5}$	$3,24 \cdot 10^{-5}$	$1,54 \cdot 10^{-5}$	$2,72 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$
13	$4,85 \cdot 10^{-5}$	$3,24 \cdot 10^{-5}$	$1,54 \cdot 10^{-5}$	$2,72 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$
14	$4,85 \cdot 10^{-5}$	$3,24 \cdot 10^{-5}$	$1,54 \cdot 10^{-5}$	$2,72 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$
15	$4,85 \cdot 10^{-5}$	$3,24 \cdot 10^{-5}$	$1,54 \cdot 10^{-5}$	$2,72 \cdot 10^{-6}$	$4,2 \cdot 10^{-7}$	$1,2 \cdot 10^{-8}$

Результат расчета вероятности ложного приема по указанной методике приведен в таблице 2.

Указанную модель несложно обобщить и для сообщений, состоящих более чем из одного блока. Состояния цепи для двухблочного сообщения:

- 0 – начало передачи (нет синхронизации);
- 1 – правильный прием двух блоков сообщения и синхросылки;
- 2 – синхросылка и один блок приняты правильно, второй блок не принят;
- 3 – не приняты оба блока, синхросылка принята;

4 – синхронизация, один блок сообщения принят ложно, второй не принят;

5 – ложный прием двух блоков сообщения и синхросылки;

6 – правильный прием недостающих блоков сообщения;

7 – не прием недостающего блока сообщения (сообщение не принято);

8 – нет приема двух блоков сообщения, есть синхронизация;

9 – ложный прием одного блока, не прием второго;

10 – окончательный ложный прием.

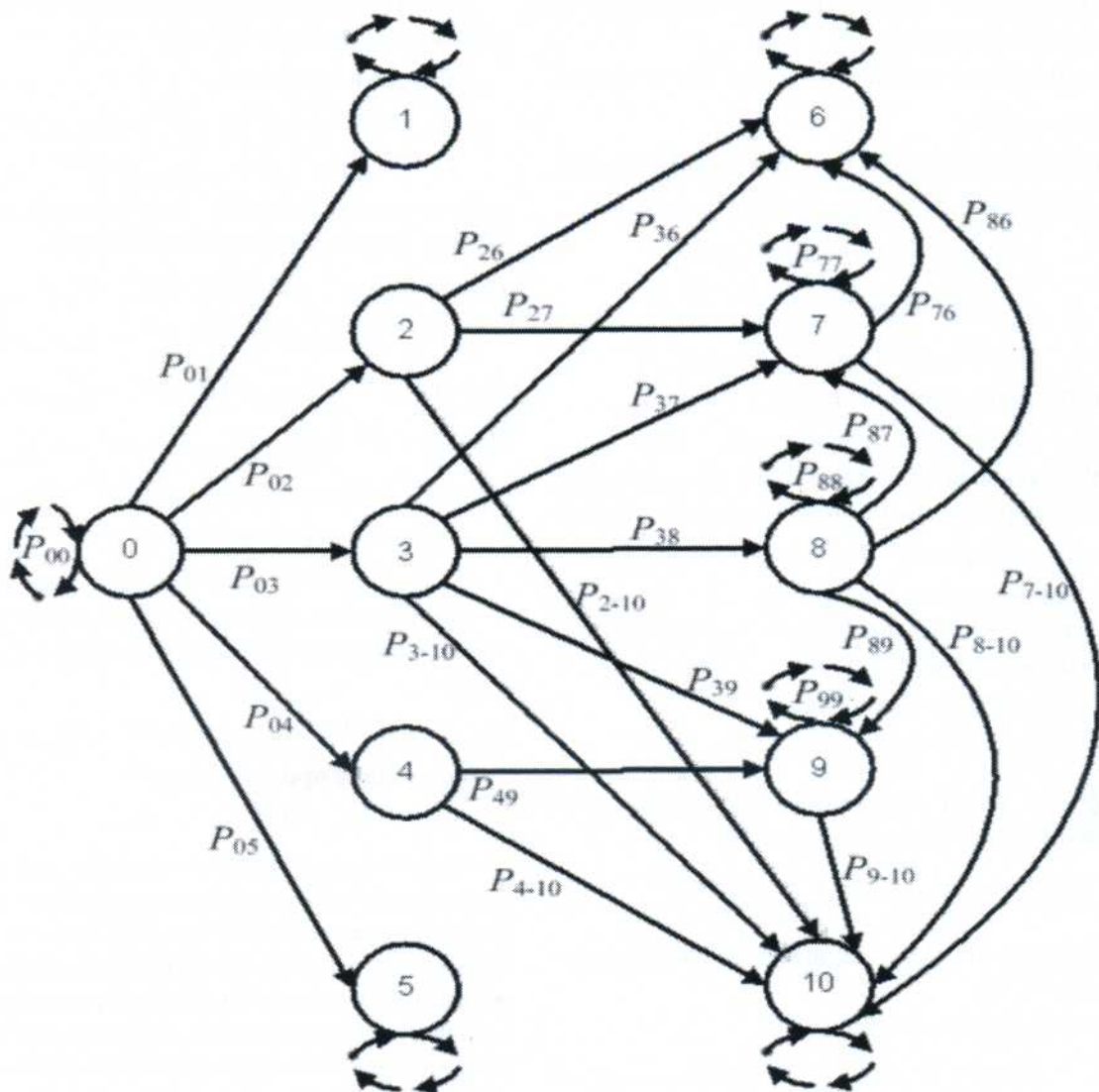


Рис.3. Граф вероятностей переходов цепи Маркова при передаче двухблочного сообщения

Для такого сообщения правильный прием – это состояния 1 и 6, а ложный – состояния 5 и 10 (рис. 3). Вероятности верного и ложного приема на i -м повторе также находится возведением матрицы переходных вероятностей в степень, равную i .

Вероятности на первом шаге приема:

несинхронизация – $P_{00} = 1 - (q^3 + 3pq^2)^{16}$,

верный прием обоих блоков сообщения –

$$P_{01} = (q^3 + 3pq^2)^{16} q^{144} q^{144},$$

прием одного блока, неприем второго блока –

$$P_{02} = (q^3 + 3pq^2)^{16} \cdot q^{144} (1 - q^{144} - P_{FALSE}) \cdot 2,$$

$$\text{где } P_{FALSE} = \frac{1}{2^{16}} \cdot (1 - \sum_{i=0}^3 C_{144}^i p^i q^{144-i}),$$

неверный прием обоих блоков –

$$P_{03} = (q^3 + 3pq^2)^{16} (1 - q^{144} - P_{FALSE})^2,$$

ложный прием одного блока и неприем другого –

$$P_{04} = (q^3 + 3pq^2)^{16} \cdot P_{FALSE} (1 - q^{144} - P_{FALSE}),$$

ложный прием сообщения –

$$P_{05} = 1 - P_{00} - P_{01} - P_{02} - P_{03} - P_{04}.$$

Вероятности на втором шаге приема, ранее один блок принят, второй – нет:

верный прием, неприем и ложный прием второго блока соответственно –

$$P_{26} = q^{144},$$

$$P_{27} = 1 - q^{144} - P_{FALSE},$$

$$P_{2-10} = P_{FALSE}.$$

Вероятности на втором шаге приема, ранее оба блока не приняты:

верный прием обоих блоков после повторения – $P_{36} = q^{288}$,

один из блоков вновь не принят, а второй – принят, не принят и принят ложно соответственно:

$$P_{37} = q^{144} (1 - q^{144} - P_{FALSE}) \cdot 2,$$

$$P_{38} = (1 - q^{144} - P_{FALSE})^2,$$

$$P_{39} = P_{FALSE} (1 - q^{144} - P_{FALSE}) \cdot 2,$$

сообщение принято ложно –

$$P_{3-10} = 1 - P_{36} - P_{37} - P_{38} - P_{39}.$$

Вероятности на втором шаге приема, ранее один блок принят ложно, второй – не принят: второй блок опять не принят – $P_{49} = 1 - q^{144} - P_{FALSE}$, сообщение принято ложно – $P_{4-10} = 1 - P_{49}$.

Вероятности на последующих шагах приема при одном не принятом блоке:

прием блока и сообщения –

$$P_{76} = q^{144} + (1 - q^{144} - P_{FALSE}) Q^{144},$$

где $Q = q^3 + 3pq^2$ – вероятность исправления искаженного бита блока. Полагая, что

$$P_{FALSE-VOTE} = \frac{1}{2^{16}} \cdot (1 - \sum_{i=0}^3 C_{144}^i P^i Q^{144-i}) -$$

вероятность ложного исправления по голосованию, $P = 1 - Q$,

ложный прием сообщения –

$$P_{7-10} = P_{FALSE} + (1 - q^{144} - P_{FALSE}) P_{FALSE-VOTE},$$

неприем недостающего блока и сообщения –

$$P_{77} = 1 - P_{76} - P_{7-10}.$$

Вероятности на последующих шагах при обоих ранее не принятых блоках:

оба блока приняты –

$$P_{86} = q^{288} + 2q^{144} (1 - q^{144} - P_{FALSE}) Q^{144} + (1 - q^{144} - P_{FALSE})^2 Q^{288},$$

один не принят, а второй – принят верно, не принят или принят ложно соответственно –

$$P_{87} = 2q^{144} (1 - q^{144} - P_{FALSE}) (1 - Q^{144} - P_{FALSE-VOTE}) + 2(1 - q^{144} - P_{FALSE})^2 Q^{144} (1 - Q^{144} - P_{FALSE-VOTE}),$$

$$P_{88} = (1 - q^{144} - P_{FALSE})^2 (1 - Q^{144} - P_{FALSE-VOTE})^2,$$

$$P_{89} = 2(1 - q^{144} - P_{FALSE}) P_{FALSE} (1 - Q^{144} - P_{FALSE-VOTE}) + 2(1 - q^{144} - P_{FALSE})^2 P_{FALSE-VOTE} (1 - Q^{144} - P_{FALSE-VOTE}),$$

сообщение принято ложно –

$$P_{8-10} = 1 - P_{86} - P_{87} - P_{88} - P_{89}.$$

Вероятности при одном ранее ложно принятом блоке и не принятом втором: неприем второго блока –

$$P_{99} = (1 - q^{144} - P_{FALSE}) (1 - Q^{144} - P_{FALSE-VOTE}),$$

сообщение принято ложно –

$$P_{9-10} = 1 - P_{99}.$$

Таким образом, в работе получены выражения и процедуры для вычисления вероятности ошибочного приема сообщений, вероятности достоверного приема, а также функции распределения времени доставки сообщения (задержки в приеме) в зависимости от средней вероятности битовой ошибки канала и размера сообщения. Произведенные расчеты (таблицы 1, 2 и рисунок 2) характеризуют используемый метод приема как надежно защищенный от ложного приема данных.

СПИСОК ЛИТЕРАТУРЫ

1. Дмитриев В. И., Хромов В. В. Помехоустойчивое кодирование в системах передачи данных. Л.: Издательство ЛПИ, 1998. – 80 с.

2. Прокис Дж. Цифровая связь. Перевод с англий-

ского под редакцией Кловского Д.Д. Москва: Радио и связь, 2000. 797 с.

3. Бертсекас Д., Галлагер Р. Сети передачи данных: пер. с англ. – Москва: Мир, 1989. 544 с.