РАДИОТЕХНИКА, В ТОМ ЧИСЛЕ СИСТЕМЫ И УСТРОЙСТВА ТЕЛЕВИДЕНИЯ / RADIO ENGINEERING, INCLUDING TELEVISION SYSTEMS AND DEVICES

DOI: https://doi.org/10.60797/IRJ.2024.143.92

К ВОПРОСУ О КОДИРОВАНИИ И ДЕКОДИРОВАНИИ ИНФОРМАЦИИ В СФЕРЕ ТЕЛЕМЕДИЦИНЫ

Научная статья

Уразбахтина К.Р.[1], Рузанова Н.В.[2,] *, Хакимьянов А.Р.[3], Уразбахтин Р.Н.[4]
[1] ORCID : 0000-0001-8016-6577;
[3] ORCID : 0009-0000-7287-1065;
[4] ORCID : 0000-0002-5015-6770;
[1, 2, 3, 4] Уфимский университет науки и технологий, Уфа, Российская Федерация

* Корреспондирующий автор (nineli48[at]gmail.com)

Аннотация

В статье рассмотрено применение алгоритма расчета детектирования ошибок при передаче данных в канале связи с помощью циклического избыточного кода (CRC) в области телемедицины, проанализировано его специфическое применение различных направлениях дистанционной медицины, выявлены основные достоинства и недостатки применения CRC в этой сфере здравоохранения и проведено динамическое моделирование работы кода CRC-32-IEEE 802.3. Целью работы являлось установление надежности применения циклического избыточного кода для защиты медицинских данных путем определения влияния отношения количества необнаруженных ошибок к их общему количеству – вероятности необнаруженной ошибки к вероятности ошибки в канале связи. Исследование проводилось с помощью программы динамического моделирования SimInTech, в результате чего была установлена эффективность применения данного алгоритма для проверки целостности медицинской информации, а также установлено, что аспект передачи и интерпретации данных в вопросе дистанционного консультирования пациентов является важной составляющей проблемы взаимодействия врач-пациент в современной системе здравоохранения.

Ключевые слова: телемедицина, циклический избыточный код, детектирование ошибок, моделирование CRC-32-IEEE 802.3.

TO THE ISSUE OF INFORMATION CODING AND DECODING IN THE FIELD OF TELEMEDICINE

Research article

Urazbakhtina K.R.[1], Ruzanova N.V.[2,] *, Khakimyanov A.R.[3], Urazbakhtin R.N.[4]
[1] ORCID : 0000-0001-8016-6577;
[3] ORCID : 0009-0000-7287-1065;
[4] ORCID : 0000-0002-5015-6770;
[1, 2, 3, 4] Ufa University of Science and Technology, Ufa, Russian Federation

* Corresponding author (nineli48[at]gmail.com)

Abstract

The article examines the application of the algorithm for calculating error detection during data transmission in the communication channel using cyclic redundant code (CRC) in the field of telemedicine, analyses its specific application in various areas of remote medicine, identifies the main advantages and disadvantages of CRC application in this field of healthcare and conducts dynamic simulation of the CRC-32-IEEE 802.3 code. The aim of the work was to establish the reliability of the application of cyclic redundant code for the protection of medical data by determining the effect of the ratio of the number of undetected errors to the total number of errors – the probability of undetected error to the probability of error in the communication channel. The study was carried out using the SimInTech dynamic modelling software, as a result of which the effectiveness of using this algorithm to verify the integrity of medical information was established, and it was also established that the aspect of data transmission and interpretation in the issue of remote patient counselling is an important component of the problem of doctor-patient interaction in the modern healthcare system.

Keywords: telemedicine, cyclic redundant code, error detection, CRC-32-IEEE 802.3 modelling.

Введение

В современном мире информационные технологии являются очень важной составляющей нашей жизни. Универсальность применения позволяет внедрять их во множество областей профессиональной деятельности. Исключением не является и медицина. Применение информационных и компьютерных технологий для оказания медицинских услуг получило название телемедицины, также называемой дистанционной медициной [1].

Телемедицина позволяет обеспечить взаимодействие между пациентом и врачом, находящимися на удаленном расстоянии друг от друга. Еще одно ее применение – профессиональное обучение медицинских работников в дистанционном формате.

Таким образом, можно выделить отдельные направления использования информационных технологий для оказания помощи в сфере здравоохранения:

- Консультации – осуществление обмена медицинскими данными посредством телефона или интернета. Могут проводиться как в режиме реального времени, так и в отложенном формате.

- Обучение – проведение лекций, консультаций в режиме обратной связи или без нее для повышения квалификации. Также может использоваться формат записанных трансляций в качестве обучающих материалов или прямая трансляция для организации «наставничества» в режиме реального времени.

- Дистанционный контроль – медицинское оборудование, снимающее и передающее показания в медицинское учреждение для дальнейшего исследования и обработки. Это направление актуально для лиц, страдающих хроническими заболеваниями, проходящих лечение на дому или нуждающихся в периодическом мониторинге.

Применение циклических избыточных кодов в телемедицине

В России сфера телемедицины активно развивается последние три десятилетия. Большая часть населения считает ее перспективной и относятся к ней положительно или нейтрально [2]. Особое внимание проблематике внедрения технологии дистанционного взаимодействия врач – пациент получила при пандемии COVID-19. Использование телемедицины позволяет сократить экономические расходы в медицинских центрах на обслуживание пациентов, в обучающих сферах – на организацию и логистику мероприятий. Также это способствует решению кадровой проблемы – в условиях нехватки узких специалистов в отдаленных районах использование дистанционных технологий поможет перераспределить врачебную нагрузку и обеспечить большему количеству пациентов возможность получения медицинской помощи.

Можно выделить ряд требований, предъявляемых к подобного рода услугам:

1. Обеспечение конфиденциальности персональных данных.
2. Обеспечение защиту персональных данных в случаях киберопасности.
3. Обеспечение надежности передаваемых данных.

Основным принципом телемедицины является организация многостороннего, безопасного и достоверного обмена данными о состоянии здоровья граждан.

Конфиденциальность обеспечивается путем ограничения круга лиц, имеющих доступ к информации, использованием медицинских информационных систем и сетевых хранилищ, работающих локально в пределах конкретного медицинского учреждения [3].

Кибербезопасность обеспечивается путем применения определенных протоколов, технологий шифрования данных, организации различных систем аутентификации с использованием биометрии и криптографии [4].

Важной частью оказания дистанционных медицинских услуг является надежность передаваемой информации. Надежный обмен данными обеспечивает достоверность и целостность передаваемой информации, что в контексте состояния здоровья человека играет основополагающую роль.

Шумы, наводки и случайные сбои могут внести искажения в канал передачи. Целостность выходных данных в таких случаях реализуется с использованием алгоритмов обнаружения и устранения ошибок. Стоит отметить, что существуют алгоритмы, позволяющие только обнаружить ошибку и алгоритмы, определяющие и корректирующие ошибку. В отличие от обычных, более сложны в использовании.

К алгоритмам устранения ошибок можно отнести два метода.

Первый метод – контроль четности. Каждый блок данных имеет соответствующее ему кодовое слово. Определяются избыточность кода и вероятность детектирования ошибки. Прибавление к блоку данных бита четности позволяет снизить эту вероятность. Метод полезен при определении независимых ошибок, но не имеет смысла при кластерных ошибках.

Второй метод используется как раз для обнаружения таких ошибок. Он получил название алгоритма нахождения контрольной суммы CRC – циклический избыточный код. Передаваемый блок данных делится на один из стандартизированных полиномов, и остаток от деления и является контрольной суммой. Вероятность детектирования ошибки зависит от степени полинома.

Если разложить область применения избыточного кодирования в передаче информации, касающейся сферы здравоохранения, на предметные составляющие, то получается следующее: графическое изображение, видеоизображение, телефонная связь, электронная связь посредством сети интернет или специализированных приложений, видеоконференции.

Таким образом, использование CRC в области телемедицины может иметь следующее применение:

1. Передача изображений медицинской информации - рентгеновские снимки, снимки магнитно-резонансной томографии (МРТ-изображения), снимки компьютерной томографии (КТ-изображения). Для их передачи используется специализированный протокол передачи цифровых изображений в медицине DICOM. Каждое информационное сообщение в этом протоколе снабжается вычисленным передающей стороной на его основе CRC, который сравнивается с вычисленным на принимающей стороне. Соответственно, при несовпадении значений в канале передачи появилась ошибка, и процедура начинается заново, либо может быть скорректирована другими алгоритмами в составе протокола. Протокол DICOM использует в своих алгоритмах циклический код CRC-32.

2. Передача электрокардиографической информации (записи ЭКГ процедуры) в случае их сохранения и передачи в цифровом виде. Передача данных возможна в двух вариантах: передача записанной информации и передача ЭКГ-сигнала в режиме реального времени. В медицине даже существует отдельное направление – телекардиология [5]. При расшифровке сигнала и обнаружении ошибки с помощью CRC, над ошибочным блоком будет отображаться предупреждение. На рисунке изображено влияние ошибки восстановления 13 мкВ при передаче на форму сигнала (см. рис. 1):

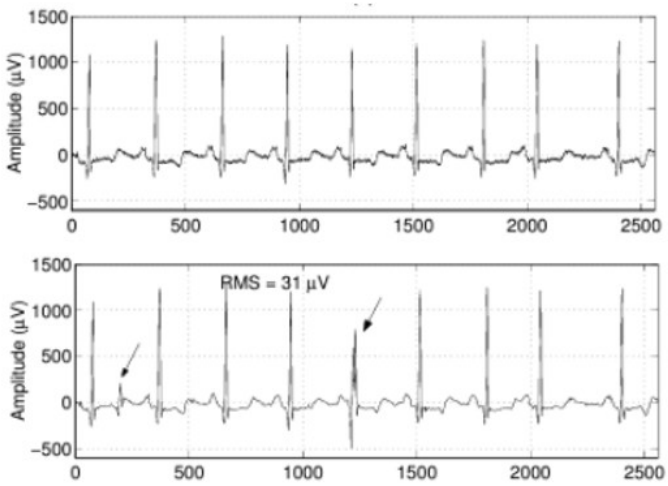

Рисунок 1 - Выявление ошибки с помощью CRC
DOI: https://doi.org/10.60797/IRJ.2024.143.92.1

3. Передача документации в электронном формате, в том числе электронных медицинских карт, больничных, справок, рабочих отчетов, отчетов для вышестоящих органов контроля и проверки, отчетов для страховых медицинских организаций.

4. Передача данных в специализированных медицинских приложениях для контроля и мониторинга состояния здоровья пациента (данные пульса, уровня кислорода в крови, тоны сердца, данные сна и физической активности), если речь идет о передаче таких данных в медицинскую организацию в беспроводном формате.

5. Передача видеосигнала в телемедицинских консультациях. CRC обеспечивает отвечает за надежность передаваемого потока, обеспечивая целостное и качественное изображение и звук для двухсторонней связи. В этом случае сигнал передается фрагментарно, используя для каждого фрагмента свой CRC. Также стоит отметить, что CRC в данном случае используется непосредственно на низких уровнях сетевого стека – уровнях канала Ethernet или Wi-Fi, а не на уровне самого видеоизображения. На нем используются алгоритмы детектирования и коррекции ошибок.

6. Медицинское оборудование для дистанционного контроля с беспроводной передачей данных. Принцип действия схож с передачей данных в специализированных приложениях, но список снимаемых параметров намного шире. От датчиков можно получать информацию о температуре, уровне сахара в крови, давлении. Также этом может использоваться в зубных щетках с датчиками уровня чистки зубов, смарт-капах, биосенсорах. В многих случаях смарт-устройства действуют в связке со специально разработанными для них приложениями, и CRC используется в последовательности передатчик (устройство) – приемник (приложение), передатчик (приложение) – приемник (информационная система медицинской организации).

7. Медицинское оборудование со встроенной беспроводной передачей данных. К нему можно отнести электрокардиографы, мониторы состояния пациента и в принципе любые устройства, оснащенные этой функцией. Для проверки целостности передаваемых данных и выявления ошибок используются CRC-16 и CRC-32.

8. Передача медицинской информации посредством электронной почты. В двухточечном протоколе PPP, определенном в RFC 1662, используется CRC-32, но это далеко не основной алгоритм проверки целостности данных.

По передаче данных по сети интернет чаще всего для вычисления контрольной суммы используется CRC-32 (протоколы TCP/IP, Ethernet, IPv4 или IPv6, UPD и прочие). Также в некоторых случаях для специфических протоколов используют CRC-16 – системы связи, промышленные сети. Учитывая ограниченность и закрытость этой сферы, применение возможно только в рамках военной телемедицины.

Важную роль в передаче информации играет вид беспроводной связи, по которой передаются информационные сообщения.

Самыми часто используемыми является беспроводная связь, осуществляемая через Bluetooth и Wi-Fi.

При передаче медицинской информации через Bluetooth обычно используется алгоритм вычисления контрольной суммы с помощью CRC-8. Несмотря на более низкую, по сравнению с другими кодами надежность, он выбран за оптимальные значения низкой вычислительной сложности и уменьшение нагрузки на вычислительные ресурсы процессора. Для этого вида передачи важными критериями являются скорость передачи данных, минимальные затраты на вычисление данных при передаче сигнала, низкое энергопотребление. CRC-8, благодаря длине вычисляемой контрольной суммы, является лучшим вариантом.

При передаче медицинской информации через Wi-Fi обычно используется алгоритм вычисления контрольной суммы с помощью CRC-32. Алгоритм выбран также из-за длины контрольной суммы и высокой надежности. Вычислительные способности Wi-Fi позволяют считать длину 32-битного кода относительно небольшой и быстро выполнять необходимые вычисления.

В области здравоохранения существуют общепринятые стандарты для обмена цифровой информацией [6]:

- DICOM – стандарт, уже упомянутый выше, использует в своих алгоритмах вычисления CRC-32.
- ACR/NEMA – стандарт для передачи, хранения и печати медицинских изображений, в нем может использоваться CRC-16.

- HL7 – стандарт, используемый при передаче электронных медицинских записей, в нем может использоваться CRC-16.

- XML DS – стандарт для проверки целостности при подписании и верификации электронных медицинских документов, использующих формат XML. В стандарте может использоваться алгоритм вычисления контрольной суммы CRC-32 или CRC-32C.

- ASTM – стандарт, используемый для передачи клинических результатов, может использовать для проверки CRC-32.

На территории Российской Федерации действует стандарт, определяющий требования к сетям вещательного цифрового телевидения [7]. Передача сигнала в телемедицине также подчиняется этому стандарту. Согласно спецификации, применяемый стандарт передачи данных графических изображений и звуковых сигналов – MPEG-4, используемый способ детектирования ошибки – циклический код CRC-32 с побитовым сдвигом.

Можно выделить преимущества использования нахождения контрольной суммы CRC для определения ошибок:

- большая вероятность нахождения ошибки и, как следствие, высокая надежность передачи целостного информационного слова с передатчика на приемник;

- универсальность, которая позволяет использовать алгоритм CRC в различных протоколах передачи медицинских данных;

- простота аппаратной реализации по сравнению с алгоритмами обнаружения и коррекции ошибок и, как следствие, высокая вычислительная скорость.

Наряду с достоинствами, алгоритмы CRC не лишены недостатков:

- невозможность коррекции ошибок и, как следствие, данные должны передаваться заново, что сказывается на временных затратах;

- неспособность к обнаружению шаблонных ошибок;

- необходимость в поиске компромисса между битовой длиной вычисленной контрольной суммы и временем ее вычисления – чем длиннее сумма, тем больше увеличивается время расчета;

- существование более новых алгоритмов детектирования и коррекции ошибок, которые эффективнее и надежнее сохраняют целостность передаваемых данных.

Конкретно в области применения телемедицины, можно выделить следующие преимущества использования CRC:

- Сохранение целостности передаваемых данных. В случае медицины полнота передаваемой информации является критично важным параметром. Рассмотренная выше ошибка при передаче ЭКГ-сигнала кажется незначительной, но даже такая малая величина ошибки может повлиять на точность расшифровки данных, что может сказаться на постановке диагноза и назначенном лечении.

- Повышение доверительного уровня пациентов к телемедицинским системам. Повышенная надежность и безопасность переданных данных дает уверенность в правильной интерпретации медицинских показателей.

- Обеспечение кибербезопасности. Попытки вмешательства в систему медицинских учреждений или попытки изменения данных с большой вероятностью будут обнаружены при расчете CRC.

Недостатки использования CRC в телемедицине не специфичны и ничем не отличаются от общих для всех областей применения.

С практической точки зрения это реализуется как вычисление кода на основе исходного слова. Данный код записывается после всех битов передаваемого сообщения. Избыточным код называется по причине того, что информационно никакого смысла не несет, но его присутствие позволяет определить ошибку в передаваемом сообщении.

Принцип работы алгоритмов нахождения ошибок

Рассмотрение алгоритмов нахождения ошибок необходимо начать с определения функционирования процедур, происходящих во время передачи информационного сообщения.

При использовании алгоритмов детектирования ошибок приемник и передатчик обеспечиваются обратной связью друг с другом. Приемник фиксирует наличие ошибки, но не корректирует ее, а запрашивает повторную передачу данных. При этом передатчик должен быть уведомлен о появлении ошибки. Такие алгоритмы называются автоматическим запросом повторной передачи ARQ (Automatic Repeat Request) [8].

Алгоритмы ARQ могут реализовать функцию обеспечения целостности передаваемого сообщения разными способами.

1. Режим остановка-запрос-ожидание. Соединение осуществляется по одному каналу связи, с временным разделением. Передатчик отправляет блок данных, приемник получает его и при отсутствии ошибок отправляет сигнал позитивного подтверждения передатчику. Если в данных появляется ошибка, приемник отправляет сигнал негативного подтверждения передатчику. Пример такой передачи изображен на рисунке (см. рис. 2):

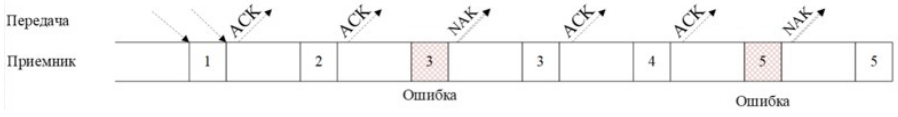

Рисунок 2 - Режим остановка-запрос-ожидание

DOI: https://doi.org/10.60797/IRJ.2024.143.92.2

2. Непрерывный режим запрос-возврат. Соединение осуществляется одновременно по разделенным каналам приема-передачи. Необходимо установление временной задержки для точного согласования отправленных и принятых блоков с сигналами подтверждения. При получении сигнала об ошибке передатчик повторно отправляет данные через временной интервал, соответствующей установленной задержке, начиная с поврежденного блока. Пример такой передачи изображен на рисунке (см. рис. 3):

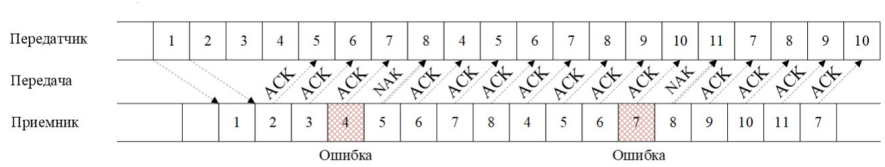

Рисунок 3 - Непрерывный режим запрос-возврат
DOI: https://doi.org/10.60797/IRJ.2024.143.92.3

3. Непрерывный режим с избирательной передачей. Соединение осуществляется одновременно по разделенным каналам приема-передачи. Как и в случае с режимом запрос-возврат устанавливается временной интервал, но передается только искаженный блок, а безошибочно принятые блоки – нет, затем процесс передачи сообщения возобновляется с места прерывания. Пример такой передачи изображен на рисунке (см. рис. 4):

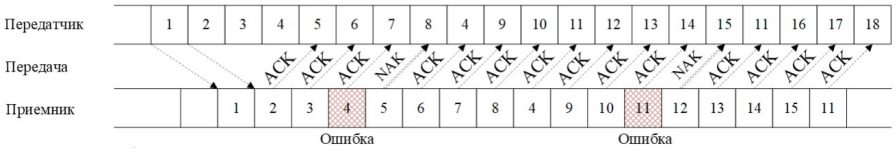

Рисунок 4 - Непрерывный режим с избирательной передачей
DOI: https://doi.org/10.60797/IRJ.2024.143.92.4

Основополагающим моментом алгоритмов автоматического запроса повторной передачи являются механизмы, использующие циклические блочные коды для определения ошибки в полученных данных.

CRC – циклический избыточный код, предназначенный для обнаружения ошибок при проверке целостности данных.

Алгоритм вычисления можно описать следующим образом [9]: к M-битному сообщению добавляется K-битный избыточный код. Новое информационное слово должно делиться на число, выбранное определенным способом. При делении без остатка ошибка исключается, если же появляется остаток, то при передаче данные были повреждены.

После добавления битов код будет иметь длину A битов и называться (A,M)-битным кодом. Для него выбирается полином g(x), высшей степенью которого является число A-M=K, которое и генерирует число избыточных битов.

Алгоритм также можно записать в математическом виде.

Информационное сообщение:

$$M(x) = m_{M-1}\mathrm{X}^{M-1} + m_{M-2}{}^{M-2} + \cdots m_1 X + m_0 \quad (1)$$

Коэффициенты полинома:

$$K(x) = k_{K-1}\mathrm{X}^{K-1} + k_{K-2}{}^{K-2} + \cdots k_1 X + k_0 \quad (2)$$

Полиномиальный генератор:

$$G(x) = g_{K-1}\mathrm{X}^{K-1} + g_{K-2}{}^{K-2} + \cdots g_1 X + g_0 \quad (3)$$

Связь между полиномами описывается соотношениями:

$$B(x) + C(x) = (M(x)X^K)/(G(x)) \quad (4)$$

$$M(x) = B(x)G(x) + C(x) \quad (5)$$

где B(x) – частное от деления сгенерированного информационного сообщения на порождающий полином, при дальнейшем рассмотрении не участвует и отбрасывается; C(x) – остаток от деления сгенерированного информационного сообщения на порождающий полином, является контрольной суммой, и именно по нему определяют наличие ошибок при передаче.

Добавление избыточного кода осуществляется записью его разрядов после младшего бита информационного слова.

Операция деления выполняется по модулю 2 без переноса разрядов, что эквивалентно логической операции XOR. Данные вычисления носят название CRC-арифметики.

Можно выделить наиболее широко используемые полиномы: CRC-8, CRC-16 и CRC-32. Увеличение длины порождающего полинома обеспечивает достижение большей надежности. Так, при использовании CRC-32 надежность достигает значения 2^{32}, то есть вероятность обнаружения ошибки близка к стопроцентной.

Алгоритм контрольной суммы CRC-32-IEEE 802.3 имеет вид:

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1 \quad (6)$$

Используется в процедурах передачи звуковых сигналов и видеоизображений с использованием MPEG-2, при передаче изображений формата PNG, в протоколах связи модемов.

Рассмотренный выше алгоритм – не единственный способ вычисления циклического кода. Возможно практическое применение его модификации, упрощающей вычисления с принимающей стороны [10]. Для аппаратной реализации следующий метод вычисления называется «стандартным»:

1. Во все биты регистра загружаются нули. Движение разрядов происходит от младшего к старшему.
2. Происходит сдвиг от младшего разряда к старшему, старший бит выносится за пределы регистра, в младший бит записывается первый бит информационного сообщения.
3. Если вынесенный бит – 1, то происходит операция XOR битов регистра с битами выбранного полинома, за исключением старшего.
4. Если вынесенный бит 0 – снова происходит сдвиг разрядов по пункту 2.
5. Сдвиг происходит до тех пор, пока все биты информационного слова не поступят в регистр, иначе – пункт 2.
6. В итоге регистр содержит контрольную сумму CRC.

Наиболее часто используемым для вычисления контрольной суммы применяется циклический код CRC-32. Эта контрольная сумма используется в процедурах передачи звуковых сигналов и видеоизображений с использованием MPEG-2, при передаче графики формата PNG, в протоколах связи модемов, в протоколах сжатия архиваторов и для подтверждения целостности других стандартов.

Стоит отметить, что речь идет об алгоритме контрольной суммы CRC-32-IEEE 802.3, полином которого был приведен выше. Для вычисления CRC матрица будет выглядеть немного иначе, учитывая степень порождающего полинома. Объем памяти, выделенный устройством, должен составлять минимум 32 байта [11], а по алгоритму, рассчитанному в другом источнике, уже 1024 байта [12]. Схема матричных вычислений однобайтового сдвига для CRC-32 выглядит следующим образом (см. рис. 5):

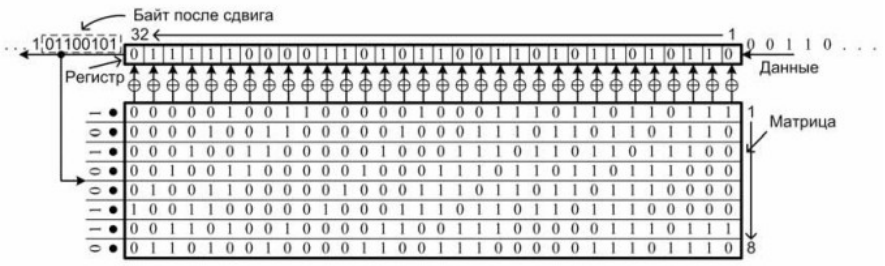

Рисунок 5 - Схема матричного метода вычисления CRC-32
DOI: https://doi.org/10.60797/IRJ.2024.143.92.5

Описанные действия используют в своей основе однобайтовый сдвиг. На практике применяется также вынесение сразу 4 байт (четырехбайтовый сдвиг). При этом количество строк матрицы увеличивается до 32. Объем памяти, выделенный устройством, должен составлять минимум 128 байт.

Также стоит отметить, что для любой длины порождающего полинома используется одна и та же, поэтому строки в ней совпадают, различается только их количество в зависимости от длины информационного сообщения. Схема матричных вычислений четырехбайтового сдвига для CRC-32 представлена на рисунке (см. рис. 6):

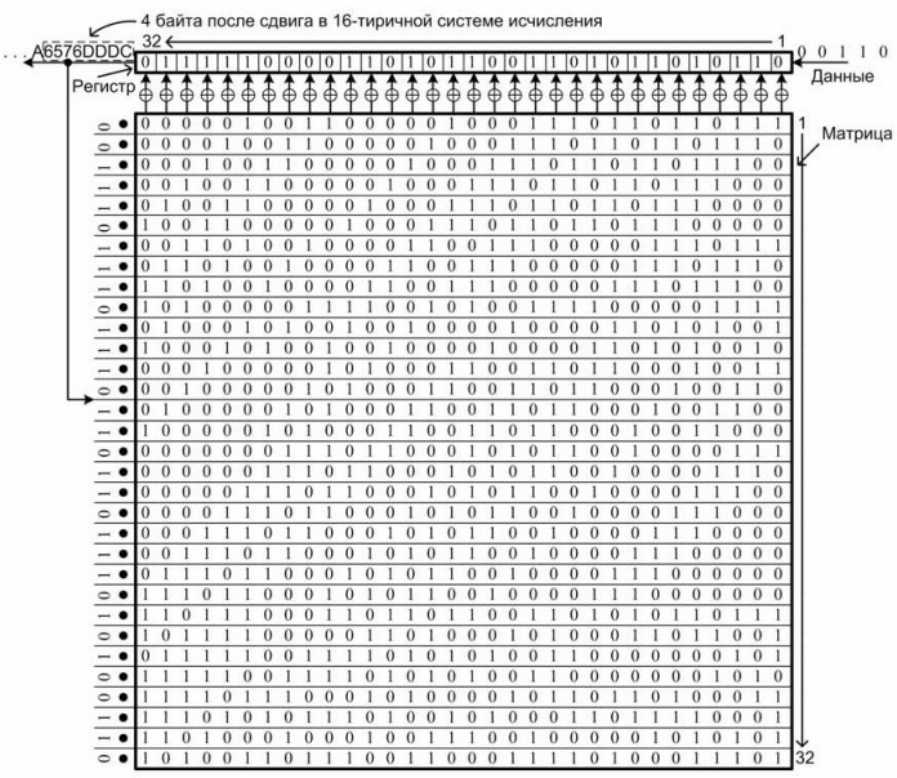

Рисунок 6 - Схема матричного метода вычисления CRC-32 с 4-байтовым сдвигом
DOI: https://doi.org/10.60797/IRJ.2024.143.92.6

Методы исследования

Далее представлено моделирование работы системы циклических избыточных кодов для проверки целостности данных в программе динамического моделирования SimInTech.

Рассматривается CRC-код со следующим набором параметров:

- Название алгоритма (Alg): CRC-32-IEEE 802.3.
- Полиномиальный генератор (g(X)): 0x04C11DB7.
- Инициализирующее значение регистров (Init): 0xFFFFFFFF.
- Флаг, указывающий, инвертируется ли порядок битов сообщения при входе в регистры (RefIn): false.
- Флаг, указывающий, инвертируется ли порядок битов регистра при выходе (RefOut): false.
- Число, с которым складывается по модулю 2 проверочные биты (XorOut): 0x0.

Основные результаты

Модель представлена на рисунке (см. рис. 7).

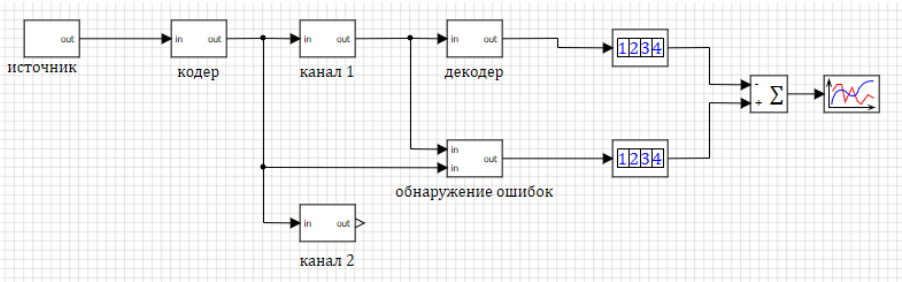

Рисунок 7 - Модель работы системы циклических избыточных кодов для проверки целостности данных
DOI: https://doi.org/10.60797/IRJ.2024.143.92.7

Содержание отдельных субмодулей представлено ниже.

1. Источник

Модель источника передаваемых данных, формирует случайное информационное сообщение заданной длины, а затем формирует 0 на выходе в течение времени формирования заданного числа проверочных бит. Содержание субмодуля «Источник» представлено на рисунке (см. рис. 8).

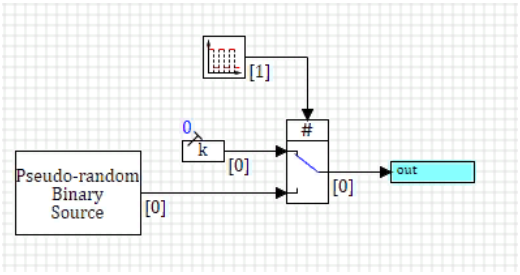

Рисунок 8 - Субмодуль «Источник»
DOI: https://doi.org/10.60797/IRJ.2024.143.92.8

2. Кодер

Модель кодера содержит ключи, которые должны переключаться после передачи информационных бит сообщения. Необходимо сформировать сигнал, который будет равен «1» в течение передачи информационных бит и «0» в течение передачи проверочных бит. Блоки «Запаздывание на период квантования» моделируют сдвиговые регистры кодера. Информационный бит должен задерживаться в регистре на 1 период передачи. Также, после завершения кодирования следует сбросить значения, содержащиеся в регистрах, чтобы они не повлияли на кодирование следующего информационного сообщения. Для корректной работы кодера после передачи информационных бит в цепь обратной связи регистров следует подавать «0». Реализация работы субмодуля «Кодер» представлена на рисунке (см. рис. 9).

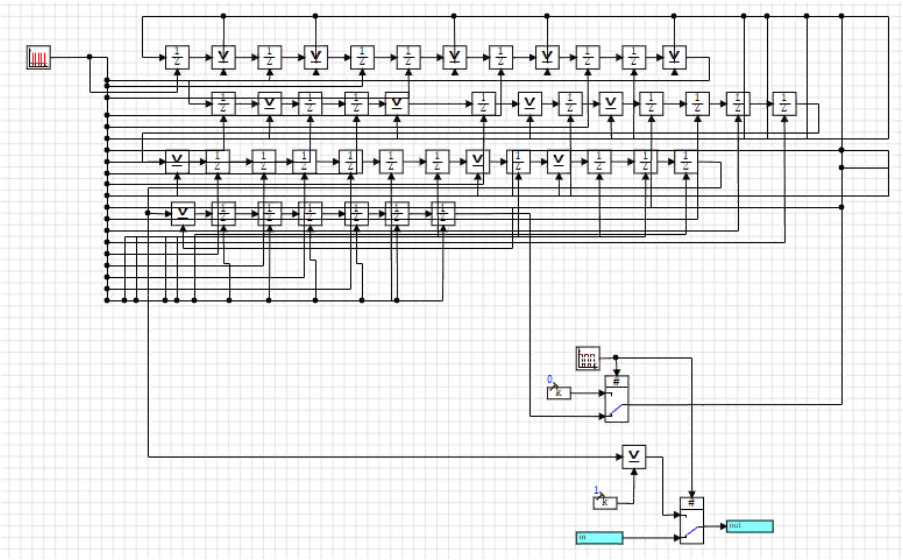

Рисунок 9 - Субмодуль «Кодер»
DOI: https://doi.org/10.60797/IRJ.2024.143.92.9

2. Канал 1

Модель канала связи должна функционировать следующим образом: блок «Равномерный шум» должен формировать случайное число в диапазоне от 0 до 1, в блоке «Константа» должна задаваться вероятность ошибки в канале связи. Если случайное число меньше заданной вероятности, то к информационному биту добавляется ошибка при помощи блока «XOR». Реализация работы субмодуля «Канал 1» представлена на рисунке (см. рис. 10).

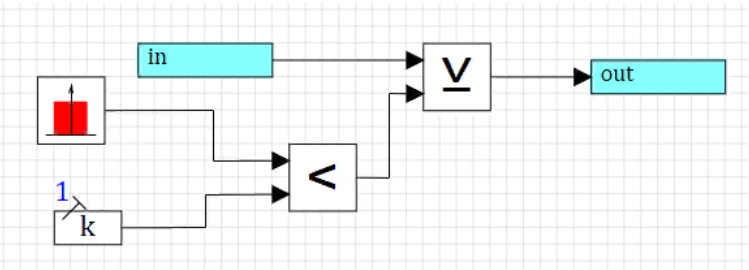

Рисунок 10 - Субмодуль «Канал 1»
DOI: https://doi.org/10.60797/IRJ.2024.143.92.10

3. Канал 2

Модель канала связи функционирует следующим образом: вероятность возникновения ошибки динамически изменяется в процессе передачи сообщения, благодаря этому возможно гарантировать, что для каждого передаваемого сообщения возникнет заданное количество ошибок. Реализация работы субмодуля «Канал 2» представлена на рисунке (см. рис. 11).

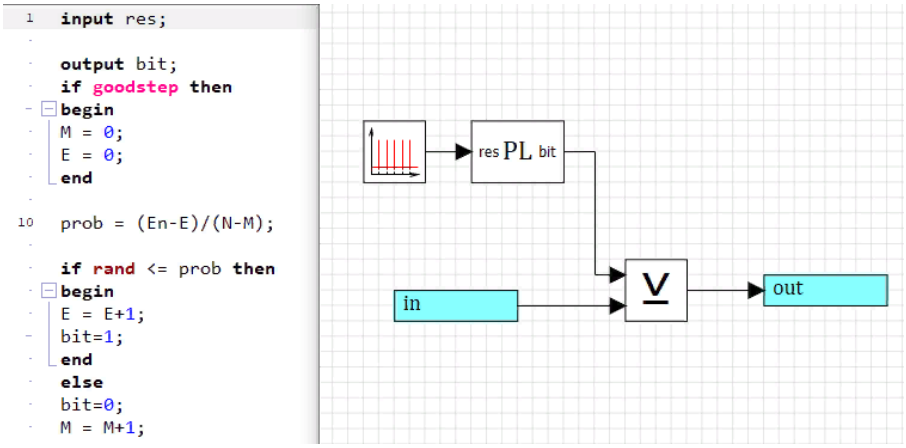

Рисунок 11 - Субмодуль «Канал 2»

DOI: https://doi.org/10.60797/IRJ.2024.143.92.11

4. Декодер

Следует сформировать сигнал сброса, который будет равен «1» в момент времени перед началом декодирования нового информационного сообщения. Для определения наличия ошибки в полученном сообщении следует просуммировать значения, оставшиеся в сдвиговых регистрах после завершения декодирования, при помощи блока «Суммирование элементов вектора». Сигнал о наличии ошибки будет сформирован в момент окончания декодирования, во время декодирования необходимо формировать на выходе декодера нулевой сигнал. Реализация работы субмодуля «Декодер» представлена на рисунке (см. рис. 12).

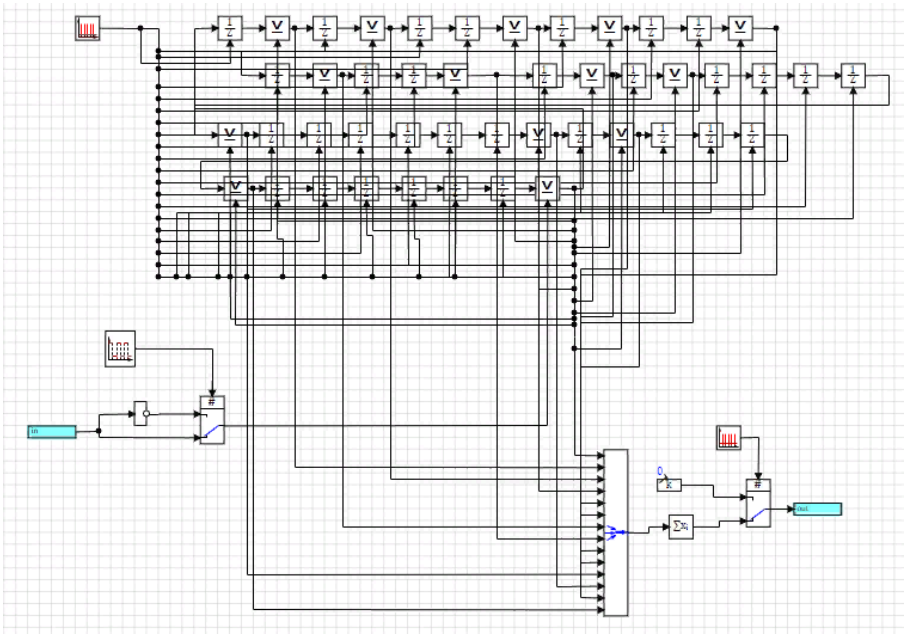

Рисунок 12 - Субмодуль «Декодер»

DOI: https://doi.org/10.60797/IRJ.2024.143.92.12

6. Обнаружение ошибок

Блоки «Буфер последовательного ввода данных» должны объединять принятые биты в вектор сообщения заданной длины. После окончания принятия сообщения следует очистить буферы и вывести количество отличающихся бит на выходной порт субмодели. Реализация работы субмодуля «Обнаружение ошибок» представлена на рисунке (см. рис. 13).

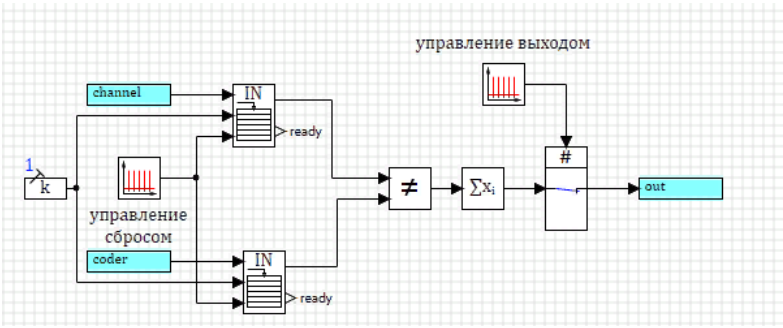

Рисунок 13 - Субмодуль «Обнаружение ошибок»
DOI: https://doi.org/10.60797/IRJ.2024.143.92.13

Параметры, заданные перед началом моделирования представлены в таблице (см. табл. 1).

Таблица 1 - Параметры моделирования

DOI: https://doi.org/10.60797/IRJ.2024.143.92.14

Сокращение	Значение	Пояснение
K	384	Количество информационных бит
P	9	Количество проверочных бит
T	0,1	Период передачи одного бита
En	1	Количество ошибок
W	1000	Количество переданных слов

При вероятности ошибки в канале связи, равной 1, реализация динамического моделирования представлена на рисунке (см. рис. 14).

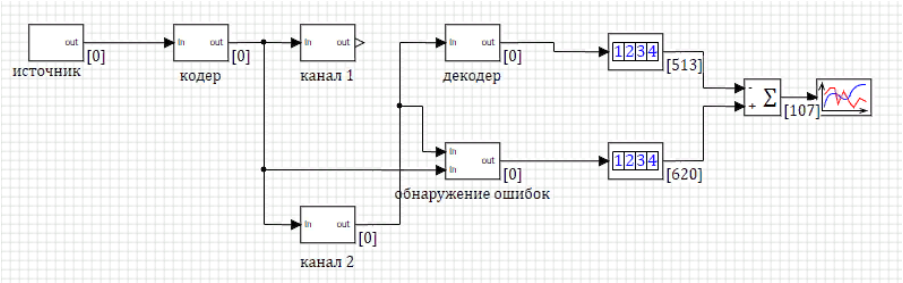

Рисунок 14 - Реализация динамического моделирования
DOI: https://doi.org/10.60797/IRJ.2024.143.92.15

Объективность модели и системы распознавания ошибки была проверена следующей формулой:

$$P_{\text{необ}}(E_{\text{р}}) = k/m \quad (7)$$

где $P_{\text{необ.}}$ – Вероятность необнаруженной ошибки; $E_{\text{р}}$ – вероятности ошибки в канале связи; k – количество необнаруженных ошибок; m – общее количество ошибок.

Подведение итогов моделирования работы CRC-32-IEEE 802.3 представлено в таблице (см. табл. 2).

Таблица 2 - Подведение итогов моделирования работы CRC-32-IEEE 802.3

DOI: https://doi.org/10.60797/IRJ.2024.143.92.16

Вероятности ошибки в	0,10	0,20	0,30	0,40	0,50	0,60	0,70	0,80	0,90	1,00

канале связи ($P_{необ.}$)										
Вероятность необнаруженной ошибки (E_p)	0,08	0,20	0,16	0,17	0,16	0,20	0,20	0,19	0,18	0,17
Количество необнаруженных ошибок (k)	51	134	103	104	101	136	129	120	113	107
Общее количество ошибок (m)	637	644	617	616	612	648	640	633	624	620

Результаты моделирования работы CRC-32-IEEE 802.3 говорят о высокой степени защиты данных, передаваемых по каналам связи и оптимальной работе всей системы.

Заключение

Таким образом, в статье были рассмотрены области применения телемедицины и определен ряд предъявляемых к ней требований, что позволило выделить самое главное из них – надежность. Были определены основные алгоритмы проверки целостности, увеличивающие значение надежности, и подробно разобран один из них – циклический избыточный код (CRC), позволяющий детектировать ошибки в данных при передаче, и схематично рассмотрен принцип работы и методы вычисления CRC. Было проведено моделирование работы CRC-32-IEEE 802.3 и сделаны выводы о его высокой надежности путем определения влияния отношения количества необнаруженных ошибок к их общему количеству – вероятности необнаруженной ошибки к вероятности ошибки в канале связи.

На основании проведенного анализа можно сделать вывод, что применение CRC обеспечивают сохранение целостности передаваемого сигнала, тем самым повышая надежность телемедицинских систем, позволяя осуществлять обмен медицинской информацией с минимальной вероятностью появления ошибки в принятых данных. Этот факт является критически важным, что говорит о точности и безопасности телемедицинских систем как с точки зрения здравоохранения – повышением качества оказываемых услуг, так и со стороны социального аспекта – увеличением уровня доверия населения и созданием положительного образа телемедицины.

Конфликт интересов

Не указан.

Рецензия

Сообщество рецензентов Международного научно-исследовательского журнала
DOI: https://doi.org/10.60797/IRJ.2024.143.92.17

Conflict of Interest

None declared.

Review

International Research Journal Reviewers Community
DOI: https://doi.org/10.60797/IRJ.2024.143.92.17

Список литературы / References

1. Карев С.А.. Нормативно-правовая база и инновации дистанционной медицины / С.А. Карев // Социально-экономическая эффективность управления общественным здоровьем: философско-методологические основания; под ред. Л.А. Тутова — Москва: ТЕИС, 2018. — с. 133-136.

2. Мороз И.Н. Этические и деонтологические аспекты телемедицины / И.Н. Мороз, В.Ч. Можейко // Бюллетень Национального научно-исследовательского института общественного здоровья имени Н. А. Семашко. — 2017. — 1.

3. Журавлев М.С. Защита персональных данных в телемедицине / М.С. Журавлев // Право. Журнал Высшей школы экономики. — 2016. — 3.

4. Перепечина И.О. Криминалистическое прогнозирование и криминалистическая превенция киберпреступлений в сфере здравоохранения / И.О. Перепечина, Д.В. Перепечин // Пробелы в российском законодательстве. — 2020. — 5.

— URL: https://cyberleninka.ru/article/n/kriminalisticheskoe-prognozirovanie-i-kriminalisticheskaya-preventsiya-kiberprestupleniy-v-sfere-zdravoohraneniya (дата обращения: 08.03.2024)

5. Alesanco A. The effects of transmission errors in ECG real-timewavelet compression codecs / A. Alesanco, R. Istepanian, J. Garcia // Computers in Cardiology. — 2005. — 1. — p. 45-48. — DOI: 10.1109/CIC.2005.1588029.

6. Плотников, А.В. Стандарт DICOM в компьютерных медицинских технологиях / А.В. Плотников, Д.А. Прилуцкий, С.В. Селищев // МИЭТ. — URL: https://mks.ru/library/article/1997/dicom.html?ysclid=ltmv8on8m5876732553 (дата обращения: 10.03.2024)

7. ГОСТ Р 54714-2011. Телевидение вещательное цифровое. Наземное цифровое телевизионное вещание. Синхронизация одночастотных сетей. Общие технические требования — Введ. 2012-09-01. — Москва: Стандартинформ, 2012.— 20 с.

8. Применение циклических избыточных кодов для проверки целостности данных // Справочная система SimInTech. — URL: https://help.simintech.ru/index.html?q=/4_nachalo_raboty/laboratornye_raboty_organizacii/RGRTU/cifrovaya_svyaz/DAT_primenenie_ciklicheskix_izbytochnyx_kodov.html (дата обращения: 09.03.2024)

9. Темников Ф.Е. Теоретические основы информационной техники / Ф.Е. Темников, В.А. Афонин, В.И. Дмитриев — Москва: Энергия, 1979. — 512 с.

10. Мальчуков А.Н. Быстрое вычисление контрольной суммы CRC: Таблица против матрицы / А.Н. Мальчуков, А.Н. Осокин // Прикладная информатика. — 2010. — 2. — URL: https://cyberleninka.ru/article/n/bystroe-vychislenie-kontrolnoy-summy-crc-tablitsa-protiv-matritsy (дата обращения: 09.03.2024)

11. Буркатовская Ю.Б. Быстродействующие алгоритмы деления полиномов в арифметике по модулю два / Ю.Б. Буркатовская, А.Н. Мальчуков, А.Н. Осокин // Известия ТПУ. — 2006. — 1. — URL: https://cyberleninka.ru/article/n/bystrodeystvuyuschie-algoritmy-deleniya-polinomov-v-arifmetike-po-modulyu-dva (дата обращения: 09.03.2024)

12. Ross N.W. A Painless Guide to CRC Error Detection Algorithms // N.W. Ross. — 1993. — URL: http://www.ross.net/crc/download/crc_v3.txt (accessed: 10.03.2024).

Список литературы на английском языке / References in English

1. Karev S.A.. Normativno-pravovaja baza i innovatsii distantsionnoj meditsiny [Regulatory framework and innovations of distance medicine] / S.A. Karev // Socio-economic efficiency of public health management: philosophical and methodological foundations; edited by L.A. Tutova — Moskva: TEIS, 2018. — p. 133-136. [in Russian]

2. Moroz I.N. Eticheskie i deontologicheskie aspekty telemeditsiny [Ethical and deontological aspects of telemedicine] / I.N. Moroz, V.Ch. Mozhejko // Bulletin of the N. A. Semashko National Research Institute of Public Health. — 2017. — 1. [in Russian]

3. Zhuravlev M.S. Zaschita personal'nyh dannyh v telemeditsine [Personal data protection in telemedicine] / M.S. Zhuravlev // Law. Journal of the Higher School of Economics. — 2016. — 3. [in Russian]

4. Perepechina I.O. Kriminalisticheskoe prognozirovanie i kriminalisticheskaja preventsija kiberprestuplenij v sfere zdravoohranenija [Forensic forecasting and forensic prevention of cybercrimes in the field of healthcare] / I.O. Perepechina, D.V. Perepechin // Gaps in Russian legislation. — 2020. — 5. — URL: https://cyberleninka.ru/article/n/kriminalisticheskoe-prognozirovanie-i-kriminalisticheskaya-preventsiya-kiberprestupleniy-v-sfere-zdravoohraneniya (accessed: 08.03.2024) [in Russian]

5. Alesanco A. The effects of transmission errors in ECG real-timewavelet compression codecs / A. Alesanco, R. Istepanian, J. Garcia // Computers in Cardiology. — 2005. — 1. — p. 45-48. — DOI: 10.1109/CIC.2005.1588029.

6. Plotnikov, A.V. Standart DICOM v komp'yuternyh medicinskih tekhnologiyah [DICOM standard in computer medical technologies] / A.V. Plotnikov, D.A. Prilutsky, S.V. Selishchev // MIET. — URL: https://mks.ru/library/article/1997/dicom.html?ysclid=ltmv8on8m5876732553 (accessed: 10.03.2024) [in Russian]

7. GOST R 54714-2011. Televidenie veschatel'noe tsifrovoe. Nazemnoe tsifrovoe televizionnoe veschanie. Sinhronizatsija odnochastotnyh setej. Obschie tehnicheskie trebovanija [Digital broadcast television. Terrestrial digital television broadcasting. Synchronization of single-frequency networks. General technical requirements] — Introduced 2012-09-01. — Moskva: Standartinform, 2012.— 20 p. [in Russian]

8. Primenenie ciklicheskih izbytochnyh kodov dlya proverki celostnosti dannyh [The use of cyclic redundant codes to verify data integrity] // Spravochnaya sistema SimInTech [SimInTech Help System]. — URL: https://help.simintech.ru/index.html?q=/4_nachalo_raboty/laboratornye_raboty_organizacii/RGRTU/cifrovaya_svyaz/DAT_primenenie_ciklicheskix_izbytochnyx_kodov.html (accessed: 09.03.2024) [in Russian]

9. Temnikov F.E. Teoreticheskie osnovy informatsionnoj tehniki [Theoretical foundations of information technology] / F.E. Temnikov, V.A. Afonin, V.I. Dmitriev — Moskva: Energija, 1979. — 512 p. [in Russian]

10. Mal'chukov A.N. Bystroe vychislenie kontrol'noj summy CRC: Tablitsa protiv matritsy [Quick calculation of the CRC Checksum: Table vs. Matrix] / A.N. Mal'chukov, A.N. Osokin // Applied Computer Science. — 2010. — 2. — URL: https://cyberleninka.ru/article/n/bystroe-vychislenie-kontrolnoy-summy-crc-tablitsa-protiv-matritsy (accessed: 09.03.2024) [in Russian]

11. Burkatovskaja Ju.B. Bystrodejstvujuschie algoritmy delenija polinomov v arifmetike po modulju dva [High-speed algorithms for dividing polynomials in arithmetic modulo two] / Ju.B. Burkatovskaja, A.N. Mal'chukov, A.N. Osokin // TPU News. — 2006. — 1. — URL: https://cyberleninka.ru/article/n/bystrodeystvuyuschie-algoritmy-deleniya-polinomov-v-arifmetike-po-modulyu-dva (accessed: 09.03.2024) [in Russian]

12. Ross N.W. A Painless Guide to CRC Error Detection Algorithms // N.W. Ross. — 1993. — URL: http://www.ross.net/crc/download/crc_v3.txt (accessed: 10.03.2024).