УДК 616-71

К ВОПРОСУ ЗАЩИТЫ ДАННЫХ В БИОТЕХНИЧЕСКИХ СИСТЕМАХ МЕДИЦИНСКОГО НАЗНАЧЕНИЯ

О.Б. Зельманский, С.Н. Петров, Д.А. Фомин

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» Минск, Беларусь

Аннотация. Цифровизация системы здравоохранения в Республике Беларусь предусматривает интеграцию синтезируемых биотехнических систем медицинского назначения в медицинскую информационную сеть. Стандарт обмена, управления и интеграции электронной медицинской информации HL7 может применяться для организации процессов обработки, передачи и хранения медицинских данных. При этом актуальной задачей остается обеспечение безопасности медицинских данных, передаваемых биотехническими системами в медицинскую информационную сеть. Настоящая работа содержит описание разработанного веб-приложения, в котором реализована передача информации в формате HL7 сообщений. Для решения вопроса обеспечения защиты информации, передаваемой посредствам HL7 сообщений, проанализированы такие алгоритмы шифрования, как Mars, AES (Rijndel), Twofish, а также их RSA надстройки. С целью обеспечения защиты медицинской

информации обосновано применения в биотехнических системах медицинского назначения алгоритма шифрования Twofish.
Ключевые слова: синтез биотехнических систем; разработка медицинского оборудования; безопасность данных пациентов; защита медицинских данных; HL7 сообщение; цифровизация здравоохранения; eHealth.

TO THE ISSUE OF DATA PROTECTION IN MEDICAL PURPOSE BIOTECHNICAL SYSTEMS

O.B. Zelmanski, S.N. Petrov, D.A. Fomin
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Digitalization of the healthcare system in the Republic of Belarus involves the integration of synthesized biotechnical systems for medical purposes into the medical information network. The standard for the exchange, management and integration of electronic medical information HL7 can be used to organize the processes of processing, transfer and storage of medical data. At the same time, ensuring the security of medical data transmitted by biotechnical systems to the medical information network remains an urgent task. This work contains a description of the developed web application, which implements the transfer of information in the HL7 message format. To solve the issue of ensuring the protection of information transmitted via HL7 messages, such encryption algorithms as Mars, AES (Rijndel), Twofish, as well as their RSA add-ons are analyzed. In order to ensure the protection of medical information, the use of the Twofish encryption algorithm in biotechnical systems for medical purposes is justified.
Keywords: synthesis of biotechnical systems; development of medical equipment; patient data security; protection of medical data; HL7 message; digitalization of healthcare; eHealth.

Введение

В современном информационном обществе цифровизация становится ключевым элементом эффективного функционирования различных областей, включая систему здравоохранения [1]. Республика Беларусь, как одна из стран, активно внедряющих инновационные технологии в сферу здравоохранения, стремится обеспечить высокий уровень медицинского обслуживания и улучшить качество жизни своих граждан. Цифровизация системы здравоохранения в Республике Беларусь – это комплексный процесс, охватывающий внедрение современных информационных технологий для оптимизации медицинских процессов, повышения доступности медицинской помощи и обеспечения безопасности данных пациента. На фоне активных изменений в сфере здравоохранения Республики Беларуси, цифровые технологии становятся неотъемлемой частью системы обеспечения качественных и эффективных медицинских услуг. Таким образом, при разработке медицинских устройств и систем необходимо уделять особое внимание возможности их интеграции в медицинскую информационную сеть посредствам современных коммуникационных технологий, решая при этом задачу обеспечения защиты передаваемых медицинских данных, в том числе персональных.

Стандарт передачи медицинских данных HL7

Одной из актуальных задач в рамках цифровизации здравоохранения является стандартизация процессов обработки, передачи и хранения медицинских данных. Для ее решения международным сообществом по вопросам информатизации здравоохранения Health Level Seven International предложен стандарт HL7 (Health Level Seven), к которому в 2018 году присоединилась Республика Беларусь. Данные в стандарте HL7 организованы в логические блоки, называемые сегментами. Каждый сегмент представляет собой набор полей, которые содержат конкретные элементы информации,

такие как имя пациента, дата рождения и другие медицинские данные. Сегменты объединяются в группы, называемые сообщениями. Группы сегментов образуют структуру сообщений, представляющую собой логически связанный набор данных. Для обработки информации в формате HL7 предлагается протокол MLP (Medical Link Protocol), который предусматривает преобразование информации из HL7 в DICOM (Digital Imaging and Communications in Medicine), являющийся протоколом взаимодействия с медицинским оборудованием. Протокол MLP представляет собой стандарт, разработанный для обмена медицинскими данными между различными системами и приложениями в области здравоохранения. Он обеспечивает эффективный способ передачи информации о пациентах и клинических данных, способствуя интеграции и взаимодействию между различными участниками системы здравоохранения. Использование стандарта HL7 в здравоохранении предоставляет множество преимуществ, но в то же время имеет проблему обеспечения безопасности медицинских данных [2], поскольку он не предоставляет встроенных функций безопасности. Наиболее очевидные угрозы безопасности HL7 аналогичны Telnet и FTP. Это открытый текст, отсутствие аутентификации, отсутствие проверки и необязательность подтверждений [3]. Решение этой проблемы может быть основано на использовании алгоритмов шифрования [4, 5]. Одним из основных требований, которые должны предъявляться к алгоритмам шифрования информации, обрабатываемой в синтезируемых биотехнических системах, является высокая производительность.

Обоснование выбора алгоритма шифрования медицинских данных

С целью реализации обмена информацией по стандарту HL7 на языке программирования «Java Script» было разработано веб-приложение, использующее библиотеку SMART on FHIR JavaScript и реализующее взаимодействие с открытым тестовым медицинским сервером FHIR REST API server. В приложении реализована аутентификация пользователя и доступ к базе электронных медицинских карт пациентов. SMART on FHIR использует протокол OAuth 2.0 для аутентификации и авторизации. Библиотека предоставляет готовые методы для получения токенов доступа, что позволяет безопасно взаимодействовать с защищенными ресурсами. Библиотека предлагает удобные функции для выполнения запросов к API FHIR, включая создание, чтение, обновление и удаление ресурсов. Библиотека совместима с различными веб-платформами и может использоваться как в клиентских, так и в серверных приложениях. Это делает ее универсальным инструментом для разработчиков. С целью выбора алгоритма шифрования медицинских данных на основе результатов исследования, проведенных институтом NIST [4], в качестве объектов исследования были выбраны следующие алгоритмы шифрования данных: Mars, AES (Rijndel), Twofish, а также их RSA надстройки [6]. В процессе проведения исследований было выполнено более 11 000 экспериментов. Суть исследования состояла в оценке скорости шифрования данных различных форматов (*.doc, *.pdf, *.rar, *.ova, *.win, *.bak), различного размера (1 МБ, 5 МБ, 20 МБ, 100 МБ, 500 МБ, 2 ГБ, 5 ГБ, 20 ГБ), на различных аппаратных платформах. В результате установлено, что для защиты информации, передаваемой посредствам HL7 сообщений, целесообразно использовать алгоритм шифрования Twofish.

Заключение

На основе результатов проведенных исследований можно заключить, что в разрабатываемых биотехнических системах наиболее целесообразно использовать

алгоритм шифрования Twofish для защиты информации, передаваемой посредствам HL7 сообщений. Это обусловлено тем, что процесс шифрования как малых, так и больших массивов данных с использованием этого алгоритма характеризуется более высоким быстродействие по сравнению с процессами шифрования массивов данных с использованием других алгоритмов, рекомендуемых в настоящее время NIST.

Список использованных источников

1. Пономарев А.А. Использование Open XML для формирования клинических документов в формате HL7 CDA / А.А. Пономарев, Тап Ван Фам // Экономика, Статистика и Информатика. – 2010. – № 3. – С. 147–152.

2. Магомедов Ш.Г. Анализ защиты компьютерных сетей и приложений информационных процессов учреждений здравоохранения / Ш. Г. Магомедов // Cloud of Science. – 2020. – № 7(3). – С. 685–704.

3. Даллас Хазелхорст. Взлом интерфейсов данных HL7 в медицинских средах: атака и защита – ахиллесова пята здравоохранения [Электронный ресурс]. – Режим доступа: https://linuxincluded.com/hl7-medical-attacking-defending/: 24.02.2025.

4. Рябко Б.Я., Криптография в информационном мире / Б.Я. Рябко, А.Н. Фионов. – М.: Горячая Линия - Телеком, 2018. – 302 с.

5. Хан А.А. Специальный выпуск по информационной безопасности и криптографии: роль передовых цифровых технологий / А. А. Хан. Л. Й. Пор // Прикладные науки. – 2024. – № 14(5), 2045.

6. Баскаков И.В. Защита информации в информационных системах : учебное пособие / И.В. Баскаков, В.Л. Евсеев, А.В. Пролетарский. А.М. Суровов. – Москва : Рудомино. 2011. – 362 с.

References

1. Ponomarev, A. A. Using open xml in order to implement the electronic documents in the clinical format hl7 CDA / A. A. Ponomarev, Tap Van Pham // Economy, Statistics and informatics. – 2010. – № 3. – P. 147–152.

2. Magomedov, S. G. Security Analysis of Computer Networks and Applications of the Healthcare Organizations Information Processes / S. G. Magomedov // Cloud of Science. – 2020. – № 7(3). – P. 685–704.

3. Dallas Haselhorst. Hacking HL7 Data Interfaces in Medical Environments: Attacking and Defending the Achille's Heel of Healthcare [Electronic resource]. – Access mode: https://linuxincluded.com/hl7-medical-attacking-defending/: 24.02.2025.

4. Ryabko, B.Y. Cryptography in the information world / B.Y. Ryabko, A.N. Fionov. – M.: Hot Line - Telecom, 2018. – 302 p.

5. Khan, A. A. Special issue on information security and cryptography: the role of advanced digital technology / A. A. Khan. L. Y. Por // Applied Sciences. – 2024. – № 14 (5), 2045.

6. Baskakov, I.V. Information protection in information systems / I.V. Baskakov, V.L. Evseev, A.V. Proletarsky, A.M. Surovov. – Moscow : Rudomino, 2011. – 361 p.

Сведения об авторах

Зельманский О.Б., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», 7650772@rambler.ru.
Петров С.Н., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». petrov@bsuir.by.
Фомин Д.А., магистрант каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». d.fomin@bsuir.by.

Information about the authors

Zelmanski O.B., Cand. of Sci., Associate Professor, Associate Professor of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", 7650772@rambler.ru
Petrov S.N., Cand. of Sci., Associate Professor, Associate Professor of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", petrov@bsuir.by
Fomin D.A., Master student of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", d.fomin@bsuir.by.