http://dx.doi.org/10.35596/1729-7648-2026-32-2-28-34

УДК 004.056:616-071:615.47

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ МЕДИЦИНСКИХ ДАННЫХ ПАЦИЕНТОВ В БИОТЕХНИЧЕСКИХ СИСТЕМАХ

О. Б. ЗЕЛЬМАНСКИЙ, В. А. БОГУШ

Белорусский государственный университет информатики и радиоэлектроники (Минск, Республика Беларусь)

Аннотация. Рассмотрена интеграция биотехнических устройств и систем в медицинскую информационную сеть. Обосновано применение методов криптографической защиты медицинских данных, передаваемых между различными системами, приложениями и организациями здравоохранения, с целью обеспечения их конфиденциальности и целостности с учетом требований по работе с персональными данными и к врачебной тайне. Разработано программное средство, реализующее обработку информации в формате сообщений стандарта Health Level Seven, их шифрование и дешифрование. Исследованы зависимости скорости шифрования и объема выходных данных от применяемого криптографического алгоритма, что позволило обосновать выбор алгоритма, обладающего высоким быстродействием и минимальным влиянием на функционирование биотехнических систем. На основе результатов исследования по защите информации, передаваемой с использованием Health Level Seven, продемонстрирована целесообразность гибридного шифрования.

Ключевые слова: биотехнические системы, стандарт Health Level Seven, криптография, защита персональных данных, врачебная тайна, цифровизация здравоохранения.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Зельманский, О. Б. Обеспечение защиты медицинских данных пациентов в биотехнических системах / О. Б. Зельманский, В. А. Богуш // Цифровая трансформация. 2026. Т. 32, № 2. С. 28–34. http://dx.doi.org/10.35596/1729-7648-2026-32-2-28-34.

ENSURING THE PROTECTION OF PATIENT MEDICAL DATA IN BIOTECHNICAL SYSTEMS

OLEG ZELMANSKI, VADIM BOGUSH

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Abstract. This paper examines the integration of biotechnical devices and systems into a medical information network. The use of cryptographic protection methods for medical data transferred between various systems, applications, and healthcare organizations is substantiated to ensure their confidentiality and integrity, taking into account requirements for handling personal data and medical confidentiality. A software tool has been developed that implements the processing of information in the Health Level Seven message format, as well as their encryption and decryption. The dependence of encryption speed and output data size on the cryptographic algorithm used is analyzed, allowing for the selection of an algorithm offering high performance and minimal impact on the functioning of biotechnical systems. Based on the results of the study on the protection of information transferred using Health Level Seven, the feasibility of hybrid encryption is demonstrated.

Keywords: biotechnical systems, Health Level Seven standard, cryptography, personal data protection, medical confidentiality, digitalization of healthcare.

Conflict of interests. The authors declare that there is no conflict of interests.

For citation. Zelmanski O., Bogush V. (2026) Ensuring the Protection of Patient Medical Data in Biotechnical Systems. *Digital Transformation.* 32 (2), 28–34. http://dx.doi.org/10.35596/1729-7648-2026-32-2-28-34 (in Russian).

Введение

Одной из актуальных задач в рамках цифровизации системы здравоохранения является стандартизация процессов обработки, хранения и передачи медицинских данных в информационных системах при взаимодействии организаций, участвующих в оказании медицинской помощи[1,2]. Для ее решения международным сообществом по вопросам информатизации здравоохранения Health Level Seven International, аккредитованным American National Standards Institute, предложен стандарт HL7 (Health Level Seven), к которому в 2018 году в рамках реализации проекта «Модернизация системы здравоохранения Республики Беларусь» присоединилась наша страна.

Стандарт HL7 используется в качестве основы для цифровой трансформации здравоохранения, обеспечивая совместимость данных для электронных медицинских карт, телемедицины и управления здоровьем населения. Для здравоохранения документ предоставляет множество преимуществ. Однако HL7 не решает проблему безопасности медицинских данных, в том числе персональных [1], поскольку не содержит встроенных функций обеспечения конфиденциальности и целостности. Наиболее очевидные угрозы безопасности, изложенные в HL7, аналогичны Telnet (Teletype Network) и FTP (File Transfer Protocol) и связаны с открытостью текста, отсутствием аутентификации и проверок, с иными уязвимостями[3]. Поэтому для защиты медицинской информации (Protected Health Information) необходимо применять сторонние средства защиты на сетевом (протокол Internet Protocol Security), транспортном (протокол Transport Layer Security 1.3) или прикладном (протокол Hyper Text Transfer Protocol Secure) уровнях модели взаимодействия открытых систем или обеспечивать безопасность всей среды передачи (частная закрытая сеть, защищенная канальными средствами).

В то же время решение задачи обеспечения безопасности передаваемой медицинской информации в соответствии со стандартом HL7 [2, 3] может быть основано на использовании алгоритмов шифрования. Основные требования, которые должны предъявляться к алгоритмам шифрования информации, обрабатываемой в синтезируемых биотехнических системах, – это высокая криптографическая стойкость и производительность.

Анализ формата медицинских данных,
передаваемых с использованием стандарта Health Level Seven

Наиболее распространенными версиями стандарта HL7 являются HL7 Version 2.x (v2) и HL7 Version 3 (v3). Версия HL7 Version 2.x (v2), широко применяемая на практике для обмена клиническими и административными данными между информационными системами учреждения здравоохранения, обеспечивает обратную совместимость между версиями 2.x. Однако в HL7 Version 2.x (v2) отсутствуют встроенные механизмы защиты передаваемых данных, передача сообщений осуществляется в открытом виде с помощью протокола низкого уровня MLLP (Minimal Lower Layer Protocol), инкапсулированного в стек протоколов TCP/IP.

Версия HL7 Version 3 (v3) отличается более строгой и формально определенной структурой сообщений, такой как CDA (Clinical Document Architecture) XML-структура. Несмотря на предусмотренные метаданные безопасности, в частности, пометки о конфиденциальности отдельных элементов данных, проблема их защиты остается актуальной и для HL7 Version 3 (v3). Передача сообщений в HL7 Version 3 (v3) осуществляется с использованием веб-сервисов SOAP/Web Services, REST/HTTP. Следует отметить, что ввиду большого объема, избыточной сложности и отсутствия совместимости с HL7 Version 2.x (v2), затрудняющих переход с уже налаженных интерфейсов, версия HL7 Version 3 (v3) не получила широкого практического применения.

[1] Об утверждении Концепции развития электронного здравоохранения Республики Беларусь: приказ Министерства здравоохранения Республики Беларусь от 20 марта 2018 г. № 244 [Электронный ресурс] // Министерство здравоохранения Республики Беларусь. Режим доступа: https://www.grsmu.by/files/file/university/accreditation/eHealth_conception.pdf. Дата доступа: 04.02.2026.

[2] Об утверждении Концепции создания единой государственной информационной системы в сфере здравоохранения: приказ Министерства здравоохранения и социального развития Российской Федерации от 28 апреля 2011 г. № 364 [Электронный ресурс] // Министерство здравоохранения и социального развития Российской Федерации. Режим доступа: https://minzdrav.gov.ru/documents/%207200-prikaz-minzdravsotsrazvitiya-rossii-364-ot-28-aprelya-2011-g. Дата доступа: 04.02.2026.

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

Сочетание идей HL7 Version 2.x (v2) и HL7 Version 3 (v3) и упрощение интеграции благодаря использованию веб-технологий позволили сообществу Health Level Seven International разработать новый стандарт для обмена медицинскими данными FHIR (Fast Healthcare Interoperability Resources). FHIR поддерживает современные методы передачи данных, а именно – RESTful API, что улучшает совместимость с веб-сервисами и мобильными приложениями, но в то же время увеличивает вероятность атак через API и получения несанкционированного доступа к медицинским данным, например, в случае использования недостаточно надежной аутентификации или слабых методов авторизации. FHIR описывает только структуры и методы представления данных, а также основанный на использовании меток подход к управлению доступом, но не определяет способы реализации функции безопасности.

Требования законодательства Республики Беларусь к защите медицинских данных

Обмен HL7-сообщениями, содержащими данные пациентов, регламентируется нормами законодательства о персональных данных и врачебной тайне. В Республике Беларусь сформирована правовая база[4], устанавливающая строгие требования к обработке и передаче информации о пациенте в электронной форме.

Следует отметить, что информация о пациенте в HL7-сообщениях представляет собой персональные данные, а биометрическая информация и сведения о здоровье – это специальная категория данных. В связи с чем необходимы наличие законных оснований для обработки таких данных (согласие пациента, исполнение медучреждением своих обязанностей) и соблюдение принципов минимизации, целевой обусловленности. Более того, оператор (и уполномоченные лица) обязан принимать правовые, организационные и технические меры защиты персональных данных от несанкционированного доступа, изменения, распространения и иных неправомерных действий.

Принятый в Республике Беларусь закон[4] прямо указывает на обязательные меры, включающие техническую и криптографическую защиту персональных данных, предусматривает заключение соглашений с уполномоченными лицами (IT-подрядчиками), где отдельно прописываются обязанности по сохранению конфиденциальности персональных данных и обеспечению мер защиты. Работник, который обязан сохранять врачебную тайну, считается соблюдающим требования по защите данных, однако и от него требуется выполнение мер безопасности.

Согласно закону «О здравоохранении»[5], к сведениям, составляющим врачебную тайну, относится информация о факте обращения человека за медицинской помощью, состоянии здоровья, диагнозе, методах лечения и прогнозе. Медицинские работники и организации обязаны хранить данную информацию в тайне и не разглашать ее без согласия пациента (за исключением случаев, прямо предусмотренных законом).

Таким образом, диагнозы, результаты обследований, личные данные пациентов, передаваемые посредством HL7-сообщений, подпадают под действие закона[5]. HL7-сообщения, содержащие персональные медицинские данные, должны передаваться с соблюдением строгих мер защиты, запрещающих доступ к несанкционированному раскрытию врачебной тайны. С учетом требований законодательства применение криптографических методов защиты является обоснованным и необходимым при передаче информации через общедоступные сети.

Результаты исследований программных средств шифрования и их обсуждение

С целью организации обмена информацией в соответствии со стандартом HL7 и выполнения шифрования и дешифрования HL7-сообщений на языке C# (.NET Core) было разработано консольное программное средство, позволяющее оценить скорость шифрования и объем выходных данных для симметричного алгоритма шифрования на примере AES и асимметричного алгоритма шифрования на примере RSA. Программное средство поддерживает работу с такими основными типами HL7-сообщений, как административные (ADM/ADT), заказы на исследования (ORM), результаты обследований (ORU), финансовые транзакции (DFT) и др. [4]. Наиболее распространенным, содержащим типовой набор персональных данных, пересылаемых между

[4] О защите персональных данных: Закон Республики Беларусь от 7 мая 2021 г. № 99-З // Национальный реестр правовых актов Республики Беларусь. 2021. № 5/2.

[5] О здравоохранении: Закон Республики Беларусь от 18 июня 1993 г. № 2435-XII // Ведомости Верховного Совета Республики Беларусь. 1993. № 24. (В редакции Закона Республики Беларусь от 11.01.2023 № 214-З).

информационными системами, является административное HL7-сообщение ADT^A01 о госпитализации/приеме пациента, формируемое при его поступлении в стационар. Структура данного сообщения состоит из ключевых полей, содержащих следующую информацию:

– идентификационные данные пациента: номер медицинской карты, номер истории болезни, номер страхового свидетельства (сегмент PID, поле ID);

– персональные данные пациента: фамилия, имя, отчество, дата рождения, пол, адрес регистрации, контактный телефон (сегмент PID, поля Patient Name, DOB, Sex, Address, Phone);

– медицинские сведения пациента: текущий диагноз или причина госпитализации (сегмент DG1, поле Diagnosis), информация об аллергиях (сегмент AL1) или о проведенных процедурах при приеме;

– административные данные пациента: код отделения/палаты, данные о врачах (лечащий врач, направивший врач), дата и время поступления (сегмент PV1);

– страховые и финансовые данные пациента: информация о страховой компании, страховом полисе, платежных гарантиях (сегменты IN1/IN2).

Таким образом, содержащаяся в ADT^A01 HL7-сообщения информация представляет собой персональные данные, составляет врачебную тайну и подпадает под действие законов[4,5]. В связи с чем ее хранение и передача посредством открытых сетей требуют применения криптографических мер защиты. С целью обоснования выбора криптографического алгоритма шифрования предлагаются следующие критерии:

– криптостойкость, характеризующая надежность и устойчивость шифрования;

– скорость шифрования/расшифрования, поскольку медицинские интерфейсы часто работают в режиме реального времени, обмениваясь сотнями сообщений в минуту;

– эффективность по объему – минимизация добавления криптографических служебных данных, что является немаловажным критерием при ограничении пропускной способности канала связи.

Приведем описание используемых в программном средстве .NET библиотек:

System – включает в себя базовые классы и типы, такие как строки, коллекции, операции ввода/вывода и др.;

System.Diagnostics – содержит классы для взаимодействия с такими диагностическими инструментами, как таймеры и логи. Используется для измерения времени шифрования;

System.Security.Cryptography – пространство имен для работы с криптографическими алгоритмами. Включает классы для симметричного и асимметричного шифрования, хеширования, создания подписей и других криптографических операций;

System.Text – предоставляет классы для работы с текстом (строками), кодировками и т. д. Используется для кодирования и декодирования HL7-сообщений в байтовый формат.

В качестве входных данных программного средства выступает строка sampleHl7, содержащая формируемые веб-приложением HL7-сообщения. В случае симметричного алгоритма AES создается новый объект aes с ключом 256 бит и блоком 128 бит, генерируются случайный ключ и необходимый для режима шифрования CBC (Cipher Block Chaining) вектор инициализации с помощью aes.GenerateKey() и aes.GenerateIV() соответственно. Далее функция AesEncrypt() выполняет шифрование. При этом данные записываются в поток CryptoStream, результат сохраняется в MemoryStream, а через консоль выводится время, затраченное на шифрование. Для получения измеримого времени при очень быстрых операциях процесс шифрования включает 1000 повторений. После чего измеряется и выводится через консоль объем полученного шифротекста в байтах, а также часть зашифрованных данных в шестнадцатеричном виде. Функция AesDecrypt() выполняет дешифрование данных, используя тот же ключ и вектор инициализации, что и при шифровании. Далее расшифрованное сообщение выводится через консоль и сопоставляется с исходным. В случае асимметричного алгоритма RSA создается объект RSA с парой ключей размером 2048 бит. Открытый ключ экспортируется для шифрования данных функцией RsaEncrypt(), закрытый – для их дешифрования. Выходными данными программного средства являются время шифрования и объем зашифрованных сообщений. Диаграмма классов разработанного программного средства шифрования и дешифрования HL7-сообщений приведена на рис. 1.

Было выполнено более 11 000 измерений для генерируемых HL7-сообщений, содержащих различный набор данных. Диаграмма сравнения скорости шифрования $\log_{10}$ и криптографической избыточности алгоритмов шифрования AES и RSA разработанного программного средства приведена на рис. 2.

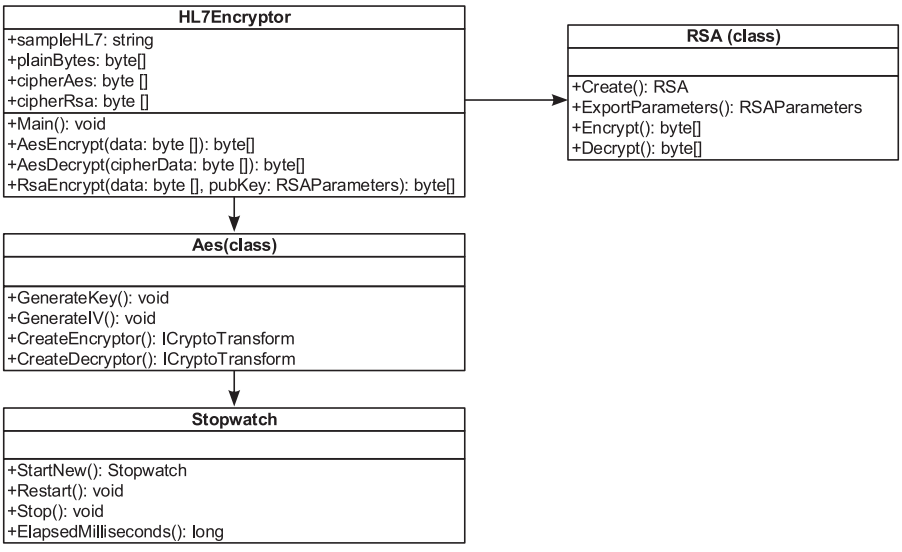

Рис. 1. Диаграмма классов программного средства шифрования и дешифрования HL7-сообщений
Fig. 1. Class diagram of the software for encryption and decryption of HL7 messages

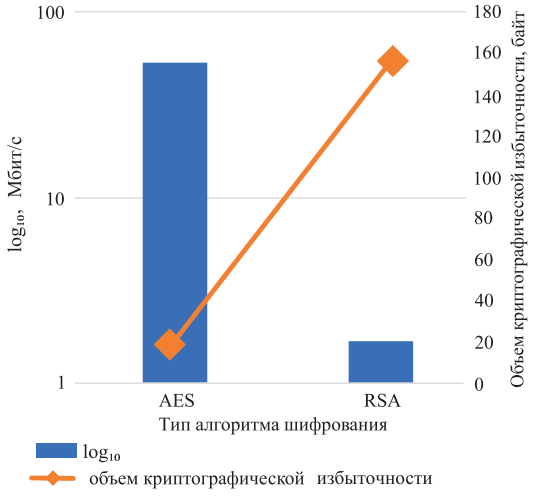

Рис. 2. Диаграмма сравнения производительности и криптографической избыточности алгоритмов шифрования AES и RSA
Fig. 2. Comparative diagram of performance and cryptographic overhead of AES and RSA encryption algorithms

Анализ результатов работы алгоритмов AES и RSA демонстрирует следующее:

– объем исходного HL7-сообщения – 163 байта (UTF8). После AES-шифрования объем шифротекста на 13 байтов превысил объем исходного сообщения за счет добавления служебных данных и составил 176 байтов. RSA-шифрование потребовало разделить исходное сообщение на блоки объемом не более 100 байтов, объем шифротекста после RSA-шифрования каждого блока был определен размером ключа и составил 256 байтов;

– AES-шифрование исходного сообщения объемом 163 байта заняло примерно 0,025 мс, RSA-шифрование одного блока исходного сообщения объемом 100 байтов – 0,48 мс;

– оба алгоритма шифрования не допустили ошибок в процессе шифрования/расшифрования.

Таким образом, при шифровании HL7-сообщений алгоритм AES работает быстрее и незначительно увеличивает объем данных по сравнению с RSA.

Для использования в Республике Беларусь с учетом требований нормативных документов рассмотрен симметричный алгоритм шифрования «БелТ»[6], представляющий собой усиленную

[6] Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности: СТБ 34.101.31–2020. Введ. 01.09.2021. Минск: Госстандарт, 2020.

для соответствия современным требованиям версию ГОСТ 28147–89, аналогом которой является разработанный в Российской Федерации алгоритм по ГОСТ Р 34.12–2015. Указанный алгоритм характеризуется размером блока 64 бита, длиной ключа 256 бит, 32 раундами замен и перестановок. Алгоритм надежен, прост в реализации, имеет невысокие требования к памяти, но может уступать AES по скорости при наличии аппаратно-ускоренного AES. Однако в случае оптимизации и наличия поддержки расширений, например, в российских процессорах «Эльбрус», имеет сопоставимое с AES быстродействие. Объем дополнительных служебных данных составляет объем заполнения до кратности блока (в среднем 8 байтов), а при использовании режима гаммирования с обратной связью – дополнительно длину вектора инициализации 8 байтов.

Таким образом, с учетом национальных нормативных требований для внутренних сертифицируемых систем криптографическую защиту информации, передаваемой с использованием стандарта Health Level Seven, можно обеспечивать с помощью симметричного алгоритма «БелТ», обладающего высоким быстродействием (в сравнении с алгоритмами с открытым ключом) и достаточным уровнем стойкости [5]. С другой стороны, учитывая международную интеграцию в сфере здравоохранения, развитие медицинского туризма и экспорта медицинских услуг, для совместимости с международными системами целесообразной представляется поддержка продемонстрировавшего в ходе проведенных исследований более высокое быстродействие при шифровании как малых, так и больших массивов данных алгоритма AES [6], рекомендованного в настоящее время NIST. С практической точки зрения реализация AES доступна во всех стандартных библиотеках ввиду того, что AES является мировым стандартом, в то время как для «БелТ» потребуются либо сторонние библиотеки, либо собственная реализация. При этом для организации гибридной криптографической системы возможно применение асимметричного алгоритма RSA с целью шифрования сессионных ключей.

Заключение

1. Проведен анализ уязвимостей стандарта Health Level Seven. Установлено, что он не имеет встроенных механизмов защиты передаваемых данных. Предложено использование криптографических методов защиты, основанных на применении алгоритмов шифрования. С целью организации обмена информацией в соответствии со стандартом HL7 разработано программное средство, которое поддерживает работу с основными типами HL7-сообщений, их шифрование и дешифрование, а также позволяет оценить скорость шифрования и объем выходных данных для симметричного алгоритма шифрования на примере AES и асимметричного алгоритма шифрования на примере RSA. Установлено, что при шифровании HL7-сообщений алгоритм AES работает до 20 раз быстрее (0,025 мс для исходного сообщения объемом 163 байта) и незначительно увеличивает объем данных (13 байтов для исходного сообщения объемом 163 байта) по сравнению с алгоритмом RSA (0,48 мс и 156 байтов для исходного сообщения объемом 100 байтов).

2. Обосновано применение симметричного алгоритма шифрования «БелТ» для шифрования информации, передаваемой с использованием стандарта HL7 в национальных сертифицируемых системах Беларуси. Однако, учитывая международную интеграцию в сфере здравоохранения, развитие медицинского туризма и экспорта медицинских услуг, для совместимости с международными системами целесообразной представляется также поддержка алгоритма AES. Для решения задач интеграции целесообразно применение гибридных криптосистем, в которых шифрование пользовательских данных выполняется с помощью симметричных алгоритмов, а шифрование их сессионных ключей – посредством асимметричного алгоритма RSA.

3. Научные исследования выполнены в рамках гранта Президента Республики Беларусь.

Список литературы

1. Магомедов, Ш. Г. Анализ защиты компьютерных сетей и приложений информационных процессов учреждений здравоохранения / Ш. Г. Магомедов // Cloud of Science. 2020. Т. 7, № 3. С. 685–704.
2. Рябко, Б. Я. Криптография в информационном мире / Б. Я. Рябко, А. Н. Фионов. М.: Горячая линия – Телеком, 2018.
3. 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. Vol. 14, No 5. DOI: 10.3390/app14052045.

4. Зельманский, О. Б. К вопросу защиты данных в биотехнических системах медицинского назначения / О. Б. Зельманский, С. Н. Петров, Д. А. Фомин // Технические средства защиты информации: материалы XXIII Белор.-Рос. науч.-техн. конф., Минск, 8 апр. 2025 г. Минск, 2025. С. 168–171.
5. Зельманский, О. Б. Обеспечение защиты медицинских данных в биотехнических системах / О. Б. Зельманский // Современные средства связи: материалы XXX Междунар. науч.-техн. конф., Минск, 30–31 окт. 2025 г. Минск, 2025. С. 80–81.
6. Justification of Encryption Algorithm for Systems Monitoring Personnel Condition of Critical Informatization Objects / O. Boiprav [et al.] // Problems of Information Technology. 2024. Vol. 15, No 2. P. 3–8.

Поступила 27.02.2026 Принята в печать 09.03.2026 Доступна на сайте 10.07.2026

References

1. Magomedov S. G. (2020) Security Analysis of Computer Networks and Applications of the Healthcare Organizations Information Processes. *Cloud of Science*. 7 (3), 685–704 (in Russian).
2. Ryabko B. Ya., Fionov A. N. (2018) *Cryptography in the Information World*. Moscow, Hot Line – Telecom (in Russian).
3. Khan A. A., Por L. Y. (2024) Special Issue on Information Security and Cryptography: The Role of Advanced Digital Technology. *Applied Sciences*. 14 (5). DOI: 10.3390/app14052045.
4. Zelmanski O. B., Petrov S. N., Fomin D. A. (2025) On the Issue of Data Protection in Medical Biotechnical Systems. *Technical Means of Information Protection, Proceedings of the XXIII Belarusian-Russian Scientific and Technical Conference, Minsk, April 8*. Minsk, Belarusian State University of Informatics and Radioelectronics. 168–171 (in Russian).
5. Zelmanski O. B. (2025) Ensuring the Protection of Medical Data in Biotechnical Systems. *Modern Means of Communication, Proceedings of the XXX International Scientific and Technical Conference, Minsk, Oct. 30–31*. Minsk. 80–81 (in Russian).
6. Boiprav O., Zelmanski O., Hasanov M., Makarenya E. (2024) Justification of Encryption Algorithm for Systems Monitoring Personnel Condition of Critical Informatization Objects. *Problems of Information Technology*. 15 (2), 3–8.

Received: 27 February 2026 Accepted: 9 March 2026 Available on the website: 10 July 2026

Вклад авторов

Зельманский О. Б. выполнил исследования, интерпретировал полученные результаты, подготовил рукопись статьи.

Богуш В. А. осуществил постановку задачи для проведения исследования, рассмотрел рукопись статьи.

Authors' contribution

Zelmanski O. carried out the research, interpreted the results obtained, and prepared the manuscript of the article.

Bogush V. formulated the problem for the study and reviewed the manuscript.

Сведения об авторах

Зельманский О. Б., канд. техн. наук, доц., доц. каф. защиты информации, Белорусский государственный университет информатики и радиоэлектроники

Богуш В. А., д-р физ.-мат. наук, проф., ректор Белорусского государственного университета информатики и радиоэлектроники

Адрес для корреспонденции

220013, Республика Беларусь,
Минск, ул. П. Бровки, 6
Белорусский государственный университет
информатики и радиоэлектроники
Тел.: +375 17 293-85-58
E-mail: 7650772@rambler.ru
Зельманский Олег Борисович

Information about the authors

Zelmanski O., Cand. Sci. (Tech.), Associate Professor, Associate Professor of the Department of Information Security, Belarusian State University of Informatics and Radioelectronics

Bogush V., Dr. Sci. (Phys. and Math.), Professor, Rector of the Belarusian State University of Informatics and Radioelectronics

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki St., 6
Belarusian State University
of Informatics and Radioelectronics
Tel.: +375 17 293-85-58
E-mail: 7650772@rambler.ru
Zelmanski Oleg