Автоматизация и моделирование в проектировании и управлении. 2026. № 1 (31). С. 75-80.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2026. № 1 (31). P. 75-80.

Научная статья
Статья в открытом доступе
УДК 004.056
doi: 10.30987/2658-6436-2026-1-75-80

ПРОЕКТИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ОБРАБОТКИ МЕДИЦИНСКИХ ДАННЫХ С УЧЕТОМ АСПЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Наталия Михайловна Кузнецова[1], Татьяна Владимировна Карлова[2]
[1] Московский государственный технологический университет «СТАНКИН», г. Москва, Россия
[2] Институт конструкторско-технологической информатики Российской академии наук, г. Москва, Россия
[1] knm87@mail.ru
[2] karlova-t@yandex.ru

Аннотация. *Целью научной работы является проектирование модели автоматизированной системы обработки медицинских данных с учетом аспектов информационной безопасности. Для достижения поставленной цели в работе сформулированы основные задачи автоматизированной системы обработки медицинских данных, предложен принцип построения автоматизированной системы с учетом аспектов информационной безопасности, приведена архитектура автоматизированной системы обработки медицинских данных, представлена методика анализа уязвимостей автоматизированной системы обработки медицинских данных с учетом базы данных ФСТЭК РФ и MITRE. Новизной работы является предложенная креативная концепция разделения архитектуры автоматизированной системы на уровни представления, обработки и хранения медицинских данных. Также в статье предложены определения субъектов и объектов угроз информационной безопасности. Результатом исследования являются модель автоматизированной системы обработки медицинских данных, а также методика анализа уязвимостей на основе базы данных уязвимостей ФСТЭК РФ и базы данных MITRE.*

Ключевые слова: автоматизация, защита медицинских данных, защита информации, информационная безопасность, защита от целевых атак

Для цитирования: Кузнецова Н.М., Карлова Т.В. Проектирование автоматизированной системы обработки медицинских данных с учетом аспектов информационной безопасности // Автоматизация и моделирование в проектировании и управлении. 2026. №1 (31). С. 75-80. doi: 10.30987/2658-6436-2026-1-75-80.

Original article
Open Access Article

DESIGNING AN AUTOMATED MEDICAL DATA PROCESSING SYSTEM CONSIDERING INFORMATION SECURITY

Natalia M. Kuznetsova[1], Tatyana V. Karlova[2]
[1] Moscow State University of Technology «STANKIN», Moscow, Russia
[2] Institute for Design-Technological Informatics of the Russian Academy of Sciences, Moscow, Russia
[1] knm87@mail.ru
[2] karlova-t@yandex.ru

Abstract. *The aim of this research is to design a model of an automated medical data processing system considering information security. To achieve this goal, the paper formulates the main objectives of an automated medical data processing system; proposes a design principle for an automated system considering information security; presents the architecture of an automated medical data processing system, and presents a methodology for analysing the vulnerabilities of an automated medical data processing system using the FSTEC RF and MITRE databases. The novelty of this work lies in the proposed creative concept of dividing the automated system architecture into the presentation, processing, and storage levels of medical data. The article also proposes definitions of subjects and objects of information security threats. The research results include a model of an automated medical data processing system, as well as a vulnerability analysis methodology based on the FSTEC Russian Federation vulnerability database and the MITRE database.*

Keywords: automation, medical data protection, information security, IT security, protection against targeted attacks

For citation: Kuznetsova N.M., Karlova T.V. Designing an Automated Medical Data Processing System Considering Information Security. Automation and modeling in design and management, 2026, no. 1 (31). pp. 75-80. doi: 10.30987/2658-6436-2026-1-75-80.

Введение

Обеспечение защиты медицинских данных является актуальной задачей. В связи с активным процессом цифровизации [1], медицинские данные переносятся в единые интегрированные информационные системы (ЕИИС), такие как «Госуслуги» [2], «ЕМИАС» [3], «MOS.RU» [4], «Социальный Фонд России» [5] и т.д. Кроме того, медицинские данные могут относиться к врачебной [6], коммерческой [7], государственной тайне [8], что обуславливает необходимость наличия высокого уровня их защиты. Статья посвящена решению поставленных задач защиты данных за счет внедрения автоматизированной системы обработки медицинских данных (АСОМД) с учетом аспектов информационной безопасности.

Основные задачи автоматизированной системы обработки медицинских данных с учетом аспектов информационной безопасности

К основным задачам АСОМД относятся:

– сохранение врачебной тайны;

– сохранение коммерческой тайны;

– сохранение государственной тайны;

– минимизация времени принятия управленческого решения (всеми участниками информационного взаимодействия: врачом, администратором, пациентом);

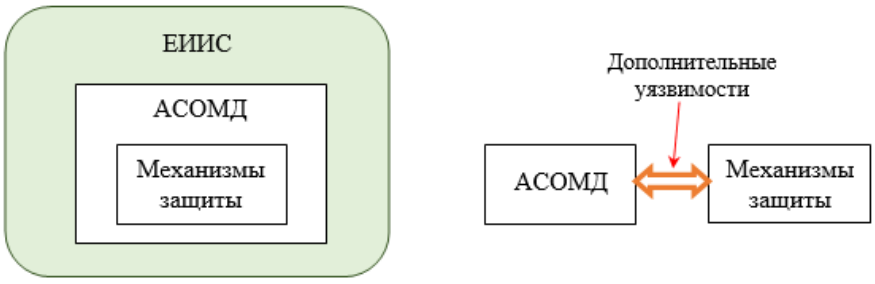
– повышение уровня удобства для всех участников информационного взаимодействия;

– обеспечение безопасности информации (конфиденциальности, доступности, целостности) [9 – 12] при взаимодействии ЕИИС;

– защита от кибератак, в том числе от комплексных целевых кибератак (англ. *APT – Advanced Persistent Threats*), которые на данный момент считаются наиболее опасными [13 – 15].

Проектирование автоматизированной системы обработки медицинских данных с учетом аспектов информационной безопасности

На рис. 1 представлены схемы проектирования АСОМД, как «встроенных» (*а*) и «надстроенных» (*б*) механизмов защиты.



а) *б*)

Рис. 1. Схемы проектирования АСОМД как «встроенных» (*а*) и «надстроенных» (*б*) механизмов защиты
Fig. 1. Design schemes for ASOMD as "built-in" (a) and "overbuilt" (b) protection mechanisms

Согласно рис. 1, в случае, когда механизмы защиты являются «надстроенными», появляются дополнительные уязвимости на «участке» передачи данных между объектом защиты (АСОМД) и субъектом защиты (механизмами защиты).

В связи с этим, уже при проектировании АСОМД необходимо учитывать интеграцию механизмов защиты.

Построение архитектуры автоматизированной системы обработки медицинских данных

Автоматизированная система обработки медицинских данных имеет клиент-серверную архитектуру. На стороне клиента производятся обращения к АСОМД от участников информационного взаимодействия: врачей; пациентов; администраторов.

На стороне сервера производятся обработка и хранение медицинских данных.

На рис. 2 представлена архитектура АСОМД.

Рис. 2. Архитектура АСОМД
Fig. 2. AMDPS Architecture

Согласно рис. 2, архитектура АСОМД имеет три уровня: уровень представления данных; уровень обработки данных; уровень хранения данных и инструментов.

Для обеспечения высокого уровня информационной безопасности всей АСОМД необходимо комплексное обеспечение конфиденциальности, целостности и доступности данных на всех уровнях архитектуры. Однако наибольшего внимания требует обеспечение: конфиденциальности на уровне представления; целостности на уровне обработки данных АСОМД; доступности на уровне хранения данных и инструментов АСОМД.

К уровню представления данных относится модуль визуализации АСОМД.

К уровню обработки данных относятся модули АСОМД: модуль аутентификации; модуль постановки диагноза; модуль статистики; модуль организации приема; модуль энциклопедии заболеваний; модуль оценки качества медицинских услуг; модуль составления расписания.

К уровню хранения данных и инструментов относятся: искусственные нейронные сети (ИНС); экспертные системы (ЭС); база знаний (БЗ) заболеваний; база данных (БД) аутентификаторов; БД пациентов (хранит историю болезни каждого пациента); БД врачей (хранит информацию об образовании и местах работы каждого врача).

Модуль энциклопедии заболеваний обращается к ресурсам: ИНС; ЭС; БЗ заболеваний.

Важно отметить, что обращение производится с наличием обратной связи: модуль энциклопедии заболеваний анализирует данные, полученные от ИНС, ЭС и БЗ заболеваний, а

также преобразует их и возвращает результат анализа ИНС, ЭС и БЗ заболеваний (осуществляет обращение к ИНС, ЭС и БЗ заболеваний как «по чтению», так и «по записи»).

Модуль аутентификации обращается к БД аутентификаторов.

Модуль оценки качества медицинских услуг и модуль составления расписания обращаются к БД пациентов и БД врачей.

Модуль постановки диагноза взаимодействует с модулем энциклопедии заболеваний, производит обращение к БД пациентов и БД врачей для проведения анализа истории болезни пациента.

Модуль статистики взаимодействует с модулем энциклопедии заболеваний и модулем оценки качества медицинских услуг.

Модуль организации приема взаимодействует с модулем оценки качества медицинских услуг и модулем составления расписания.

Для всех перечисленных модулей и инструментов АСОМД необходимо обеспечение высокого уровня информационной безопасности: в том числе для модуля энциклопедии заболеваний, т.к. несмотря на возможность связи с сетью Интернет, необходимо обеспечивать защиту ИНС, ЭС, БЗ заболеваний от внешних угроз потери целостности данных.

Таким образом, в представленной трехуровневой архитектуре АСОМД обеспечивается максимальный для медицинских данных уровень конфиденциальности, что обеспечивает сохранение врачебной, коммерческой и государственной тайны.

Методика анализа уязвимостей автоматизированной системы обработки медицинских данных с учетом базы данных ФСТЭК РФ и базы данных *MITRE*

На рис. 3 представлена схема анализа уязвимостей АСОМД с учетом БД ФСТЭК РФ [16] и БД *MITRE* [17].

Рис. 3. Схема анализа уязвимостей АСОМД с учетом БД ФСТЭК РФ и БД MITRE
Fig. 3. AMDPS vulnerability analysis scheme taking into account the FSTEC RF database and the MITRE database

Согласно рис. 3, к субъектам угроз относятся:

– человек:

а) внутренний нарушитель (пользователь АСОМД);

б) внешний нарушитель;

– организация (конкурент и т.д.).

К объектам угроз относятся: медицинские данные; алгоритмы обработки медицинских данных; модули АСОМД; БД аутентификаторов; БД пациентов; БД врачей; БЗ заболеваний; ИНС; ЭС.

При этом работа с БД угроз ФСТЭК РФ предполагает направление анализа от объекта угрозы к субъекту угрозы, в то время как работа с БД угроз *MITRE* предполагает противоположное направление анализа – от субъекта к объекту угрозы [18].

Приведенная схема анализа уязвимостей АСОМД позволит учесть максимальное

количество угроз информационной безопасности обрабатываемых и хранимых медицинских данных, что в свою очередь позволит предотвратить реализацию множества современных атак, в том числе атак класса *APT*.

Удобство применения автоматизированной системы обработки медицинских данных

Применение представленной трехуровневой архитектуры АСОМД позволит решить задачу предоставления медицинских данных с учетом правил разделения доступа для участников информационного взаимодействия с помощью модуля аутентификации, что в свою очередь позволит:

– минимизировать время принятия управленческого решения;

– повысить уровень удобства.

Выводы

Приведенная в статье модель проектирования автоматизированной системы обработки медицинских данных с учетом аспектов информационной безопасности позволит обеспечить конфиденциальность, доступность и целостность медицинских данных. Также применение представленной в статье методики анализа уязвимостей, учитывающей БД угроз ФСТЭК РФ и БД угроз *MITRE*, позволит своевременно детектировать и предотвратить большинство современных кибератак, включая наиболее опасные атаки класса *APT*. Представленная авторская концепция трехуровневой архитектуры проектируемой автоматизированной системы обработки медицинских данных позволит провести четкое разделение процессов представления, обработки и хранения медицинских данных, что позволит повысить общий уровень информационной безопасности медицинских данных, а также удобство их представления.

Список источников:

1. Распоряжение Правительства РФ от 22 октября 2021 г. № 2998-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления».
2. Портал государственных услуг Российской Федерации [Электронный ресурс]. – режим доступа URL:https://www.gosuslugi.ru (дата обращения: 15.09.2025).
3. Единая медицинская информационно-аналитическая система (ЕМИАС) города Москвы [Электронный ресурс]. – режим доступа URL: https://emias.info (дата обращения: 15.09.2025).
4. Официальный сайт Мэра Москвы «MOS.RU» [Электронный ресурс]. – режим доступа URL: https://mos.ru (дата обращения: 15.09.2025).
5. Социальный Фонд России [Электронный ресурс]. – режим доступа URL: https://sfr.gov.ru (дата обращения: 15.09.2025).
6. Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 23.07.2025) «Об основах охраны здоровья граждан в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2025) Статья 13. Соблюдение врачебной тайны.
7. Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ.
8. Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1.
9. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие для студ. высш. учеб. заведений – 4-е изд., стер. – М.: Издательский центр «Академия», 2008. – 256 с.
10. Милославская Н.Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. – М.: Горячая линия – Телеком, 2021 г. – 432 с.

References:

1. Decree of the Government of the Russian Federation «On Approval of the Strategic Direction in the Field of Digital Transformation of Public Administration»; 2021 Oct 22.
2. Russian Federation Government Services Portal [Internet] [cited 2025 Sep 15]. Available from: https://www.gosuslugi.ru
3. Unified Medical Information and Analytical System (UMIAS) of Moscow [Internet] [cited 2025 Sep 15]. Available from: https://emias.info
4. MOS.RU – Official Website of the Mayor of Moscow [Internet] [cited 2025 Sep 15]. Available from: https://mos.ru
5. Social Fund of Russia [Internet] [cited 2025 Sep 15]. Available from: https://sfr.gov.ru
6. Federal Law No. 323-FZ “On the Fundamentals of Protecting the Health of Citizens in the Russian Federation”. Article 13. Compliance with Medical Confidentiality; 2011 Nov 21.
7. Federal Law No. 98-FZ «On Commercial Secrets»; 2004 Jul 29.
8. Law of the Russian Federation No. 5485-1 «On State Secrets»; 1993 Jul 21.
9. Khorev P.B. Methods and Means of Information Security in Computer Systems. 4th ed. Moscow: Academia; 2008.
10. Miloslavskaya N.G. Scientific Foundations for Constructing Network Security Control Centres in Information and Telecommunication Networks. Moscow: Hotline Telecom; 2021.

11. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Иерархические уровни конфиденциальности информационных ресурсов промышленного предприятия в зависимости от этапов жизненного цикла производства // Автоматизация и моделирование в проектировании и управлении. – 2024. – №4 (26). – С. 59-65.

12. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Проектирование вспомогательной автоматизированной системы принятия управленческих решений на основе анализа уровня информационной безопасности // Автоматизация и моделирование в проектировании и управлении. – 2023. – №3 (21). – С. 13-22.

13. Кузнецова Н.М. Методология защиты от целевых кибератак повышенной сложности в автоматизированных системах промышленного предприятия (монография) // М.: «Янус-К», 2024. – 132 с.

14. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Y. Method of Timely Prevention from Advanced Persistent Threats on the Enterprise Automated Systems // 2022 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS).

15. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Решение задачи автоматизации процессов защиты стратегически важных ресурсов предприятия от комплексных кибер-атак на основе анализа тактик злоумышленников // Вестник Брянского государственного технического университета. – 2020. – № 7(92). –С. 48-53.

16. ФСТЭК России Банк данных угроз безопасности информации [Электронный ресурс]. – режим доступа URL: bdu.fstec.ru/threats (дата обращения: 15.09.2025).

17. MITRE [Электронный ресурс]. – режим доступа URL: attack.mitre.org (дата обращения: 15.09.2025).

18. Кузнецова Н.М., Карлова Т.В. Влияние неудовлетворенного работника предприятия на уровень информационной безопасности // Автоматизация и моделирование в проектировании и управлении. – 2025. – №3 (29). – С. 73-79.

11. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Hierarchical Levels of Confidentiality in Industrial Enterprise' Information Resources Depending on Stages of the Production Cycle. Automation and Modeling in Design and Management. 2024;4(26):59-65.

12. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Designing an Auxiliary Automated Management Decision-Making System Based on Information Security Level Analysis. Automation and Modelling in Design and Management. 2023;3(21):13-22.

13. Kuznetsova N.M. Methodology of Protection Against Targeted Cyber Attacks of Increased Complexity in Automated Systems of an Industrial Enterprise. Moscow: Yanus-K; 2024.

14. Kuznetsova NM, Karlova TV, Bekmeshov AY. Method of Timely Prevention from Advanced Persistent Threats on the Enterprise Automated Systems. In: Proceedings of the 2022 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS); 2022. p. 158-161.

15. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Solution of Protection Automation Problem of Company Strategic Resources Against Complex Cyberattacks Based on Criminal Tactics Analysis. Bulletin of Bryansk State Technical University. 2020;7(92):48-53.

16. FSTEC of Russia. Database of Information Security Threats [Internet] [cited 2025 Sep 15]. Available from: bdu.fstec.ru/threats

17. MITRE [Internet] [cited 2025 Sep 15]. Available from: attack.mitre.org

18. Kuznetsova N.M., Karlova T.V. The Impact of Enterprise's Dissatisfied Employee on the Information Security Level. Automation and Modeling in Design and Management. 2025;3(29);73-79.

Информация об авторах:

Кузнецова Наталия Михайловна
Кандидат технических наук, доцент Московского государственного технологического университета «СТАНКИН».

Карлова Татьяна Владимировна
Доктор социологических наук, кандидат технических наук, профессор Института конструкторско-технологической информатики Российской академии наук.

Information about the authors:

Kuznetsova Natalia Mikhailovna
Candidate of Technical Sciences, Associate Professor of Moscow State University of Technology «STANKIN»

Karlova Tatyana Vladimirovna
Doctor of Sociology, Candidate of Technical Sciences, Professor of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Статья поступила в редакцию 15.10.2025; одобрена после рецензирования 01.11.2025; принята к публикации 14.11.2025.

The article was submitted 15.10.2025; approved after reviewing 01.11.2025; accepted for publication 14.11.2025.

Рецензент – Пугачев А.А., доктор технических наук, доцент, Брянский государственный технический университет.

Reviewer – Pugachev A.A., Doctor of Technical Sciences, Associate Professor, Bryansk State Technical University.