# TECHNICAL SCIENCES

## A RISK-BASED DATA PROTECTION MODEL FOR HEALTHCARE ORGANIZATIONS

**Berkhantsykov D.**
*Postgraduate Student, Irkutsk National ResearchTechnical University, Irkutsk, Russia*
https://orcid.org/0009-0009-9778-7359
**Marinov A.**
*PhD in Economic Sciences, associate Professor at the Cybersecurity Competence Center, Irkutsk National ResearchTechnical University, Irkutsk, Russia*
https://orcid.org/0000-0003-2238-2751

## МОДЕЛЬ ЗАЩИТЫ ДАННЫХ В МЕДИЦИНСКИХ ОРГАНИЗАЦИЯХ НА ОСНОВЕ ТЕОРИИ РИСКА

**Берханцыков Д.И.**
*аспирант ФГБОУ ВО «Иркутский национальный исследовательский технический университет», г. Иркутск, Россия.*
*https://orcid.org/0009-0009-9778-7359*
**Маринов А.А.**
*кандидат экономических наук, доцент центра компетенций по кибербезопасности, ФГБОУ ВО «Иркутский национальный исследовательский технический университет», г. Иркутск, Россия.*
*https://orcid.org/0000-0003-2238-2751*
https://doi.org/10.5281/zenodo.18414011

**Abstract**
This article examines the challenge of ensuring the protection of medical data in healthcare organizations in the context of digitalization and the growth of processed medical information (information processed in medical information systems). It is worth noting that traditional approaches to information security do not fully account for the specifics of medical data and the dynamics of information security threats. The paper proposes a model for assessing and managing medical data security risks that takes into account the characteristics of the data being processed, its processing environment, its intended use, the security mechanisms applied, existing security services, current threats, and potential losses.

**Аннотация**
В статье рассматривается задача обеспечения защиты медицинских данных в организациях здравоохранения в условиях цифровизации и роста объемов обрабатываемой медицинской информации (информация обрабатывается в медицинских информационных системах). Стоит отметить, что традиционные подходы к защите информации не в полной мере учитывают специфику медицинских данных и динамику угроз информационной безопасности. В работе предложена модель оценки и управления рисками защиты медицинских данных, учитывающая характеристики обрабатываемых данных, среду их обработки, цели использования, применяемые механизмы безопасности, существующие услуги безопасности, актуальные угрозы и возможные убытки.

**Keywords:** medical information systems, medical data, information security, healthcare, risk theory, risk assessment, security model, cortege.

**Ключевые слова:** медицинские информационные системы, медицинские данные, защита информации, здравоохранение, теория риска, оценка рисков, модель защиты, кортеж.

### Модель защиты данных в медицинских организациях

Для определения входящих, исходящих и внутренних параметров модели обеспечения защиты данных могу быть применены международные стандарты [1-5] и существующие методики [6], на основе которых и будет разрабатываться модель защиты данных на основе оценки рисков.

Итоговая модель содержит набор параметров представления рисков защиты персональных данных, имеет типовую структуру и реализуется путём выполнения 6 этапов (рисунок 1).

Интегрированное представление параметров риска с отображением на сферу защиты медицинских данных осуществляется в виде кортежа, который можно представить в следующем виде: <A, B, C, D, E, F,G, H, I>, где: A – характеристика данных (идентификация их состава и содержания); B – характеристика среды обработки данных; C – цель обработки данных; D – аудит применяемых механизмов безопасности; E – характеристика существующих функциональных услуг безопасности; F – идентификация угроз безопасности данных при обработке; G – величина возможных убытков от потери данных; H - оценка риска защиты данных; I –

управление риском и достижение необходимого уровня гарантий защиты медицинских данных.

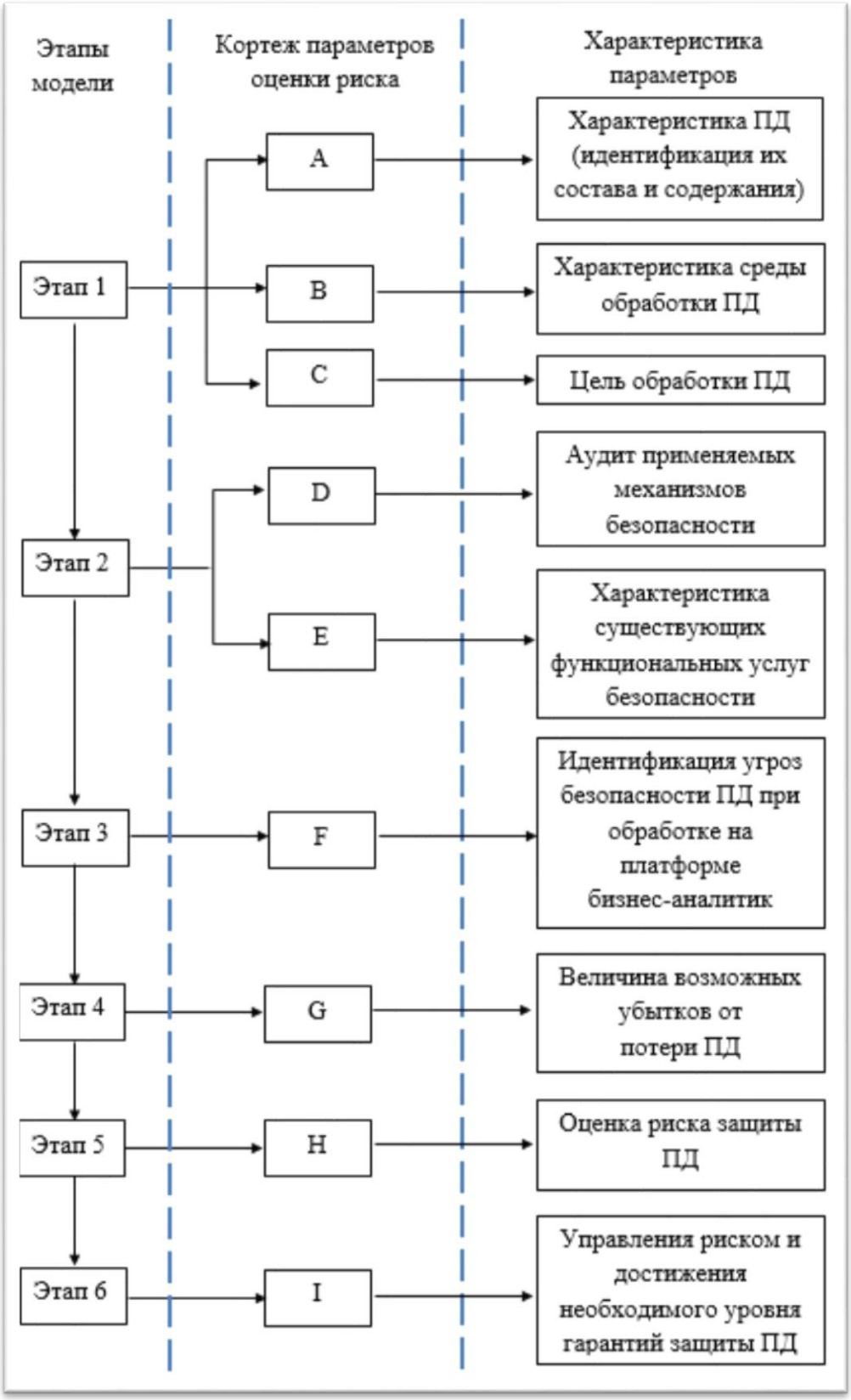


*Рисунок 1 – Модель защиты медицинских данных на основе оценки риска Примечание: составлено авторами*

Первый из компонентов в кортеже – характеристика и идентификация состава и содержания медицинских данных (А). Рассмотрим общеизвестно классификации состава и содержания медицинских данных, которые можно отобразить в виде символьной переменной A$n$, что принимает одно и то же значение конечного множества идентификаторов A$n$ ∈ {A1, A2, A3, A4, ..., A$nn$}, где индекс n –

номер идентификатора состава данных. Состав классификации указанных данных можно представить следующим образом:

а) набор данных содержит сведения о биометрии (A1);

б) набор данных содержит сведения о состоянии здоровья (A2);

в) набор данных не включает в себя сведения о состоянии здоровья или биометрию (A3);

г) данные являются общедоступными (A4);

д) иной вид данных (Ai).

Классификация категорий медицинских данных в зависимости от их состава и их коэффициенты важности $K_{vd}$, составляющей ценности для владельца, приведены в таблице 1.

Под вторым компонентом кортежа – средой обработки медицинских данных (B), следует понимать объекты информатизации, которыми производится обработка данных. Значение коэффициента функциональной сложности $K_{vp}$ приведено в таблице 2.

Таблица 1

**Категории персональных данных и их важность**

| Параметр | Категория персональных данных | Коэффициент важности |
|---|---|---|
| A1 | Биометрические | 0,9 |
| A2 | Специальные | 0,7 |
| A3 | Иные | 0,5 |
| A4 | Общедоступные | 0,3 |
| A5 | Другие данные | [0 ÷ 1] |

Таблица 2

**Коэффициент функциональной сложности в зависимости от средств обработки информации**

| Параметр | Средство обработки информации | Коэффициент функциональной сложности |
|---|---|---|
| B1 | Цифровой рентген аппарат/ магнитно-резонансный томограф | 0,9 |
| B2 | Лабораторные анализаторы | 0,7 |
| B3 | Информационные системы с клиент-серверной системой | 0,5 |
| B4 | Единичные компьютеры | 0,3 |
| B5 | Неавтоматизированная обработка информации | 0,1 |

Третий параметр оценки риска – цели обработки данных (C). Цели обработки данных определяются в зависимости от того, где именно и для какого конечного результата такие данные будут обрабатываться. Данный параметр можно определить согласно законодательству и уставным документам организации. Обобщённые примеры глобальных целей и коэффициента ущерба от нарушения конфиденциальности этих целей приведен в таблице 3.

Таблица 3

**Пример целей обработки медицинских данных**

| Параметр | Средство обработки информации | Коэффициент наступления негативных последствий |
|---|---|---|
| C1 | Данные могу быть использованы для проведения фундаментальных научных исследований | 0,9 |
| C2 | Данные могут быть использованы для обучения искусственного интеллекта | 0,8 |
| C3 | Данные используются только для оказания медицинской помощи | 0,7 |
| C4 | Иные цели обработки данных | [0 ÷ 1] |

Следующим компонентом кортежа является аудит применяемых механизмов безопасности (D). Данный компонент описывается набором элементов Dn ∈ {D1, D2, D3, ..., Di} и определяется проверкой имеющихся организационно-правовых и программно-технических мероприятий и механизмов защиты данных обрабатываемых в информационной инфраструктуре, к которым можно отнести:

а) D1 = «Разработаны и утверждены политики безопасности и проводятся организационные мероприятия»;

б) D2 = «Используются программы средства защиты информации»;

в) D3 = «В организации создано структурное подразделение, занимающееся защитой информации»;

г) D4 = «Используются системы управления информационной безопасностью и аттестованные программно-аппаратные системы защиты информации, реализующие требования все требования законодательства к обработке данных;

д) Di = «Другие механизмы защиты».

После проведения аудита используемых механизмов безопасности, целесообразным является определение имеющихся услуг безопасности (E), как пятого элемента кортежа, определяемого множеством идентификаторов E$n$ ∈ {E1, E2, E3}. С учё-

том того, что в сфере защиты информации риск связан с такими базовыми характеристиками как конфиденциальность (E1), целостность (E2) и доступность (E3), то на данном этапе следует установить существующие критерии защищённости.

Шестым параметром является угрозы безопасности медицинским данным (F). Перечень возможных угроз определяется существующими стандартами [3] и методиками анализа и оценки рисков информационной безопасности [4] и может дополняться самостоятельно. Данный параметр приводится в виде набора элементов известных угроз безопасности данных, а именно: Fn ∈ {F1, F2, F3, F4, F5, F6 ... Fi} и зависит от списка CVE.

По отношению к определённым угроз определяется вероятность их реализации (P) как «низкая» (Pr_1), «средняя» (Pr_2) и «высокая» (Pr_3).

Седьмой параметр кортежа – величина возможных убытков (G), может определяться как количественными, так и качественными показателями. Оценка ущерба проводится по шкалам известных методик [7], характеризующие материальную или моральный ущерб, вред национальной безопасности, ущерб от нарушения прав и свобод человека и тому подобное.

После определения общих параметров, переходим к восьмому параметру кортежа – оценки риска защиты (H). Под риском защиты медицинских данных при их обработке понимается функция вероятности реализации угрозы в виде величины нанесённого ущерба от возможной потери данных при наличии уязвимостей и степени их приемлемости для эксплуатации, определяется по формуле (1):

$$H = P \times G, \quad (1)$$

где P – вероятность реализации угрозы, G – величина возможных убытков.

Завершающим этапом является определение последнего параметра кортежа – управление риском и достижение необходимого уровня защищённости данных (I). На данном этапе с помощью таблицы соответствия полученных значений параметров P и G (таблица 4) определяется необходимый уровень защищённости данных от 1 до 5 баллов для применения рекомендуемой политики безопасности.

Таблица 4

**Оценка уровня защищённости персональных данных**

| Величина возможных рисков (G) | Вероятность реализации угрозы (P) | | | | |
|---|---|---|---|---|---|
| | 0 – 0,1 | 0,1 – 0,3 | 0,3 – 0,6 | 0,6 – 0,8 | 0,8 – 1,0 |
| 0 – 50.000₽ | 1 | 1 | 2 | 3 | 3 |
| 50.000-250.000₽ | 1 | 2 | 2 | 3 | 4 |
| 250.000-500.000₽ | 2 | 2 | 3 | 4 | 4 |
| 500.000-1.000.000₽ | 3 | 2 | 4 | 4 | 5 |
| >1.000.000₽ | 3 | 4 | 4 | 5 | 5 |

Рекомендуемые политики безопасности, сформированных по результатам анализа требований законодательства в сфере обеспечения защиты информации, приведены в таблице 5.

Таблица 5

**Рекомендуемые политики безопасности**

| Уровень | Рекомендуемые меры |
|---|---|
| 1 | Выполнение организационно-правовых мероприятий по защите информации |
| 2 | Создание службы защиты информации и назначение ответственных лиц |
| 3 | Использование технических и/или криптографических СЗИ |
| 4 | Использование программно-аппаратных комплексов защиты информации |
| 5 | Построение комплексной системы защиты информации |

Следует предусмотреть совокупность мероприятий по оценке риска, выбора, реализации и внедрения мероприятий (механизмов) защиты медицинских данных, что должны осуществляться в течение всего их жизненного цикла и быть направлены на достижение приемлемого уровня остаточного риска.

Рассмотрим пример работы представленной модели.

Этап 1. Определяем тип данных коэффициент их важности, в соответствии с таблицей 1. Суммарная величина коэффициентов важности определяется по формулам (2), (4):

$$K_{vd} = \sum_{i=1}^{n} K_{vdi,} n = 1 \dots 5, \quad (2)$$

где $K_{vd}$ – общий коэффициент важности документа.

Допустим, что на платформе бизнес-аналитики осуществляется обработка данных, соответствующих A2 и A3, тогда по формуле (6) получим:

$$K_{vd} = K_{vd2} + K_{vd3} = 0,7 + 0,5 = 2,2. \quad (3)$$

Максимально возможное расчётное значение риска Rmax определяется по формуле:

$$R_{max} = \frac{K_{vd} - K_{vp}}{K_{vd} + K_{vp}}, \quad (4)$$

где Kvp – коэффициент функциональной сложности.

Т.к. в качестве примера рассматривается организация, способная оказывать высокотехнологичную медицинскую помощь, возьмём Kvp равный 0,9. Получим:

$$R_{max} = \frac{K_{vd} - K_{vp}}{K_{vd} + K_{vp}} = \frac{2,2-0,9}{2,2+0,9} = 0,42. \quad (5)$$

Однако, для оценки риска защиты данных, необходимо исследовать используемые механизмы безопасности, существующие угрозы и определить соответствующий им уровень реализации.

Этап 2. На данном этапе проводится анализ функционирующих механизмов безопасности. Каждый из предложенных механизмов безопасности в модели обеспечивает корректировки определённого максимально возможного расчётного значения риска на коэффициент 0,2. Пусть для примера в организации реализовано 3 механизма безопасности (Di, i = 1 ÷ 3), тогда суммарный коэффициент Km = 3 × 0,2 = 0,6.

Этап 3. Предполагается идентификация возможных угроз безопасности данных при их обработке. Перечень этих угроз (F) определяется предложенным методом анализа и оценки рисков данных. Если во всех выбранных угрозах был определён «низкий» уровень угрозы, то Pr_z = 0,3, если установлено хотя бы один «средний» уровень», то Pr_z = 0,6 и хотя бы один «высокий» – Pr_z = 1. Тогда расчётное значение риска с учётом уровня реализации угроз корректируется ($Rz_{cor}$) и будет определяться по формуле:

$$R_{z_{cor}} = P_{r\_z} \times R_{max}\,, \quad (6)$$

где Pr_z – вероятность реализации отдельной угрозы.

Допустим, что определены угрозы с «низкими» и «средними» уровнями, то соответственно $Pr\_z$ = 0,6, тогда:

$$R_{z_{cor}} = 0{,}6 \times 0{,}42 = 0{,}25. \quad (7)$$

Этап 4. Определение величины возможного ущерба от утечки может быть организовано как количественными, так и качественными показателями. Поскольку $Rz_{cor}$ = 0,25, то согласно разработанному методу анализа и оценки рисков по таблице 4 приведены шкалы показателей величин возможных убытков: расчётный интервал риска возможной утечки данных – [0,1 ÷ 0,3]; денежный эквивалент риска возможных убытков – (1000 ÷ 10000$) балльная оценка риска данных – 2 балла.

Этап 5. Проводится оценка рисков защиты данных. На данном этапе определяется коррекция вероятности с учётом механизмов защиты ($Rc$or) по формуле:

$$R_{cor} = \left(Rz_{cor} + (I_{max} - I_{min}) \times (1 - K_m)\right), \quad (8)$$

где I – интервал вероятности риска, Km – коэффициент механизма безопасности.

Для рассматриваемого примера I = 0,25 ∈ [$I_{min}$, $I_{max}$], I ∈ [0,1 ÷ 0,3]:

$$R_{cor} = \left(0{,}25 + (0{,}3 - 0{,}1) \times (1 - 0{,}6)\right) = 0{,}33 \quad (9)$$

Аналогично определяется коррекция для денежного эквивалента:

$$R_g = G_{min} + (G_{max} - G_{min}) \times R_{cor}, \quad (10)$$

$$R_g = 1000 + (10000 - 1000) \times R_{cor} = 5500\$. \quad (11)$$

где G – величина возможных убытков.

Этап 6. Управление риском защиты данных. После проведение анализа и оценки рисков данных можно сформировать конечные выводы о состоянии уровня защищённости. А значит, можно дать рекомендации по повышению этого состояния, а именно по внедрению тех или иных механизмов безопасности, предложенных в таблице 5. Поскольку был определён риск утечки в 2 балла, то согласно таблице 5, необходимо создать службы защиты информации или назначить ответственное лицо.

**Выводы.** В результате проведённого исследования была разработана модель защиты медицинских данных в организации здравоохранения, основанная на теории риска и формализованном представлении параметров безопасности в виде кортежных компонентов. Предложенный подход позволяет комплексно учитывать характеристики персональных данных, особенности среды их обработки, цели использования, действующие механизмы и услуги безопасности, актуальные угрозы, а также возможные последствия реализации рисков.

Разработанная модель обеспечивает поэтапную оценку рисков защиты персональных данных и позволяет количественно и качественно определить уровень возможного ущерба, вероятность реализации угроз и требуемый уровень защищённости информации. Использование кортежного представления параметров повышает наглядность и структурированность процесса анализа рисков, а также облегчает принятие управленческих решений при выборе организационных, технических и программно-аппаратных мер защиты.

**Список литературы:**

1. ISO/IEC 31000 [Электронный ресурс]. – Режим доступа https://www.iso.org. – Заглавие с экрана. – (дата обращения 05.01.2026).
2. ISO/IEC 27000 [Электронный ресурс]. – Режим доступа https://www.iso.org. – Заглавие с экрана. – (дата обращения 05.01.2026).
3. ISO/IEC 27001 [Электронный ресурс]. – Режим доступа https://www.iso.org. – Заглавие с экрана. – (дата обращения 05.01.2026).
4. ISO/IEC 27002 [Электронный ресурс]. – Режим доступа https://www.iso.org. – Заглавие с экрана. – (дата обращения 05.01.2026).
5. ISO/IEC 27003 [Электронный ресурс]. – Режим доступа https://www.iso.org. – Заглавие с экрана. – (дата обращения 05.01.2026).
6. Корченко А.Г. Анализ и оценивание рисков информационной безопасности: монография / Корченко А.Г., Архипов А.Е., Казмирчук С.В. ; – К.: ООО «ЛазуритПолиграф», 2013. – 275 с.
7. CVE Program Mission [Электронный ресурс]. – Режим доступа https://www.cve.org/ – Заглавие с экрана. – (дата обращения 05.01.2026).
8. Мамедова, В. Э. Риск-ориентированный подход как методологическая основа публично-правового регулирования гарантий защиты персонифицированной медицинской информации / В. Э. Мамедова // Юридический аналитический журнал.

– 2024. – Т. 19, № 1. – С. 39-46. – DOI 10.18287/1810-4088-2024-19-1-39-46.

9. Горлов, А. П. Автоматизированная система оценки эффективности программно-аппаратных средств защиты информации / А. П. Горлов, М. Ю. Рытов, Д. А. Лысов // Автоматизация и моделирование в проектировании и управлении. – 2019. – № 2(4). – С. 25-32. – DOI 10.30987/article_5cf2d22c9dcd72.20436206.