



**ОРИГИНАЛ**

**СОГЛАСОВАНО**

Председатель ППО сотрудников

  
О.В. Ермишкина  
«21» декабря 2022 г.

Директор ОГБПОУ «Рязанский медицинский колледж»



**УТВЕРЖДАЮ**

Н.И. Литвинова  
«21» декабря 2022 г.

НОРМАТИВНЫЕ ДОКУМЕНТЫ  
регистрационный номер 443

Концепция о информационной безопасности информационных систем персональных данных ОГБПОУ «Рязанский медицинский колледж»

Рязань, 2022

**ОГЛАВЛЕНИЕ**

1. ОБЩИЕ ПОЛОЖЕНИЯ.....	3
2. ЗАДАЧИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	5
3. ОБЪЕКТЫ ЗАЩИТЫ .....	6
4. КАТЕГОРИИ СОТРУДНИКОВ ОГБПОУ «РЯЗАНСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ», УЧАСТВУЮЩИХ В ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ. ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ ЛИЦ УЧАВВСТВУЮЩИХ В ОБРАБОТКЕ, ХРАНЕНИИ, РАСПРОСТРАНЕНИИ, УНИЧТОЖЕНИИ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	6
5. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ .....	14
6. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ.....	18
7. КОНТРОЛЬ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ .....	21
8. СФЕРЫ ОТВЕТСТВЕННОСТИ ЗА БЕЗОПАСНОСТЬ.....	22
9. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ.....	22
10. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ .....	23
11. МЕХАНИЗМ РЕАЛИЗАЦИИ КОНЦЕПЦИИ.....	23
12. ОЖИДАЕМЫЙ ЭФФЕКТ ОТ РЕАЛИЗАЦИИ КОНЦЕПЦИИ .....	23

Изменение №	Дата создания 31.08.2022 г.	Версия 01
-------------	-----------------------------	-----------

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая «Концепция информационной безопасности информационной системы персональных данных ОГБПОУ «Рязанский медицинский колледж», (далее - Концепция), разработана в соответствии с федеральным законом от 27 июля 2006 г. №152 «О персональных данных», Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" является официальными документами, в которых определена система взглядов на обеспечение информационной безопасности ОГБПОУ «Рязанский медицинский колледж».

Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в ОГБПОУ «Рязанский медицинский колледж», при обработке информации вообще, и персональных данных в частности.

1.2. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (далее - СЗПДн) ОГБПОУ «Рязанский медицинский колледж». Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

1.3. Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты персональных данных (далее – ПДн), с позиции комплексного применения технических и организационных мер и средств защиты.

1.4. Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её владельцам или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

1.5. Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ОГБПОУ «Рязанский медицинский колледж», а также нормативных и методических документов, обеспечивающих её реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

1.6. Концепция является методологической основой для:  
- формирования и проведения единой политики в области обеспечения безопасности ПДн в информационной системы персональных данных (далее – ИСПДн) ОГБПОУ «Рязанский медицинский колледж»;

- принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;

- координации деятельности структурных подразделений ОГБПОУ «Рязанский медицинский колледж» при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;

- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн ОГБПОУ «Рязанский медицинский колледж».

1.7. Область применения Концепции распространяется на ОГБПОУ «Рязанский медицинский колледж», эксплуатирующий технические и программные средства ИСПДн, в которых осуществляется автоматизированная обработка ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.

1.8. Правовой базой для разработки настоящей Концепции служат требования действующих в России законодательных и нормативных документов по обеспечению безопасности ПДн.

1.9. СЗПДн представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

1.10. Безопасность персональных данных достигается путём исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.11. Структура, состав и основные функции СЗПДн определяются исходя из типа угрозы ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

Эти меры призваны обеспечить:

- конфиденциальность информации (защита от несанкционированного ознакомления);

- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

- доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

1.12. Стадии создания СЗПДн:

Изменение №	Дата создания 31.08.2022 г.	Версия 01
-------------	-----------------------------	-----------

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на её создание;
- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

1.13. Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) предусмотренных «Политикой информационной безопасности информационной системы персональных данных ОГБПОУ «Рязанский медицинский колледж» ряда организационно-распорядительных документов.

Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки и типа угроз безопасности ИСПДн ОГБПОУ «Рязанский медицинский колледж».

## **2. ЗАДАЧИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

2.1. Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

2.2. Для достижения основной цели система безопасности ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования автоматизированных систем (далее - АС) и доступ к её ресурсам должны иметь только зарегистрированные установленным порядком пользователи);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:
  - к информации, циркулирующей в ИСПДн;
  - средствам вычислительной техники ИСПДн;
  - аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;
  - регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путём анализа содержимого этих журналов;
  - контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения;

- защиту от несанкционированной модификации (изменения) и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;
- защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;
- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;
- своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

### **3. ОБЪЕКТЫ ЗАЩИТЫ**

3.1. В ОГБПОУ «Рязанский медицинский колледж» производится обработка персональных данных в информационной системе обработки персональных данных (ИСПДн).

3.2. Перечень ИСПДн и определение типа угроз безопасности определяется на основании «Отчета по результатам обследования системы защиты персональных данных информационной системы персональных данных ОГБПОУ «Рязанский медицинский колледж».

3.3. Перечень объектов защиты.

3.3.1. Объектами защиты являются – информация, обрабатываемая в ИСПДн и технические средства её обработки и защиты.

3.3.2. Объекты защиты включают в себя:

- обрабатываемую информацию;
- технологическую информацию;
- программно-технические средства обработки;
- средства защиты ПДн;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

## **4. КАТЕГОРИИ СОТРУДНИКОВ ОГБПОУ «РЯЗАНСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ», УЧАСТВУЮЩИХ В ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ ЛИЦ УЧАСТВУЮЩИЕ В ОБРАБОТКЕ, ХРАНЕНИИ, РАСПРОСТРАНЕНИИ, УНИЧТОЖЕНИИ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Лица работающие в ИСПДн ОГБПОУ «Рязанский медицинский колледж» выделены следующие группы сотрудников, участвующих в обработке и защите персональных данных:

1. Администратор информационной системы персональных данных (далее – Администратор ИСПДн), назначается приказом руководителя учреждения. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

2. Администратор безопасности информационной системы персональных данных (далее – Администратор безопасности ИСПДн) - сотрудник ОГБПОУ «Рязанский медицинский колледж», назначается приказом руководителя Учреждения. Администратор отвечает за поддержание необходимого уровня безопасности объектов защиты. Является ответственным должностным лицом учреждения, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и её ресурсов на этапах эксплуатации и модернизации..

3. Пользователь информационной системы персональных данных (далее Пользователь - ИСПДн), осуществляет обработку персональных данных в информационной системе персональных данных. Пользователем является каждый сотрудник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты..

4. Ответственный за обработку персональных данных (далее - Ответственный за обработку ПДн) - штатный сотрудник определяющий уровень доступа и ответственность лиц участвующих в обработке ПДн. Назначается приказом директора ОГБПОУ «Рязанский медицинский колледж»

Список должностей обрабатывающих персональные данные в ОГБПОУ «Рязанский медицинский колледж»:

№ п/п	Наименование отдела	Наименование должности	Функциональные обязанности	Обрабатываемые персональные данные
1	Отдел кадров	Начальник отдела кадров	Пользователь информационной системы персональных данных	Фамилия, имя, отчество, пол, дата и место рождения, адрес регистрации и фактического проживания, информация о гражданстве, реквизиты документа
2		Специалист по кадрам	Пользователь информационной системы персональных данных	
3	Бухгалтерия	Главный бухгалтер	Пользователь информационной системы персональных данных	удостоверяющего личность, контактная информация (домашний телефон, мобильный

4		Бухгалтер	Пользователь информационной системы персональных данных	телефон, адрес электронной почты), сведения об образовании (образовательное учреждение, время обучения, присвоенная квалификация, реквизиты документов об образовании), сведения о местах работ (город, название организации, должность, сроки работы) и стаже трудовой деятельности, сведения о семейном положении, детях, сведения о постановке на налоговый учёт (ИНН), сведения о регистрации в пенсионном фонде РФ (СНИЛС), сведения об открытых банковских счетах с целью выплаты заработной платы, сведения о выплатах и удержаниях заработной платы, информация о наградах, результатах и достижениях в образовательной и научной деятельности, учёное звание, учёная степень, сведения для воинского учёта, биографические сведения, фотографии, данные медицинских
5	Планово-экономический отдел	Начальник планово-экономического отдела	Пользователь информационной системы персональных данных	
6		Экономист	Пользователь информационной системы персональных данных	
7		Специалист по закупкам	Пользователь информационной системы персональных данных	
8		Хозяйственный отдел	Архивариус	
9	Общежитие	Заведующий общежитием	Пользователь информационной системы персональных данных	
10	Учебно-производительный отдел	Руководитель учебно-производительного отдела	Пользователь информационной системы персональных данных	
11		Методист	Пользователь информационной системы персональных данных	
12		Диспетчер образовательного учреждения	Пользователь информационной системы персональных данных	
13		Заведующий сектором учебной и производственной практикой	Пользователь информационной системы персональных данных	
14		Преподаватели	Пользователь информационной системы персональных данных	
15		Старший методист	Пользователь информационной системы персональных данных	

16	Отдел по воспитательной работе и социально-психологической поддержке студентов	Руководитель отдела по ВР и СППС	Пользователь информационной системы персональных данных	осмотров (на бумажных носителях)
17		Руководитель физического воспитания	Пользователь информационной системы персональных данных	
18		Социальный педагог	Пользователь информационной системы персональных данных	
19		Педагог-психолог	Пользователь информационной системы персональных данных	
20		Методист	Пользователь информационной системы персональных данных	
21		Воспитатель общежития	Пользователь информационной системы персональных данных	
22		Делопроизводитель	Пользователь информационной системы персональных данных	
23		Руководитель отдела учебных отделений	Пользователь информационной системы персональных данных	
24	Отдел учебных отделений	Заведующий учебным отделением	Пользователь информационной системы персональных данных	
25		Делопроизводитель	Пользователь информационной системы персональных данных	
26	Отдел правового контроля и обеспечения системы безопасности	Руководитель отдела правового контроля и обеспечения системы безопасности	Пользователь информационной системы персональных данных	
27		Юрисконсульт	Пользователь информационной системы	

			персональных данных
28		Делопроизводитель	Пользователь информационной системы персональных данных
29		Специалист по охране труда	Пользователь информационной системы персональных данных
30	Отдел информационно-методического обеспечения образовательного процесса	Руководитель отдела информационно-методического обеспечения образовательного процесса	Пользователь информационной системы персональных данных
31		Заведующий сектором контроля качества образовательного процесса	Пользователь информационной системы персональных данных
32		Заведующий сектором инновационного развития образовательного процесса и связям с общественностью	Пользователь информационной системы персональных данных
33		Методист	Пользователь информационной системы персональных данных
34		Главный библиотекарь	Пользователь информационной системы персональных данных
35		Библиограф	Пользователь информационной системы персональных данных
36		Библиотекарь	Пользователь информационной системы персональных данных
37	Отдел информационно-коммуникативного сопровождения	Руководитель отдела информационно-коммуникативного сопровождения	Администратор системы персональных данных

38		Старший системный администратор	Администратор системы персональных данных
39		Системный администратор	Администратор системы персональных данных
40		Специалист по защите информации	Администратор информационной безопасности системы персональных данных
41	Центр дополнительного профессионального образования	Руководитель ЦДПО	Пользователь информационной системы персональных данных
42		Руководитель учебно-методического центра непрерывного медицинского образования ЦДПО	Пользователь информационной системы персональных данных
43		Руководитель учебного центра профессиональных квалификаций ЦДПО	Пользователь информационной системы персональных данных
44		Заведующий учебным отделением ЦДПО	Пользователь информационной системы персональных данных
45		Делопроизводитель ЦДПО	Пользователь информационной системы персональных данных
46		Методист ЦДПО	Пользователь информационной системы персональных данных
47		Касимовский филиал	Руководитель филиала
48	Заведующий учебно-производственным отделом		Пользователь информационной системы персональных данных
49	Специалист по охране труда		Пользователь информационной системы

			персональных данных
50		Инженер-программист	Пользователь информационной системы персональных данных
51		Специалист по кадрам	Пользователь информационной системы персональных данных
52		Бухгалтер	Пользователь информационной системы персональных данных
53		Секретарь	Пользователь информационной системы персональных данных
54		Архивариус	Пользователь информационной системы персональных данных
55		Методист	Пользователь информационной системы персональных данных
56		Социальный педагог	Пользователь информационной системы персональных данных
57		Педагог-психолог	Пользователь информационной системы персональных данных
58		Библиотекарь	Пользователь информационной системы персональных данных
59		Воспитатель	Пользователь информационной системы персональных данных
60		Педагог-организатор	Пользователь информационной системы персональных данных
61		Преподаватели	Пользователь информационной системы персональных данных
62	Скопинский	Руководитель	Пользователь

	филиал	филиала	информационной системы персональных данных
63		Заведующий учебно-производственным отделом	Пользователь информационной системы персональных данных
64		Специалист по охране труда	Пользователь информационной системы персональных данных
65		Системный администратор	Пользователь информационной системы персональных данных
66		Инспектор по кадрам	Пользователь информационной системы персональных данных
67		Библиотекарь	Пользователь информационной системы персональных данных
68		Секретарь	Пользователь информационной системы персональных данных
69		Архивариус	Пользователь информационной системы персональных данных
70		Методист	Пользователь информационной системы персональных данных
71		Социальный педагог	Пользователь информационной системы персональных данных
72		Делопроизводитель	Пользователь информационной системы персональных данных
73		Педагог-психолог	Пользователь информационной системы персональных данных
74		Преподаватель	Пользователь информационной системы

			персональных данных	
75	Приёмная комиссия	Председатель приёмной комиссии (Директор)	Пользователь информационной системы персональных данных	
76		Ответственный секретарь	Пользователь информационной системы персональных данных	
77		Технический секретарь	Пользователь информационной системы персональных данных	
78		Системный администратор	Администратор системы персональных данных	

## 5. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. Построение системы обеспечения безопасности ПДн ИСПДн ОГБПОУ «Рязанский медицинский колледж» и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- Законность.
- Системность.
- Комплексность.
- Непрерывность.
- Своевременность.
- Преемственность и непрерывность совершенствования.
- Персональная ответственность.
- Минимизация полномочий.
- Взаимодействие и сотрудничество.
- Гибкость системы защиты.
- Открытость алгоритмов и механизмов защиты.
- Простота применения средств защиты.
- Научная обоснованность и техническая реализуемость.
- Специализация и профессионализм.
- Обязательность контроля.

В понятийном аппарате с пункта 5.1.1-5.1.15 указаны основные принципы построения системы обеспечения безопасности ПДн.

### 5.1.1. Законность

Предполагает осуществление защитных мероприятий и разработку СЗПДн ОГБПОУ «Рязанский медицинский колледж» в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утверждённых органами государственной власти и управления в пределах их компетенции.

Изменение №	Дата создания 31.08.2022 г.	Версия 01
-------------	-----------------------------	-----------

Пользователи ИСПДн, Администратор ИСПДн, Администратор безопасности ИСПДн, Ответственный за обработку ПДн должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности защиты ПДн.

#### 5.1.2. Системность

Системный подход к построению СЗПДн ОГБПОУ «Рязанский медицинский колледж» предполагает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн ОГБПОУ «Рязанский медицинский колледж».

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированного доступа к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа (далее - НСД) к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

#### 5.1.3. Комплексность

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких не взаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии виртуальных сетей (далее - VPN). Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

#### 5.1.4. Непрерывность защиты персональных данных

Защита ПДн – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имён, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления её функционирования.

#### 5.1.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и её системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счёте, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищённые системы.

#### 5.1.6. Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и её системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

#### 5.1.7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведён к минимуму.

#### 5.1.8. Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к ПДн должен предоставляться только в том случае и объёме, если это необходимо сотруднику для выполнения его должностных обязанностей.

#### 5.1.9. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн ОГБПОУ «Рязанский медицинский колледж», для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

#### 5.1.10. Гибкость системы защиты персональных данных

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определённой гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса её нормального функционирования.

#### 5.1.11. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счёт секретности структурной организации и алгоритмов функционирования её подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления (даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

#### 5.1.12. Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имён и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и Администраторов ИСПДн.

#### 5.1.13. Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

#### 5.1.14. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты

Изменение №	Дата создания 31.08.2022 г.	Версия 01
-------------	-----------------------------	-----------

должна осуществляться профессионально подготовленными специалистами ОГБПОУ «Рязанский медицинский колледж».

#### 5.1.15. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

## 6. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИЩЕННОСТИ

6.1. Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

- Законодательные (правовые);
- Морально-этические;
- Организационные (административные);
- Физические;
- Технические (аппаратные и программные).

В понятийном аппарате с пункта 6.1.1-6.1.5 указаны меры обеспечения безопасности ИСПДн.

Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных.

#### 6.1.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

#### 6.1.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ПК в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утверждённые нормативные акты, однако, их несоблюдение ведёт обычно к падению авторитета, престижа человека, группы лиц или организации.

Изменение №	Дата создания 31.08.2022 г.	Версия 01
-------------	-----------------------------	-----------

Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

### 6.1.3. Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать «Политику информационной безопасности информационной системы персональных данных ОГБПОУ «Рязанский медицинский колледж» (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация «Политики информационной безопасности информационной системы персональных данных ОГБПОУ «Рязанский медицинский колледж» состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в «Политике информационной безопасности информационной системы персональных данных ОГБПОУ «Рязанский медицинский колледж».

Примером таких решений могут быть:

- принятие решения о формировании мер обеспечения безопасности ПДн, определение ответственных за её реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;
- принятие решений по вопросам реализации мер безопасности, которые рассматриваются на уровне ОГБПОУ «Рязанский медицинский колледж» в целом;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн.

На организационном уровне определяются процедуры и правила достижения целей и решения задач «Политики информационной безопасности

Изменение №	Дата создания 31.08.2022 г.	Версия 01
-------------	-----------------------------	-----------

информационной систем персональных данных ОГБПОУ «Рязанский медицинский колледж». Эти правила определяют:

- какова область применения политики безопасности ПДн;
- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а так же их установить ответственность;
- кто имеет права доступа к ПДн;
- какими мерами и средствами обеспечивается защита ПДн;
- какими мерами и средствами обеспечивается контроль за соблюдением введённого режима безопасности.

Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;
- определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;
- организовать меры противодействия несанкционированного доступа пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

#### 6.1.4. Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путём установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключаящими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

#### 6.1.5. Аппаратно-программные средства защиты персональных данных

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн ОГБПОУ «Рязанский медицинский колледж»;
- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты ПДн.

Успешное применение технических средств защиты на основании принципов предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИСПДн;
- каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства ОГБПОУ «Рязанский медицинский колледж»;
- сетевое оборудование (коммутаторы, маршрутизаторы и т.п.) располагается с учётом ограниченного доступа к данному оборудованию, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).
- специалистами ОГБПОУ «Рязанский медицинский колледж» осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

## **7. КОНТРОЛЬ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОГБПОУ «РЯЗАНСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ»**

Контроль эффективности СЗПДн должен осуществляться на периодической основе не реже 1 раза в 3 года в соответствии с п.17 постановления правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может осуществляться Администратором безопасности как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

Контроль может проводиться как Администраторами безопасности ИСПДн (оперативный и текущий контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

## **8. СФЕРЫ ОТВЕТСТВЕННОСТИ ЗА БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ**

8.1. Общий контроль за соблюдением и обеспечением безопасности персональных данных осуществляет директор ОГБПОУ «Рязанский медицинский колледж».

8.2. Ответственным за разработку мер по обеспечению безопасности персональных данных является Администратор безопасности ИСПДн, в сферу ответственности которого входят следующие направления обеспечения безопасности ПДн:

- планирование и реализация мер по обеспечению безопасности ПДн;
- анализ угроз безопасности ПДн;
- контроль защищенности информационно-технической инфраструктуры ОГБПОУ «Рязанский медицинский колледж» от угроз информационной безопасности;
- обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;
- предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

## **9. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ**

Под нарушителем в инфраструктуре ОГБПОУ «Рязанский медицинский колледж» понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты.

Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушители делятся на две группы:

- внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
- внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Классификация нарушителей безопасности персональных данных каждой ИСПДн представлена в «Модели угроз безопасности персональных данных ОГБПОУ «Рязанский медицинский колледж».

## 10. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ

Для ИСПДн ОГБПОУ «Рязанский медицинский колледж» выделяются следующие основные категории угроз безопасности персональных данных:

- Угрозы от утечки по техническим каналам.
- Угрозы несанкционированного доступа к информации:
- Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путём физического доступа к элементам ИСПДн.
- Угрозы хищения, несанкционированной модификации или блокирования информации за счёт несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).
- Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за не надёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.
- Угрозы преднамеренных действий внутренних нарушителей.
- Угрозы несанкционированного доступа по каналам связи.

Описание угроз безопасности персональных данных каждой ИСПДн, а также вероятность их реализации, опасность и актуальность представлены в «Модели угроз безопасности персональных данных ОГБПОУ «Рязанский медицинский колледж».

## 11. МЕХАНИЗМ РЕАЛИЗАЦИИ КОНЦЕПЦИИ

Реализация Концепции должна осуществляться на основе перспективных программ и планов, колледжа по защите ПДн которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;
- постановлений Правительства Российской Федерации;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России;
- потребностей ИСПДн в средствах обеспечения безопасности информации.

## 12. ОЖИДАЕМЫЙ ЭФФЕКТ ОТ РЕАЛИЗАЦИИ КОНЦЕПЦИИ

Реализация Концепции безопасности ПДн в ИСПДн позволит:

- оценить состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить

Изменение №	Дата создания 31.08.2022 г.	Версия 01
-------------	-----------------------------	-----------

приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

- разработать распорядительные и нормативно-методические документы применительно к ИСПДн;
- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;
- обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИСПДн и создаст условия для её дальнейшего совершенствования.

#### РАЗРАБОТАЛ:

Специалист по защите информации

#### СОГЛАСОВАНО:

Заместитель директора

«26» декабря 2022 г.

Руководитель отдела информационно-коммуникативного сопровождения

«21» декабря 2022 г.

Начальник отдела кадров

«21» декабря 2022 г.

Главный бухгалтер

«21» декабря 2022 г.

Начальник планово-экономического отдела

«21» декабря 2022 г.

Руководитель учебно-производственного отдела

«21» декабря 2022 г.

Руководитель отдела по воспитательной работе и социально-психологической поддержке студентов

«21» декабря 2022 г.

Руководитель отдела учебных отделений

«21» декабря 2022 г.

Руководитель отдела информационно-методического обеспечения образовательного процесса

«21» декабря 2022 г.

Руководитель центра дополнительного профессионального образования

«21» декабря 2022 г.

Руководитель отдела правового контроля и обеспечения системы безопасности

«21» декабря 2022 г.

Д.М. Костин

Т.П. Журавлёва

С.Е. Поликашин

Е.И. Калинина

Н.В. Писаревская

И.А. Донскова

Е.М. Фатина

С.Е. Нистратова

А.В. Ермакова

С.Г. Секкай

Г.В. Римская

Ю.А. Комаров

<b>Изменение №</b>	<b>Дата создания 31.08.2022 г.</b>	<b>Версия 01</b>
--------------------	------------------------------------	------------------