



ОРИГИНАЛ

СОГЛАСОВАНО

Председатель ППО сотрудников


О.В. Ермишкина
«21» декабря 2022 г.

УТВЕРЖДАЮ

Директор ОГБПОУ «Рязанский медицинский колледж»



Н.И. Литвинова

«21» декабря 2022 г.

НОРМАТИВНЫЕ ДОКУМЕНТЫ
регистрационный номер 442

Политика информационной безопасности

Рязань, 2022

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ	3
2. СУБЪЕКТЫ ПРАВООТНОШЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЕМ ЕЁ БЕЗОПАСНОСТИ	4
3. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ИХ ИСТОЧНИКИ.....	6
4. ОЦЕНКА РИСКОВ СЕТЕВОЙ БЕЗОПАСНОСТИ.....	6
5. МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	7
6. СИСТЕМНЫЙ АУДИТ.....	8
7. АНТИВИРУСНЫЙ КОНТРОЛЬ	9
8. АНАЛИЗ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	11
9. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ	12
10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	15

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

1. Общие положения

1.1. Настоящая Политика информационной безопасности разработана в соответствии с положениями:

- Конституции Российской Федерации;
- Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федерального закона от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне";
- Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных";
- Национального стандарта РФ ГОСТ Р ИСО/МЭК 27033-1-2011 "Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции", утверждённого приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. N 683-ст);
- общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности.

1.2. Политика информационной безопасности представляет собой совокупность положений, правил, требований и принятых решений, определяющих порядок доступа к информационным ресурсам ОГБПОУ «Рязанский медицинский колледж», основные направления и способы защиты информации ОГБПОУ «Рязанский медицинский колледж».

1.3. Основными целями Политики информационной безопасности являются:

- обеспечение управления и поддержки руководством ОГБПОУ «Рязанский медицинский колледж» информационной безопасности в соответствии с требованиями законов о персональных данных;
- защита субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба;
- обеспечение целостности и конфиденциальности информации;
- обеспечение соблюдения требований законодательства, руководящих и нормативных документов и общей политики безопасности.

1.4. Основными задачами Политики информационной безопасности являются:

- доступность обрабатываемой информации;
- защита информации от несанкционированного доступа к ней посторонних лиц, от утечки по техническим каналам, от специальных воздействий на информацию в целях её блокирования, уничтожения, искажения;
- контроль целостности и аутентичности (подтверждение авторства) информации, хранимой, обрабатываемой и передаваемой по каналам связи ОГБПОУ «Рязанский медицинский колледж»;
- обеспечения конфиденциальности определённой части информации, хранимой, обрабатываемой и передаваемой по каналам связи ОГБПОУ «Рязанский медицинский колледж»;
- оценка рисков информационной безопасности.

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

1.5. Защите подлежит вся принимаемая, передаваемая, обрабатываемая и хранимая информация содержащая:

- сведения, составляющие служебную и коммерческую тайну, доступ к которым ограничен, в соответствии с положениями предоставленными Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и Федеральным законом от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне";

- персональные данные, доступ к которым ограничен в соответствии с положениями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных";

- открытые сведения, в части обеспечения доступности и целостности информации.

1.6. Основными способами защиты информационных ресурсов ОГБПОУ «Рязанский медицинский колледж» являются:

- оценка рисков сетевой безопасности;
- мониторинг информационной безопасности;
- системный аудит;
- антивирусный контроль;
- анализ инцидентов.

1.7. Основными средствами защиты информационных ресурсов ОГБПОУ «Рязанский медицинский колледж» являются:

- криптографические средства: Secret Net Studio, ViPNet 4;
- средства обеспечения и контроля целостности программных и информационных ресурсов: Secret Net Studio, Kaspersky Endpoint Security;
- средства разграничения доступа к ресурсам автоматизированной системы;
- средства идентификации и аутентификации пользователей;
- технические средства защиты.

1.8. Политика информационной безопасности утверждается директором и доводится до сведения всех работников ОГБПОУ «Рязанский медицинский колледж», а также до филиалов организации путём размещения на сайте колледжа.

1.9. Основные положения и требования настоящей Политики информационной безопасности распространяются на все структурные подразделения ОГБПОУ «Рязанский медицинский колледж».

2. Субъекты правоотношений, связанных с использованием информации и обеспечением её безопасности

2.1. К субъектам правоотношений, связанных с использованием информационных ресурсов ОГБПОУ «Рязанский медицинский колледж» и обеспечением их безопасности (далее - субъекты правоотношений) относятся:

- работники ОГБПОУ «Рязанский медицинский колледж» - пользователи информационной системы в соответствии с возложенными на них трудовыми и функциональными обязанностями;

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

- подразделения ОГБПОУ «Рязанский медицинский колледж», обеспечивающие эксплуатацию информационных ресурсов;

- иные пользователи (физические и юридические лица), информация о которых обрабатывается, накапливается и хранится в ОГБПОУ «Рязанский медицинский колледж».

2.2. Доступ к информационным ресурсам ОГБПОУ «Рязанский медицинский колледж» имеют работники допущенные к обработке, хранению и распространению персональных данных приказом директора ОГБПОУ «Рязанский медицинский колледж».

Уровень доступа к информационным ресурсам определяется для каждого работника индивидуально с соблюдением следующих требований:

- каждый работник имеет доступ только к той информации, которая необходима ему для выполнения должностных обязанностей;

- конфиденциальная и открытая информация размещается на разных серверах;

- непосредственный руководитель работника имеет право на просмотр информации, используемой работником;

В процессе использования информационных ресурсов работники обязаны соблюдать следующие требования:

- Не разглашать персональные данные других работников ОГБПОУ «Рязанский медицинский колледж» и третьих лиц, ставшие известными при исполнении должностных обязанностей.

- Не передавать обрабатываемые персональные данные другим работникам ОГБПОУ «Рязанский медицинский колледж», не допущенным к обработке персональные данные .

- Не размещать в открытом доступе (корпоративные адресные книги, справочники, портал, сайты в сети Интернет и т.п.) персональные данные работников ОГБПОУ «Рязанский медицинский колледж» и третьих лиц, за исключением данных, признанных работниками общедоступными (Ф.И.О., должность, рабочий телефоны и e-mail, фотография, число, месяц и год рождения).

Все работники должны быть ознакомлены персонально под роспись с организационно-распорядительными документами по защите информации, должны знать и неукоснительно выполнять технологические инструкции и общие обязанности по обеспечению безопасности информации.

Каждый работник при приёме на работу должен подписывать обязательство о соблюдении требований по сохранению конфиденциальной информации и ответственности за их нарушение, а также о выполнении правил работы с информацией.

Все работники, допущенные к работе с информацией в ОГБПОУ «Рязанский медицинский колледж» несут персональную ответственность за нарушение правил её использования, передачи, хранения, а также требований по сохранению конфиденциальной информации.

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

Для пользователей разрабатываются инструкции о порядке использования информационных ресурсов, включающие требования по обеспечению безопасности информации.

До предоставления доступа к информационным ресурсам пользователи должны быть ознакомлены с перечнем конфиденциальной информации и своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки такой информации.

Пользователи, допущенные к работе с информационными ресурсами, несут ответственность за нарушение правил её использования, передачи, хранения, а также требований по сохранению конфиденциальной информации.

3. Угрозы безопасности информации и их источники

3.1. Основные угрозы безопасности информации, с которыми сталкивается ОГБПОУ «Рязанский медицинский колледж», могут быть связаны с проблемами:

- несанкционированного доступа к информации,
- несанкционированной передачи информации,
- отказа в обслуживании и недоступности информации.

3.1.1. Указанные угрозы могут быть связаны с утратой:

- конфиденциальности информации (в сетях и системах, соединённых с сетями);
- целостности информации (в сетях и системах, соединённых с сетями);
- доступности информации (и систем, соединённых с сетями);
- подлинности информации;
- достоверности информации (в сетях и системах, соединённых с сетями);
- способности контролировать несанкционированное использование и эксплуатацию сетевых ресурсов, включая осуществление контроля в контексте политики безопасности организации и выполнение обязательств в отношении законодательства и предписаний;
- способности контролировать злоупотребление санкционированным доступом.

3.2. Основными источниками угроз безопасности информации являются:

- хищение (копирование) информации;
- уничтожение информации;
- модификация (искажение) информации;
- нарушение доступности (блокирование) информации;
- отрицание подлинности информации;
- навязывание ложной информации.

4. Оценка рисков сетевой безопасности

4.1. Для идентификации и подтверждения технических мер и средств контроля и управления безопасностью информации в ОГБПОУ «Рязанский медицинский колледж» проводится оценка риска сетевой безопасности в соответствии с

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

методикой оценки угроз безопасности информации утверждённой ФСТЭК России от 05.02.2021 г.

Для этого должны быть выполнены следующие основные действия:

- определение степени значимости информации, выраженной с точки зрения потенциального неблагоприятного воздействия на основную деятельность ОГБПОУ «Рязанский медицинский колледж» в случае возникновения нежелательных инцидентов;
- идентификация и оценка вероятности или уровней угроз, направленных против информации;
- идентификация и оценка степени серьёзности или уровня уязвимостей (слабых мест), которые могли бы быть использованы идентифицированными угрозами;
- оценка величины рисков, основывающихся на определённых последствиях потенциального неблагоприятного воздействия на операции деятельности ОГБПОУ «Рязанский медицинский колледж» и уровнях угроз и уязвимостей;
- идентификация аспектов специализированной архитектуры/проекта безопасности и оправданных потенциальных областей действия мер и средств контроля и управления безопасностью, необходимых для обеспечения того, чтобы оценённые риски оставались в допустимых пределах.

5. Мониторинг информационной безопасности

5.1. Мониторинг работоспособности аппаратных компонентов автоматизированных систем, обрабатывающих информацию, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования.

Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

5.2. Мониторинг парольной защиты и контроль надёжности пользовательских паролей предусматривают:

- установление сроков действия паролей;
- периодическую, не реже 90 дней, проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

5.3. Мониторинг целостности программного обеспечения включает следующие действия:

- проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
- обнаружение дубликатов идентификаторов пользователей;
- восстановление системных файлов администраторами систем с резервных копий.

5.4. Мониторинг попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств и предусматривает:

- фиксацию неудачных попыток входа в систему в системном журнале;
- протоколирование работы сетевых сервисов;
- выявление фактов сканирования определённого диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих её уязвимости.

5.5. Мониторинг производительности автоматизированных систем, обрабатывающих информацию, производится по обращениям пользователей в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлёкших существенное уменьшение производительности систем.

6. Системный аудит

6.1. Системный аудит производится структурным подразделением колледжа, либо сторонними независимыми экспертами.

6.2. Системный аудит включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

6.3. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, уровню безопасности, удовлетворяющему требованиям политики безопасности.

6.4. Обзоры безопасности должны включать:

- отчёты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имён и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;

- проверку содержимого файлов конфигурации на соответствие списку для проверки;

- обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);

- проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;

- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

6.5. Активное тестирование надёжности механизмов контроля доступа производится путём осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

6.6. Пассивное тестирование механизмов контроля доступа осуществляется путём анализа конфигурационных файлов системы.

Информация об известных уязвимостях извлекается из документации и внешних источников, затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то с целью нейтрализации уязвимостей необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

6.7. Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным документированием изменений в соответствующем журнале, уведомлением каждого сотрудника, которого касается изменение, разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесённое в неё изменение вывело её из строя.

7. Антивирусный контроль

7.1. Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
- утилиты для обнаружения и анализа новых вирусов.

7.2. К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

7.3. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

7.4. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретённых средств защиты.

7.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

7.6. Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

7.7. Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций

занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных установленных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путём перевода рабочей станции в соответствующий автоматический режим функционирования в запёртом помещении.

7.8. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съёмных носителей (магнитных дисков, оптических дисков, флеш-накопителей и т.п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после её загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

7.9. Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

7.10. На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

- осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;
- проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

7.11. На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

7.12. На всех рабочих станциях и серверах необходимо организовать регулярное обновление антивирусных баз.

7.13. Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которые распространяются вирусы.

7.14. При обнаружении заражённых вирусом файлов администратор системы должен выполнить следующие действия:

- отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и

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

т. д.) заражённого файла, типа заражённого файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

8. Анализ инцидентов информационной безопасности

8.1. Если администратор информационной системы, обрабатывающей информацию, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

- факт попытки несанкционированного доступа (далее НСД);
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- когда происходила попытка НСД;
- как и при каких обстоятельствах была предпринята попытка НСД;
- точку входа нарушителя в систему;
- была ли попытка НСД успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки НСД.

8.2. Для выявления попытки НСД необходимо:

- установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях;
- выявить подозрительную активность пользователей;
- проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго;
- проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

8.3. При анализе системных журналов администратору необходимо произвести следующие действия:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
- проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя;
- выявить наличие неудачных попыток входа в систему.

8.4. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки изменения таблиц маршрутизации и адресных таблиц;
- проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

8.5. Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

- составить базовую схему того, как обычно выглядит система;
- провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- проверить целостность системных программ;
- проверить систему аутентификации и авторизации.

8.6. В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

9. Особенности обеспечения информационной безопасности персональных данных

9.1. В ОГБПОУ «Рязанский медицинский колледж» выделяются следующие категории персональных данных:

- специальные категории персональных данных;
- общедоступные или обезличенные персональные данные;
- персональные данные, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным.

9.2. К субъектам персональных данных относятся: абитуриенты, студенты, сотрудники, слушатели отделений повышения квалификации работников со средним медицинским и фармацевтическим образованием, соискатели, родственники работников, уволенные работники, контрагенты, представители контрагентов, посетители сайта, законные представители студентов.

9.3. Все персональные сведения о субъекте персональных данных ОГБПОУ «Рязанский медицинский колледж» может получить только от него самого.

9.4. Начальник отдела кадров обязан сообщить субъекту персональных данных о целях, способах, источниках получения персональных данных, возможности установления запретов и ограничений на распространение, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работника дать письменное согласие на их получение.

9.5. Персональные данные субъекта персональных данных являются конфиденциальной информацией и не могут быть использованы ОГБПОУ «Рязанский медицинский колледж» или любым иным лицом в личных целях.

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

9.6. При определении объема и содержания персональных данных, ОГБПОУ «Рязанский медицинский колледж» руководствуется Конституцией РФ, федеральными законами, иными нормативно-правовыми актами.

9.7. ОГБПОУ «Рязанский медицинский колледж» обязано принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей по защите персональных данных, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.

ОГБПОУ «Рязанский медицинский колледж» самостоятельно определяет состав и перечень мер, необходимых для обеспечения защиты персональных данных. Осуществляется путём:

- 1) назначение ответственного за организацию обработки персональных данных;
- 2) издание документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- 3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- 4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
- 5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;
- 6) ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

9.8. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных, уполномоченное лицо по обработке персональных данных осуществляет блокирование неправомерно обрабатываемых персональных данных с момента такого обращения на период проверки.

9.9. В случае выявления неточных персональных данных при обращении субъекта персональных данных, уполномоченное лицо по обработке персональных данных осуществляет блокирование персональных данных с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

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

9.10. В случае подтверждения факта неточности персональных данных уполномоченное лицо по обработке персональных данных на основании сведений, представленных субъектом персональных данных, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

9.11. В случае выявления неправомерной обработки персональных данных, осуществляемой в ОГБПОУ «Рязанский медицинский колледж», уполномоченное лицо по обработке персональных данных в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных.

9.12. В случае если обеспечить правомерность обработки персональных данных невозможно, уполномоченное лицо по обработке персональных данных в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

9.13. Об устранении допущенных нарушений или об уничтожении персональных данных уполномоченное лицо по обработке персональных данных уведомляет субъекта персональных данных.

9.14. В случае достижения цели обработки персональных данных уполномоченное лицо по обработке персональных данных прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

9.15. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных уполномоченное лицо по обработке персональных данных прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

9.16. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 9.13-9.15 настоящей Политики, уполномоченное лицо по обработке персональных данных осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

9.17. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном Федеральными законами.

9.18. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации.

Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесённых субъектом персональных данных убытков.

10. Заключительные положения

10.1. Настоящая Политика информационной безопасности вступает в силу с момента её утверждения.

10.2. Руководитель ОГБПОУ «Рязанский медицинский колледж» обеспечивает неограниченный доступ к настоящему документу.

10.3. Настоящая Политика информационной безопасности доводится до сведения всех работников персонально под роспись.

РАЗРАБОТАЛ:

Специалист по защите информации

СОГЛАСОВАНО:

Заместитель директора

«21» 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.

И.О. 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.



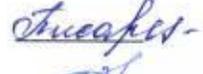
Д.М. Костин



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