МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ ЧЕЧЕНСКОЙ РЕСПУБЛИКИ.
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«РЕСПУБЛИКАНСКИЙ КЛИНИЧЕСКИЙ ЦЕНТР ИНФЕКЦИОННЫХ БОЛЕЗНЕЙ, ПРОФИЛАКТИКИ И БОРЬБЫ СО СПИД»

ПРИКАЗ №137-17

«01» 10 2026 г. г. Грозный

«Об утверждении Политики использования технологий искусственного интеллекта в ГБУ «РКЦИБ ПБ СПИД»

В соответствии с Федеральным законом от 27.07.2006 года № 142-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 года № 152-ФЗ «О персональных данных», распоряжением Правительства Чеченской Республики от 20.08.2021года № 297-р «Об утверждении Стратегии в области цифровой трансформации отраслей экономики, социальной сферы и государственного управления Чеченской Республики», в целях обеспечения информационной безопасности и минимизации правовых, технических и репутационных рисков при внедрении систем искусственного интеллекта в Министерстве здравоохранения Чеченской Республики и медицинских организациях государственной системы здравоохранения Чеченской Республики,

ПРИКАЗЫВАЮ:

1.Утвердить:

1.1. Политику использования технологий искусственного интеллекта в ГБУ «РКЦИБ ПБ СПИД» согласно приложению №1.

1.2. План мероприятий («дорожную карту») по внедрению Политики согласно приложению №2.

2. Начальнику отдела кадров Макашовой М.З. в течении 10 рабочих дней со дня издания настоящего приказа обеспечить ознакомление всех сотрудников ГБУ «РКЦИБ ПБ СПИД» с Политикой под личную подпись.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач Х.Х. Муртазалиев

Приложение № 2 к приказу

от «01» 10 2026 года №___

План мероприятий («дорожная карта»)
по внедрению Политики использования технологий искусственного интеллекта в Министерстве здравоохранения Чеченской Республики и подведомственных медицинских организациях

№ п/п	Наименование мероприятия	Срок реализации	Ответственный исполнитель	Ожидаемый результат / форма отчетности
1	Проведение комплексного аудита существующих практик и сценариев фактического применения систем искусственного интеллекта в медицинских организациях для оценки масштабов и выявления зон рисков нарушений информационной безопасности	В течение 30 рабочих дней со дня издания приказа	Руководители медицинских организаций, профильные структурные подразделения Министерства здравоохранения Чеченской Республики	Аналитическая справка о результатах аудита, направленная в Министерство здравоохранения Чеченской Республики
2	Организация образовательных мероприятий и регулярных инструктажей сотрудников Министерства и медицинских организаций по правилам цифровой гигиены и разъяснению недопустимости ввода персональных данных пациентов и врачебной тайны во внешние системы искусственного интеллекта	На постоянной основе (первичный инструктаж – в течение 15 рабочих дней)	Лицо, ответственное за организацию обработки персональных данных и цифровой трансформации в Министерстве здравоохранения Чеченской Республики, руководители медицинских организаций	Журналы учета проведения инструктажей сотрудников под личную подпись
3	Обеспечение безопасной технической альтернативы путем рассмотрения возможности предоставления сотрудникам локальных, защищенных инструментов автоматизации работы с текстами, функционирующих строго внутри закрытого защищенного контура Министерства здравоохранения Чеченской Республики без передачи информации в информационно-телекоммуникационную сеть «Интернет»	В соответствии с графиком цифровой трансформации на 2026–2027 годы	Должностное лицо, ответственное за организацию обработки и защиты персональных данных и цифровой трансформации Министерства здравоохранения Чеченской Республики, ГКУ «Управление по обеспечению деятельности Минздрава здравоохранения Чеченской Республики»	Внедрение локальных модулей автоматизации, составление технических актов ввода в эксплуатацию

Политика
использования технологий искусственного интеллекта в ГБУ «РКЦИБ ПБ СПИД» Чеченской Республики.

1. Общие положения

1.1. Настоящая Политика (далее – Политика) определяет единые правила, цели, принципы, требования и ограничения при использовании технологий искусственного интеллекта (далее – ИИ) сотрудниками ГБУ «РКЦИБ ПБ СПИД»

1.2. Политика разработана с целью обеспечения информационной безопасности, защиты прав граждан при обработке их персональных данных, соблюдения врачебной тайны и предотвращения несанкционированного доступа к конфиденциальной информации ГБУ «РКЦИБ ПБ СПИД» с:

Уголовным кодексом Российской Федерации (статья 137 «Нарушение неприкосновенности частной жизни»);

Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

Федеральным законом от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

Федеральным законом от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

Федеральным законом от 26 июля 2026 года № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации»;

постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

предварительным национальным стандартом ПНСТ 961-2024 «Системы искусственного интеллекта в здравоохранении. Этические аспекты», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 25 октября 2024 года № 68-пнст;

Кодексом этики применения искусственного интеллекта в сфере охраны здоровья (версия 2.1), утвержденным протоколом Межведомственной рабочей группы при Министерстве здравоохранения Российской Федерации по вопросам создания, развития и внедрения в клиническую практику медицинских изделий и сервисов с использованием технологий искусственного интеллекта от 14 февраля 2025 года № 90/18-0/117, иными нормативными правовыми актами Российской Федерации, нормативными актами и методическими документами уполномоченных федеральных органов исполнительной власти (Роскомнадзора, ФСТЭК России, ФСБ России), а также нормативными правовыми актами Чеченской Республики.

1.3. Действие Политики распространяется на всех сотрудников Министерства и медицинских организаций, а также на лиц, привлекаемых к работе на основании гражданско-правовых договоров, имеющих доступ к информационным системам, компонентам систем искусственного интеллекта и персональным данным.

2. Термины и определения

2.1. ИИ – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы математического моделирования), процессы и сервисы по обработке данных и поиску решений.

2.2. Генеративный ИИ – технологии и системы ИИ, предназначенные для автоматического создания (генерации) нового контента (включая текстовую, графическую, звуковую и иную цифровую информацию, а также программный код) на основе обработки и анализа обученных массивов данных.

2.3. Оператор персональных данных (далее – Оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных (далее – персональные данные), а также определяющие цели обработки, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.4. Обезличивание персональных данных (далее – обезличивание) – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

3. Цели и принципы использования ИИ

3.1. Использование ИИ в ГБУ «РКЦИБ ПБ СПИД» допускается исключительно в целях повышения эффективности, качества и доступности оказания медицинской помощи населению Чеченской Республики, оптимизации административных процессов и поддержки принятия управленческих решений.

3.2. Основными принципами использования ИИ в ГБУ «РКЦИБ ПБ СПИД» являются:

законность – любое использование ИИ должно строго соответствовать законодательству Российской Федерации и законодательству Чеченской Республики;

приоритет прав граждан – защита прав и свобод человека и гражданина имеет приоритет над технологической и экономической эффективностью;

минимизация данных – в системы ИИ передается минимально необходимый для решения конкретной задачи объем данных, прошедший процедуру обезличивания и не позволяющий идентифицировать личность пациента;

подконтрольность – решения, влияющие на права граждан или связанные с установлением диагноза и назначением лечения, не могут быть приняты исключительно на основании вывода ИИ без участия человека;

ответственность – правовые, медицинские и иные последствия применения систем ИИ в полной мере возлагаются на должностное лицо, принявшее окончательное решение с использованием указанных технологий.»

3.3. Все системы ИИ разделяются на две категории:

публичные (внешние) системы ИИ – функционирующие в информационно-телекоммуникационной сети «Интернет» платформы, серверы и провайдеры которых находятся вне защищенного контура Министерства или медицинских организаций (включая текстовые чат-боты, генераторы графического контента, автоматические переводчики).

Допускается использование исключительно отечественных публичных систем ИИ, зарегистрированных в едином реестре российского программного обеспечения;

Корпоративные (ведомственные) системы ИИ – специализированное программное обеспечение, развернутое внутри закрытого контура Министерства или медицинских организаций, прошедшее аттестацию по требованиям ФСТЭК России и ФСБ России, либо государственные информационные системы, одобренные Министерством здравоохранения Российской Федерации.

3.4. Разрешенные сценарии использования публичных систем ИИ (исключительно при работе с общедоступной информацией):

редактирование, стилистическая правка и структурирование текстов, не содержащих служебную, конфиденциальную информацию, персональные данные или сведения, составляющие врачебную тайну;

поиск и анализ открытых данных, размещенных на официальных сайтах, в статистических сборниках и средствах массовой информации;

генерация концептуальных идей для публичных мероприятий, составление планов дискуссий и презентационных материалов;

перевод общедоступных медицинских статей и зарубежных научно-методических материалов.

4. Категорические запреты

4.1. Запрещается вводить (загружать, передавать, вносить, в том числе в виде файлов, таблиц, графических образов, сканов или фотографий) в поля ввода текстовых запросов (команд) любых публичных систем ИИ персональные данные пациентов, работников и иных физических лиц (включая фамилию, имя, отчество, дату рождения, адрес проживания, страховой номер индивидуального лицевого счета (СНИЛС), идентификационный номер налогоплательщика (ИНН), номер полиса обязательного медицинского страхования (ОМС), а также сведения о состоянии здоровья, диагнозах, анамнезе, результатах лабораторных и инструментальных исследований, назначенном лечении и иную информацию, содержащуюся в медицинской документации).

4.2. Запрещается вводить в публичные системы ИИ сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, данные служебной переписки, идентификационные данные (логины и пароли) для доступа к ведомственным и государственным информационным системам (включая ЕГИСЗ, МИС, ГИСЗ ЧР), а также проекты нормативных правовых актов и внутренних распорядительных документов до их официального опубликования.

4.3. Запрещается использование несертифицированных и неавторизованных систем ИИ для обработки информации, содержащей служебную тайну или персональные данные. Категорически запрещается использовать зарубежные системы ИИ, серверные мощности и провайдеры которых расположены вне территории Российской Федерации, для решения любых задач, связанных со служебной (трудовой) деятельностью.

4.4. Запрещается принятие юридически значимых решений, а также решений, непосредственно влияющих на процесс диагностики и лечения пациентов, на основании результатов использования систем ИИ без личной проверки, валидации и утверждения уполномоченным профильным специалистом (медицинским работником).

5. Требования к использованию ИИ

5.1. Обезличивание данных. Перед передачей информации в любую систему ИИ (включая внутренние корпоративные инструменты) данные должны быть обезличены в соответствии с требованиями Приказа Роскомнадзора от 19 июня 2025 года № 140 «Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных», за исключением случаев, указанных в пункте 9.1 части 1 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». Исключение составляет использование ИИ в составе сертифицированных медицинских информационных систем (МИС), обрабатывающих данные в защищенном контуре медицинских организаций. Результатом обезличивания должно быть полное исключение возможности деанонимизации и определения конкретного физического лица (пациента)

без использования дополнительной информации, хранящейся строго внутри Министерства или медицинских организаций.

5.2. Изолированный контур. Использование ИИ для работы с персональными данными (в том числе в составе МИС) допускается исключительно в информационных системах, прошедших оценку соответствия требованиям безопасности и аттестованных в качестве объектов информатизации.

5.3. Критическая информационная инфраструктура. Информационные системы медицинских организаций, используемые для оказания медицинской помощи и обработки данных пациентов, относятся к сфере здравоохранения, которая является субъектом критической информационной инфраструктуры.

В связи с этим:

5.3.1. При интеграции ИИ в такие системы обязательно проведение категорирования объекта критической информационной инфраструктуры и выполнение требований ФСТЭК России по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

5.3.2. О любых компьютерных инцидентах, связанных с работой ИИ, необходимо незамедлительно информировать Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

5.4. Прозрачность и маркировка. При подготовке документов с использованием ИИ (проекты писем, аналитические записки) сотрудник обязан:

5.4.1. Самостоятельно проверить достоверность и корректность сгенерированного текста;

5.4.2. Убедиться в отсутствии в тексте персональных данных и служебной информации;

5.4.3. При использовании сгенерированного контента в официальных документах указывать факт применения ИИ, если это требуется внутренними правилами документооборота.

6. Ответственность

6.1. Руководители ГБУ «РКЦИБ ПБ СПИД», начальники структурных подразделений, а также сотрудники несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации за:

6.1.1. Нарушение требований Политики;

6.1.2. Неправомерную обработку персональных данных, включая их передачу в системы ИИ;

6.1.3. Разглашение информации ограниченного доступа и сведений, составляющих врачебную тайну.

6.2. Нарушение требований законодательства Российской Федерации в области персональных данных и информационной безопасности, допущенное при использовании систем ИИ, влечет за собой:

6.2.1. Дисциплинарную ответственность в соответствии с Трудовым кодексом Российской Федерации, включая увольнение по основаниям, предусмотренным пунктом 6 части 1 статьи 81 Трудового кодекса Российской Федерации;

6.2.2. Административную ответственность в соответствии со статьей 13.11 Кодекса Российской Федерации об административных правонарушениях;

6.2.3. Уголовную ответственность в соответствии со статьями 137, 272 Уголовного кодекса Российской Федерации.

7. Контроль и аудит

7.1. Текущий контроль за соблюдением Политики осуществляется лицом, ответственным за организацию обработки персональных данных в ГБУ «РКЦИБ ПБ СПИД», должностным лицом, ответственным за цифровую трансформацию, руководителями структурных подразделений, а также руководителями медицинских организаций.

7.2. При выявлении фактов нарушения настоящей Политики применение систем ИИ в ГБУ «РКЦИБ ПБ СПИД» приостанавливается до полного устранения выявленных нарушений и реализации мер по обеспечению информационной безопасности.

8. Заключительные положения

8.1. Руководители ГБУ «РКЦИБ ПБ СПИД» обязаны организовать техническое ограничение доступа (блокировку на уровне прокси-серверов и сетевых экранов) к списку запрещенных зарубежных сервисов искусственного интеллекта на рабочих местах сотрудников.