УТВЕРЖДЕНА
распоряжением ОАО «РЖД»
от _____2022 г. № _____

КОНЦЕПЦИЯ
применения искусственного интеллекта в ОАО «РЖД»

МОСКВА 2022

Электронная подпись. Подписал: Чаркин Е.И.
№334/р от 14.02.2022

СОДЕРЖАНИЕ

1. Общие положения

1.1. Настоящая Концепция применения искусственного интеллекта (далее – Концепция) определяет цели, принципы, а также меры, направленные на использование технологий искусственного интеллекта в открытом акционерном обществе «Российские железные дороги» (далее – ОАО «РЖД», Компания).

1.2. Настоящая Концепция является основой для технической политики, нормативных, программных, методических и других документов ОАО «РЖД», дочерних и зависимых обществ ОАО «РЖД» в области технологий искусственного интеллекта.

1.3. Настоящая Концепция разработана с учетом следующих документов:

Национальная стратегия развития искусственного интеллекта на период до 2030 года, утвержденная Указом Президента Российской Федерации от 10 октября 2019 г. № 490 (далее – Национальная стратегия);

Распоряжение Правительства РФ от 19 августа 2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года»;

Приказ Министерства экономического развития Российской Федерации от 29.06.2021 № 392 «Об утверждении критериев определения принадлежности проектов к проектам в сфере искусственного интеллекта»;

Перечень поручений Президента Российской Федерации по итогам конференции «Путешествие в мир искусственного интеллекта» (Пр-2242 от 31 декабря 2020 г.).

1.4. Термины в области искусственного интеллекта, используемые в настоящей Концепции, употребляются в значении, приведенном в Национальной стратегии.

В частности искусственный интеллект в Национальной стратегии определяется как 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 машинного обучения), процессы и сервисы по обработке данных и поиску решений.

Другие используемые в настоящей Концепции термины и определения приведены в разделе 7.

1.5. Принципы классификации и подходы к созданию технологий искусственного интеллекта приведены в приложении 1. Описание основных технологий искусственного интеллекта приведено в приложении 2.

1.6. Корректировка настоящей Концепции осуществляется не реже чем каждые два года с даты утверждения на основании предложений Департамента информатизации ОАО «РЖД».

1.7. Экономические и иные эффекты от мероприятий и проектов ОАО «РЖД», использующих для получения своих результатов технологии искусственного интеллекта, должны включать в себя эффекты от применения технологий искусственного интеллекта. Отдельно от мероприятий и проектов ОАО «РЖД» экономические и иные эффекты от применения технологий искусственного интеллекта не рассчитываются.

2. Цели и основные направления применения технологий искусственного интеллекта

2.1. Целями применения в ОАО «РЖД» технологий искусственного интеллекта являются реализация стратегии цифровой трансформации ОАО «РЖД», вывод на рынок новых продуктов и услуг, основанных на технологиях ИИ, а также повышение надежности и эффективности существующих услуг и бизнес-процессов за счет использования технологий ИИ.

2.2. Достижение целей применения технологий искусственного интеллекта в ОАО «РЖД» осуществляется с учетом следующих принципов:

постоянное наращивание технологического потенциала, основанное на создании и развитии центров компетенции по ключевым технологиям искусственного интеллекта в периметре Компании;

общая техническая политика, предусматривающая централизованную координацию, унификацию и регулирование применения искусственного интеллекта подразделениями и обществами Компании;

преимущественное использование российских технологий и открытого программного обеспечения;

обязательность обоснованной оценки рисков причинения вреда жизни и здоровью пассажиров и работников при применении технологий искусственного интеллекта;

непосредственная вовлеченность подразделений Компании в применение технологий искусственного интеллекта в своей операционной деятельности.

2.3. Приоритетными направлениями применения технологий искусственного интеллекта в ОАО «РЖД» являются:

повышение эффективности процессов планирования, прогнозирования и управления (оптимизация производственных процессов, управление закупками, взаимоотношениями с поставщиками, логистикой, прогнозирование отказов и инцидентов, планирование ремонтов);

автоматизация рутинных (повторяющихся) производственных операций (диагностика состояния оборудования, оптимизация процессов взаимодействия с клиентами, контроль и управление доступом на объекты);

повышение безопасности сотрудников при выполнении бизнес-процессов (прогнозирование рисков и неблагоприятных событий, снижение степени непосредственного участия человека в процессах, связанных с повышенным риском для жизни и здоровья);

использование автономного интеллектуального оборудования и робототехнических комплексов (управление подвижным составом в автоматическом режиме, применение автопогрузчиков);

повышение лояльности и удовлетворенности клиентов (повышение качества оказания услуг за счет учета предпочтений клиентов, повышение качества информационно-справочного обслуживания);

оптимизация процессов подбора и обучения кадров, составление оптимального графика работы сотрудников с учетом различных факторов.

2.4. Для развития ИИ по указанным направлениям применяются следующие технологии, основанные на использовании ИИ:

а) компьютерное зрение;

б) обработка естественного языка;

в) распознавание и синтез речи;

г) интеллектуальные системы поддержки принятия решений на основе интерпретируемой обработки данных.

А также перспективные методы ИИ:

а) автономное решение различных задач;

б) автоматический дизайн физических объектов;

в) автоматическое машинное обучение;

г) алгоритмы решения задач на основе данных с частичной разметкой и (или) незначительных объёмов данных;

д) обработка информации на основе новых типов вычислительных систем;

е) интерпретируемая разработка.

Перечень технологических задач в транспорте и логистике ОАО «РЖД», решаемых с использованием технологий ИИ, приведены приложении 3.

Перечень применяемых технологий и технологических задач подлежит регулярному пересмотру и корректируется в соответствии с планами корректировки, указанными в п. 1.6 настоящей Концепции.

3. Механизмы реализации концепции

3.1. Реализация настоящей Концепции обеспечивается согласованными действиями подразделений ОАО «РЖД».

3.2. Общую координацию, контроль и мониторинг применения технологий искусственного интеллекта и настоящей Концепции осуществляет Департамент информатизации ОАО «РЖД», в том числе:

разработку и утверждение плана мероприятий по реализации настоящей Концепции;

определение технологических решений и продуктов в области искусственного интеллекта, применяемых в ОАО «РЖД» и дочерних обществах ОАО «РЖД»;

координацию и регулирование деятельности участников, проектов и мероприятий, осуществляемых в ОАО «РЖД» с применением технологий искусственного интеллекта;

определение и оценку базовых и целевых показателей динамики реализации технологий искусственного интеллекта в ОАО «РЖД»;

координацию с мероприятиями и программами в области цифровых технологий, включая:

1) мероприятия цифровой трансформации ОАО «РЖД»;

2) мероприятия импортозамещения ОАО «РЖД»;

привлечение к научно-технической экспертизе, апробации и реализации технологий искусственного интеллекта для нужд ОАО «РЖД» внутренних подразделений, дочерних обществ, научно-технического комплекса ОАО «РЖД», внешних поставщиков.

3.3. Финансовое обеспечение реализации настоящей Концепции осуществляется в рамках процессов инвестиционной деятельности ОАО «РЖД» в установленном порядке. На разных стадиях реализации проектов могут использоваться разные источники, в том числе программа информатизации, план НТР, бюджеты филиалов и прочие.

3.4. Применение технологий искусственного интеллекта в проектах ОАО «РЖД» осуществляется с учетом уровня готовности технологий и зрелости инновационного продукта к внедрению в ОАО «РЖД» в соответствии с приложением 2.

3.5. Оценка и сравнение с рынком (бенчмаркинг) показателей динамики реализации технологий искусственного интеллекта осуществляется с учетом показателей, приведенных в приложении 4.

3.6. Информационная безопасность применения технологий искусственного интеллекта обеспечивается с учетом нормативной базы, приведенной в приложении 5.

3.7. При реализации технологий искусственного интеллекта для нужд ОАО «РЖД» приоритетными подходами следует считать:

использование знаний, экспертизы, услуг, решений и продуктов от российских поставщиков, включая научно-технический комплекс ОАО «РЖД»[1];

использование свободно распространяемого программного обеспечения с открытым исходным кодом.

3.8. Реализация и распространение технологий ИИ требует узкопрофильных высококвалифицированных специалистов, которые будут как

[1] Департамент технической политики ОАО «РЖД» (ЦТЕХ), Центр инновационного развития – филиал ОАО «РЖД» (ЦИР), Центр научно-технической информации и библиотек – филиал ОАО «РЖД» (ЦНТИБ), АО «НИИАС», АО «ВНИИЖТ», отраслевые проектные бюро.

разрабатывать, так и использовать соответствующие программные инструменты и приложения для ИИ. В связи с чем в плане кадрового обучения необходимо предусмотреть мероприятия по обучению разработчиков и пользователей соответствующих программных решений, использующих технологий ИИ.

4. Этапы реализации концепции

4.1. Реализация настоящей Концепции осуществляется поэтапно:

этап 1 «Быстрый старт»;

этап 2 «Надежное развитие».

4.2. Этап 1 «Быстрый старт»

4.2.1. Назначение и сроки выполнения этапа

Назначение этапа – получение результатов от применения технологий искусственного интеллекта высокого уровня готовности.

Сроки выполнения этапа – 2021-2022 гг.

4.2.2. Основные мероприятия этапа.

Основными мероприятиями этапа являются:

1) запуск и развитие решений с применением перспективных методов ИИ:

а) автономное решение различных задач;

б) автоматический дизайн физических объектов;

в) автоматическое машинное обучение;

г) алгоритмы решения задач на основе данных с частичной разметкой и (или) незначительных объёмов данных;

д) обработка информации на основе новых типов вычислительных систем;

е) интеллектуальные системы поддержки принятия решений на основе интерпретируемой обработки данных;

2) определение и формирование центров компетенций ОАО «РЖД» по ключевым технологиям искусственного интеллекта;

3) разработка и гармонизация нормативной базы, регулирующей управление применением и развитием технологий искусственного интеллекта в ОАО «РЖД»;

4) формирование кадрового потенциала ОАО «РЖД» в области технологий искусственного интеллекта.

4.2.3. Научно-исследовательские и опытно-конструкторские работы

В рамках этапа «Быстрый старт» необходимо предусмотреть запуск системы научно-исследовательских и опытно-конструкторских работ (далее – НИОКТР) на кастомизацию («приземление») «технологий среднего уровня

готовности» под специфику ОАО «РЖД» за счет использования в них перспективных методов ИИ, указанных в пункте 4.2, направленных на создание принципиально новой научно-технической продукции, в том числе в целях разработки универсального (сильного) ИИ. Результатом НИОКТР должны стать опытные образцы, испытания которых продемонстрируют целесообразность использования конкретных технологий ИИ в конкретных задачах ОАО «РЖД». Таким образом, организуется фундаментальная база для этапа «Надежное развитие».

4.3. Этап 2 «Надежное развитие»

4.3.1. Назначение и сроки выполнения этапа

Назначение этапа – исследование потенциала и получение результатов от применения перспективных методов искусственного интеллекта, приведённых в пункте 4.2.

Сроки выполнения этапа – 2023-2025 гг.

4.3.2. Основные мероприятия этапа

Основными мероприятиями этапа являются:

1) запуск и развитие решений, выполняющих конкретные технологические задачи по следующим направлениям:
   а) обнаружение мошенничества и аномалий;
   б) системы автоматизированного (беспилотного) управления;
   в) компьютерное (машинное) зрение и распознавание изображений;
2) апробация опытных образцов, сформированных на первом этапе реализации Концепции;
3) развитие инфраструктуры для технологий искусственного интеллекта.

4.4. Распределение по этапам направлений применения технологий искусственного интеллекта осуществляется с учетом:

уровня готовности технологий ИИ;

готовности нормативной и законодательной базы для применения технологий ИИ;

наличия в ОАО «РЖД» успешных прототипов и пилотных проектов с применением соответствующих технологий ИИ;

экономической целесообразности и эффектов от реализации проектов, применяющих технологии ИИ.

5. Ожидаемые результаты реализации концепции

5.1. Реализация настоящей Концепции будет способствовать:

созданию новых и развитию существующих продуктов, сервисов и услуг для клиентов ОАО «РЖД»;

созданию новых и развитию существующих продуктов, сервисов и услуг для работников ОАО «РЖД»;

совершенствованию бизнес-процессов ОАО «РЖД»;

цифровой трансформации ОАО «РЖД».

6. Сокращения

В настоящем документе используются следующие сокращения:

№	Сокращение	Расшифровка
1.	ИИ	Искусственный интеллект
2.	ОАО «РЖД»	Открытое акционерное общество «Российские железные дороги»
3.	НИОКТР	Научно-исследовательские, опытно-конструкторские, опытно-технологические работы

7. Термины и определения

В настоящем документе используются следующие термины и их определения:

№	Термин	Определение
1.	Машинное обучение	Процесс, с помощью которого функциональный блок улучшает свои функциональные характеристики путем приобретения новых знаний или опыта или путем реорганизации существующих знаний и опыта [ГОСТ 33707–2016, п. 4.801]
2.	Бенчмаркинг	Процесс сопоставления стратегий, процессов, продукции организации и/или других объектов с объектами той же природы, при тех же обстоятельствах и аналогичными способами [ГОСТ Р 50779.100–2017, п. 3.2]

3.	Заадресовка	Перевозка груза или вагона на конкретную станцию назначения либо конкретному грузополучателю
4.	Технология	Результат научно-технической деятельности, предназначенный для использования и реализации, который включает в том или ином сочетании изобретения, полезные модели, промышленные образцы и другие объекты, подлежащие правовой охране, а также технические данные и другую информацию [№ 1899/р от 01.09.2021[2], раздел «Термины и определения»]
5.	Уровень готовности технологии	Степень развития разрабатываемой технологии с целью ее внедрения в производство конечного продукта [№ 1899/р от 01.09.2021, раздел «Термины и определения»]
6.	Фулфилмент	Комплекс операций с момента оформления заказа покупателем и до момента получения им покупки (от англ. fulfillment или брит. англ. Fulfilment – «выполнение, исполнение»)

[2] «Методика оценки зрелости инновационного продукта/технологии к внедрению в ОАО «РЖД» и рисков недостижения уровня готовности инновационных проектов в ОАО «РЖД» с их применением через соответствующие уровни готовности», утвержденная распоряжением ОАО «РЖД» от 1 сентября 2021 г. № 1899/р

Приложение 1.

Классификация и основные подходы к созданию технологий искусственного интеллекта

1. Классификация искусственного интеллекта

1.1. Существуют различные подходы к классификации технологий искусственного интеллекта.

Для целей настоящей концепции используется классификация технологий искусственного интеллекта на основе сравнения с интеллектуальными возможностями человека:

узкий искусственный интеллект;

общий искусственный интеллект;

искусственный супер-интеллект.

1.2. Узкий искусственный интеллект (англ. artificial narrow intelligence) – это ИИ, который решает узкие, ограниченные интеллектуальные задачи. В решении этих задач узкий ИИ может превосходить способности человека. В русскоязычных источниках узкий ИИ имеет следующие синонимы: слабый ИИ, ограниченный ИИ.

1.3. Общий искусственный интеллект (англ. artificial general intelligence) – это ИИ, находящийся на одном уровне с интеллектом человека и способный решать широкий круг интеллектуальных задач. В русскоязычных источниках общий ИИ имеет следующие синонимы: сильный ИИ.

1.4. Искусственный супер-интеллект (англ. artificial superintelligence) – это ИИ, превосходящий по интеллектуальным способностям отдельного человека или человечество в целом.

1.5. На текущий момент все технологии искусственного интеллекта в мире являются узким искусственным интеллектом.

1.6. Вопросы философии искусственного интеллекта, включая вопросы применимости к ИИ свойств человеческого сознания, в рамках настоящей концепции не рассматриваются.

2. Основные подходы к созданию искусственного интеллекта

2.1. В настоящий момент максимально широкое распространение получили следующие основные подходы для создания технологий ИИ:

1) символьный искусственный интеллект;

2) искусственные нейронные сети.

2.2. Символьный искусственный интеллект

Подход основан на предположении о том, что интеллект человека связан с процессом мышления без привязки к устройству мозга на физическом и биологическом уровне.

В этом подходе при создании искусственного интеллекта разработчики выделяют, формализуют и моделируют алгоритмы рассуждений и этапы процесса решения человеком интеллектуальных задач.

Схема подхода с использованием символьного искусственного интеллекта представлена на рисунке 1.

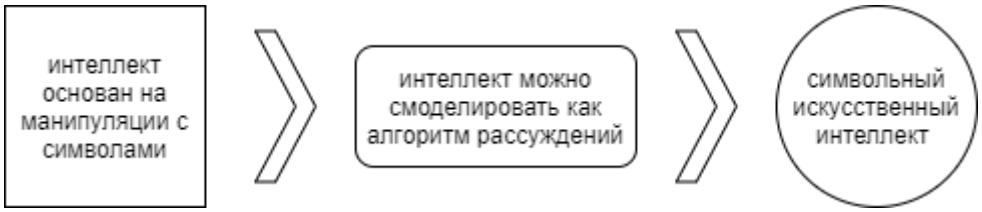

Рисунок 1

Одной из распространённых технологий, основанной на данном принципе, является технология экспертных систем (англ. expert system).

2.3. Искусственные нейронные сети

Подход основан на предположении о том, что интеллект человека связан с биологией и устройством человеческого мозга – нейроны, нейронные сети, структуры мозга.

В этом подходе при создании технологий искусственного интеллекта разработчики моделируют механизм работы интеллекта, отталкиваясь от его биологической основы.

Схема подхода с использованием искусственных нейронных сетей представлена на рисунке 2.

Рисунок 2

Одной из распространённых технологий, основанной на данном принципе является технология машинного обучения (англ. machine learning).

В текущий момент искусственные нейронные сети являются быстро развивающимся и основным подходом к созданию технологий искусственного интеллекта.

Приложение 2.

Технологии искусственного интеллекта

1. Уровни готовности технологий

1.1. Для оценки применимости в задачах ОАО «РЖД» технологических инноваций и инженерных разработок в области искусственного интеллекта используются уровни готовности технологий.

1.2. Уровни готовности технологий искусственного интеллекта определяются на основе методологии компании Gartner – «Цикл ожиданий». Отчет Gartner «Цикл ожиданий от искусственного интеллекта, 2020» представлен на рисунке 3.

Рисунок 3

1.3. Методология Gartner «Цикл ожиданий» включает в себя следующие уровни (сегменты) готовности технологий ИИ:

Появление инноваций (англ. Innovation Trigger);

Пик завышенных ожиданий» (англ. Peak of Inflated Expectation);

Реальная оценка возможностей (англ. Through of Disillusionment);

Прояснение возможностей (англ. Slope of Enrichment);

Плато продуктивности (англ. Plateau of Productivity).

1.4. В рамках настоящей Концепции уровень готовности технологий искусственного интеллекта указан в соответствии с отчетом Gartner «Цикл ожиданий от искусственного интеллекта, 2020». Отчет Gartner обновляется на регулярной основе, в связи с чем для оценки уровня технологической готовности следует использовать актуальный отчет на дату проведения оценки.

2. Оценка технологий искусственного интеллекта

2.1. В соответствии с отчетом Gartner «Цикл ожиданий от искусственного интеллекта, 2020» (рисунок 3) большинство технологий искусственного интеллекта находятся в сегменте «Появление инноваций» и «Пик завышенных ожиданий», что не гарантирует их дальнейший успех. При этом многие технологии, особенно в сегменте «Появление инноваций», не вышли за рамки концепций или прототипов.

2.2. В сегменте «Реальная оценка возможностей» находятся технологии, которые начинают использоваться в практических задачах: нейросети глубокого обучения, обработка естественного языка, машинное обучение, ускорители ПЛИС, чат-боты, компьютерное (техническое) зрение. Многим этим технологиям необходимо дальнейшее развитие для повышения шансов к практическому и массовому применению, и не факт, что все технологии достигнут требуемого уровня – например, для когнитивных вычислений Gartner сформирован прогноз недостижения уровня «Плато продуктивности».

2.3. В сегменте «Прояснение возможностей» находится одна работающая в практических задачах технология «Механизмы познания», которая дает возможность пользователю получать полезные сведения из больших объемов структурированных и неструктурированных данных.

2.4. В сегменте «Плато продуктивности» также находится одна технология графических процессоров, которая с недавнего времени стала применяться для задач высокопроизводительных вычислений.

3. Основные технологии искусственного интеллекта

ИИ общего назначения (англ. Artificial General Intelligence (AGI) – Ступень развития искусственного интеллекта, которая предполагает, что ИИ будет обладать признаками абстрактного и образного мышления, сможет делать отвлеченные умозаключения, строить прогнозы, то есть приблизится по своим возможностям к человеческому разуму.

Малые данные (англ. Small Data) – Наборы данных, достаточно небольшие, чтобы восприниматься человеком, но при этом поставляемые в виде и объемах, которые делают их доступными, информативными и полезными для деятельности человека. Например, данные о погоде со многих метеостанций страны или мира, каждая из которых поставляет наборы различных данных, слишком сложны для восприятия и оценки. Однако, после

обработки и анализа они приводятся во вполне воспринимаемые человеком прогнозы погоды, интерактивные карты движения грозовых фронтов и прочее.

Композитный ИИ (англ. Composite AI) – Комбинирование различных техник искусственного интеллекта для улучшения его способности к обучению, который позиционируется в качестве метода достижения ИИ ступени, общего искусственного интеллекта.

Генеративный ИИ (англ. Generative AI) – Алгоритмы, которые могут генерировать новый контент (текст, изображение и прочее), соотносящийся с информацией от предварительно обученных моделей.

Витрина моделей ИИ (англ. AI marketplace) – Виртуальное место, где разработчики могут выставлять свои предобученные модели искусственного интеллекта, а заказчики могут заказывать адаптированные модели искусственного интеллекта для своих нужд. Кроме того, в такой площадке можно осуществлять «федеративное обучение» (англ. federated learning) с привлечением различных наборов данных и моделей.

Ответственный ИИ (англ. Responsible AI) – ИИ с привлечением этических принципов, не позволяющих нарушать права человека, и направленный только на процветание человечества.

Вещи как клиенты (англ. Things as customers) – Концепция Интернета вещей IoT (англ. Internet of Things), в которой устройства, приборы, датчики («вещи») могут вести себя подобно клиентам, например, автоматически совершать транзакции. Например, умный электросчетчик сможет сам оплачивать потребленную электроэнергию через Интернет.

Нейроморфное оборудование (англ. Neuromorphic Hardware) – Устройства, в которых реализованы некоторые принципы работы нейросистемы человека. Данные принципы приводят к архитектуре вычислительных систем, принципиально отличающейся от традиционной архитектуры Фон Неймана (квантовые вычисления, нейроморфные системы).

Дополненный интеллект (англ. Augmented intelligence) – Использование информационных технологий, в том числе искусственного интеллекта, для усиления возможностей человеческого интеллекта.

ИИ для управления (англ. AI Governance) – Использование алгоритмов искусственного интеллекта для оценки и мониторинга процессов бизнеса, инвестиций, государственного и муниципального управления и прочего. Класс решений, которые проектируются и разрабатываются с использованием данной технологии, начинают называть анализ бизнес-процессов (англ. Process Intelligence).

ИИ для разработки и обучения (англ. AI developer and teaching skills) – Искусственный интеллект как инструмент разработки и обучения.

ИИ для принятия решений (англ. Decision intelligence) – Использование методов и средств ИИ в теории социальных наук, теории принятия решений и теории управления.

Умные роботы (англ. Smart Robots) – Использование средств искусственного интеллекта в робототехнике.

Разметка данных и услуги аннотирования (англ. Data Labeling and Annotation Services) – Использование методов и средств искусственного интеллекта для разметки данных и автоматического составления аннотаций.

Специализированные процессоры для глубоких нейросетей (англ. Deep Neural Network ASICs) – Разработка и производство нейросетей в виде монолитной микросхемы.

Интеллектуальные приложения (англ. Intelligent Applications) – Компьютерные программы (приложения), обладающие средствами ИИ для повышения их качества взаимодействия с человеком и уровня услуг.

Графы знаний (англ. Knowledge Graphs) – Использование ИИ в графах знаний: собрание фактов, где объекты (узлы) соединены друг с другом типизированными связями взаимозависимостей.

Цифровая этика (англ. Digital Ethics) – Междисциплинарное исследование этических, регуляторных и юридических проблем, возникающих в связи с развитием ИИ и других цифровых технологий.

Граничный ИИ (англ. Edge AI) – Использование средств искусственного интеллекта в устройствах «граничных вычислений» (англ. Edge Computing), небольших дата-центрах, развертываемых на границе сети, чтобы разгрузить магистральные сети и серверы больших дата-центров.

Облачные услуги ИИ (англ. AI Cloud Services) – Предоставление услуг искусственного интеллекта из облака.

Нейросети глубокого обучения (англ. Deep Neural Networks) – Нейросети с тремя и более слоями и разнообразными топологиями, которые способны лучше обучаться и отслеживать больше свойств и взаимозависимостей, чем однослойные сети.

Обработка естественного языка (англ. Natural Language Processing, NLP) – Средства ИИ, помогающие распознавать сообщения, произносимые на естественном языке, с возможными особенностями (акцент, дефекты речи и прочее), сленгом и отступлениями от грамматических и синтаксических норм.

Машинное обучение (англ. Machine Learning) – Обучение нейросети. Данная технология и термин часто используется как синоним искусственного интеллекта.

Ускорители на ПЛИС (англ. FGPA Accelerators) – Ускорители работы программируемых логических интегральных схем с использованием методов машинного обучения.

Чат-боты (англ. Chatbots) – Программы, которые могут имитировать речь собеседника, отвечать на вопросы и поддерживать разговор на общие или специализированные темы.

Компьютерное зрение (англ. Computer Vision) – Системы распознавания образов в изображениях и видео со средствами анализа, способные делать заключения о происходящем на видео.

Автономные транспортные средства (англ. Autonomous Vehicles) – Беспилотные автомобили и другие виды транспорта со средствами компьютерного зрения, способные безопасно ездить без вмешательства водителя. Gartner прогнозирует долгий цикл развития этой технологии.

Когнитивные вычисления (англ. Cognitive Computing) – Технологические вычислительные платформы, основанные на интеллектуальных методах обработки сигналов. В настоящее время исследования в этом направлении пока не дали практических результатов.

Механизмы познания (англ. Insight Engines) – Средства ИИ, которые дают возможность получать полезные сведения из больших объемов структурированных и неструктурированных данных (например, формирование баланса трат по кредитной карте на те или иные категории товаров и услуг с учетом контекста сделок).

Графические ускорители (англ. GPU Accelerators) – Ускорители работы графических процессоров GPU.

4. Оценка уровня зрелости конкретных инновационных продуктов, использующих перечисленные технологии ИИ и предлагаемых к внедрению в ОАО «РЖД», осуществляется с применением «Методики оценки зрелости инновационного продукта/технологии к внедрению в ОАО «РЖД» и рисков недостижения уровня готовности инновационных проектов в ОАО «РЖД» с их применением через соответствующие уровни готовности», утвержденной распоряжением ОАО «РЖД» от 1 сентября 2021 г. № 1899/р.

Приложение 3.

Искусственный интеллект в транспорте и логистике

1. В следующих направлениях деятельности отраслей транспорта и логистики наблюдается практическое применение технологий искусственного интеллекта:

административная деятельность;

управление цепочками поставок;

управление ремонтами;

фулфилмент;

взаимодействие с клиентами.

2. Ниже приведены примеры применения технологий искусственного интеллекта в перечисленных направлениях, в таблице 3.1 – примеры массового развития решений, в таблице 3.2 – примеры развития решений на стадии исследований и разработки.

Таблица 3.1 Примеры массового развития решений искусственного интеллекта

Решения ИИ	**Сфера применения**	**Смысловое описание**	**Эффекты**
Операционная деятельность			
Технологический процесс на основе компьютерного (машинного) зрения	– Местная работа на станциях – Работа на производственных площадках с регулярными маршрутами движения	Малолюдное и безлюдное управление транспортом на основе машинного зрения и движения в системе координат, сформированной сигналами датчиков инфраструктуры, датчиков электронной разметки, данными визуального наблюдения. Формирует упреждающие сигналы, команды на движение / торможение / маневры	– Сокращение влияния человеческого фактора – Сокращение затрат – Повышение безопасности
Моделирование эффективности использования парка	– Оперирование большим парком подвижного состава при разнообразных маршрутах и обширной клиентской базе	Имитационное моделирование работы парка с учетом его распределения по сети, состояния участков сети и статусов заявок на перевозку. Формирует варианты заадресовки с учетом входных данных и требуемых результатов (доставка в срок, доставка с минимальным порожним пробегом, доставка с минимальными затратами и прочее)	– Улучшение показателей порожнего пробега – Оптимизация производственного цикла подвижного состава – Повышение качества исполнения заказов клиентов – Сокращение ручного труда

Решения ИИ	Сфера применения	Смысловое описание	Эффекты
Управление цепочками поставок			
Формирование заданий на доставку в «последней миле»	– Обслуживание клиентов в ритейле (большое количество небольших заказов)	Автоматическое планирование оптимальной сети курьерских маршрутов, основанных на алгоритмах динамической маршрутизации на «последней миле» доставки заказов	– Рост производительности труда курьеров на «последней миле» – Качественная синхронизация мобильных курьерских отделений (МКО) с водителями на районных маршрутах – Высокоточный анализ качества работы и своевременности доставки груза
Выбор оптимального поставщика	– Управление поставщиками	Анализ различных наборов данных (таких как эффективность доставки, аудиты, оценки и кредитные баллы) и получение индивидуальных рекомендаций по управлению взаимоотношениями с поставщиками	– Сокращение затрат на идентификацию необходимого поставщика – Сокращение рисков в цепочке поставок

Решения ИИ	Сфера применения	Смысловое описание	Эффекты
Управление ремонтами			
Информирование о возможных инцидентах	– Управление ремонтами подвижного состава – Управление ремонтами производственного оборудования	Анализ машиночитаемой документации по обслуживанию и ремонту оборудования, данных из систем по управлению оборудованием, а также данных с датчиков оборудования для оперативного информирования специалистов по техническому обслуживанию о возможных несоответствиях и рисках	– Снижение рисков возникновения инцидентов – Сокращение влияния человеческого фактора – Повышение безопасности
Фулфилмент			
Обработка адресов доставки	– Обслуживание клиентов в ритейле (большое количество небольших заказов)	Роботизация процессов распознавания и стандартизации адресов доставки грузов	– Сокращение влияния человеческого фактора и ошибок в доставке – Сокращение затрат
Проверка достоверности документов транспортных компаний	– Маршрутизация грузов в распределительных центрах	Распознавание регистрационных свидетельств и сертификатов, выписок из торгового реестра, транспортных лицензий и проверка их достоверности путем сравнения с государственной базой данных	– Сокращение ошибок в доставке – Сокращение рисков – Сокращение затрат на проверку автомобильных перевозочных компаний

Решения ИИ	Сфера применения	Смысловое описание	Эффекты
Взаимодействие с клиентами			
Речевая аналитика	– Справки по требованию – Подбор маршрута и поезда по предпочтениям пассажира (в перспективе)	Распознавание и синтез речи, используемые для информационно-справочного обслуживания клиентов, приема стандартных заказов и анализа качества работы операторов в контакт-центре	– Повышение качества обслуживания клиентов на больших объемах и территориях

Таблица 3.2 Примеры развития решений искусственного интеллекта на стадии исследований и разработки

Решения ИИ	**Сфера применения**	**Смысловое описание**	**Эффекты**
Операционная деятельность			
Адаптивное управление движением	– Управление участниками движения на инфраструктуре, допускающей множественность вариантов действий	Сеть интеллектуальных агентов, обеспечивающая перестройку графика движения поездов в реальном времени. Использует пополняемые базы знаний и мультиагентные технологии для оперативного планирования железнодорожного движения – при возникновении непредвиденных событий технология перестраивает расписание движения с тем, чтобы минимизировать время возврата к расписанию всеми участниками и обеспечить сохранение удобства пассажиров	– Устойчивость расписания – Отсутствие задержек в движении – Соблюдение требований безопасности – Обеспечение прибытия по расписанию для пассажиров – Сокращение влияния человеческого фактора

Решения ИИ	Сфера применения	Смысловое описание	Эффекты
Управление автопогрузчиками	– Работа на складах и ограниченных территориях (заводские территории, морские порты) с инфраструктурой электронных коммуникаций и визуальной разметки	Прием и выполнение электронных заданий на размещение товаров, поиск товаров, идентификацию товаров, сборку и подготовку к отправке партий товаров в привязке к цифровым двойникам склада и действиям других погрузчиков	– Сокращение влияния человеческого фактора – Сокращение затрат
Управление цепочками поставок			
Прогнозирование времени в пути	– Планирование, организация и учет перевозок грузов	Модели машинного обучения (в частности, основанные на методе GBDT – Gradient Boosted Decision Trees), используемые для высокоточного прогнозирования времени в пути	– Повышение точности управления другими операциями цепочки поставок, включая заадресовку, балансировку распределения парка, моделирование грузовой работы

Решения ИИ	Сфера применения	Смысловое описание	Эффекты
Улучшение сквозной видимости и времени отклика по цепочке поставок	– Управление закупками в контексте цепочек поставок	Сбор и анализ в реальном времени данных от подключенных устройств и систем (включая системы SCM, ERP и CRM) для предвидения проблем (будь то внутри организации, например, из-за сбоев, или за ее пределами, например, задержка поставок) и принятия командой по закупкам решений, минимизирующих воздействия на цепочку поставок	– Сокращение объема страховых запасов – Закупки «точно по требованию»
Оптимизация склада	– Размещение товаров на складе – Определение минимально-необходимого персонала	Анализ заказов в онлайн-магазинах для определения наибольшего потребительского спроса и прогнозирования тенденций торговли с целью своевременной адаптации систем управления складом с адресным хранением (WMS)	– Сокращение издержек в складской деятельности – Снижение рисков низкого качества обслуживания в «пиковые» периоды

Решения ИИ	Сфера применения	Смысловое описание	Эффекты
Управление ремонтами			
Планирование ремонтов по прогнозу событий	– Управление ремонтами подвижного состава – Управление ремонтами производственного оборудования	Предиктивный анализ состояния оборудования, используемый для выработки рекомендаций по оптимальным действиям на основе потокового анализа данных, поступающих с оборудования, а также данных по фактической утилизации и планируемой загрузке	– Повышение коэффициентов полезного использования оборудования – Сокращение затрат, связанных с инцидентами и ремонтами – Повышение безопасности
Контроль состояния агрегата по анализу звука	– Диагностика состояния и ремонт сложных агрегатов	Анализ спектра побочных шумов с выделением шумов на разных режимах работы агрегатов, указывающих на возможные проблемы (нейронная сеть с технологией глубокого обучения).	– Повышение качества диагностики и ремонтов

Решения ИИ	Сфера применения	Смысловое описание	Эффекты
Взаимодействие с клиентами			
Речевая аналитика и умные чат-боты	– Подбор маршрута и поезда по предпочтениям пассажира (в перспективе)	Распознавание и синтез речи, взаимодействие с информационными системами продажи товаров и услуг (например, билетов), взаимодействие с системами оплаты с целью оказания конечной услуги клиенту.	– Повышение качества обслуживания клиентов – Расшивка «узких мест» в каналах продаж стандартных товаров и услуг

Приложение 4.

Состав и значения типовых показателей динамики реализации в ОАО «РЖД технологий искусственного интеллекта

В таблице 4.1 представлен набор агрегированных (усредненных по отраслям) показателей, связанных с развитием технологий искусственного интеллекта, на момент 2020 года, а также варианты сравнения показателей ОАО «РЖД» с данными показателями.

Таблица 4.1

№ п/п	Аналитические данные	Показатель	Порядок сравнения	Критерий сравнения
1.	Более 85 % крупных российских организаций уже реализовали или пилотируют ИИ-инициативы (tadviser.ru)	Факт реализации или пилотирования инициатив, связанных с применением технологий ИИ в отчетном году	– По результатам отчетного года устанавливаются факты реализации или пилотирования инициатив, связанных с применением технологий ИИ в ОАО «РЖД» – Подсчитывается количество выявленных фактов	– Превышение – по итогам отчетного года имеется несколько реализованных и/или пилотируемых ИИ-инициатив – Соответствие – по итогам отчетного года имеется одна реализованная и/или пилотируемая ИИ-инициатива – Недостижение – по итогам отчетного года нет реализованных и/или пилотируемых ИИ-инициатив

№ п/п	Аналитические данные	Показатель	Порядок сравнения	Критерий сравнения
2.	Около 70 % компаний внедрят как минимум один тип технологии искусственного интеллекта к 2030 году (mckinsey.com)	Факт внедрения в промышленную эксплуатацию решений на основе какой-либо технологии ИИ с подтверждением запланированных эффектов в отчетном году	– По результатам отчетного года устанавливаются факты внедрения в ОАО «РЖД» в промышленную эксплуатацию решений на основе различных типов технологий ИИ с подтверждением запланированных эффектов по проектам – По результатам отчетного года подсчитывается доля установленных фактов от количества всех запланированных к внедрению в ОАО «РЖД» решений ИИ	– Превышение – в отчетном году внедрены в промышленную эксплуатацию более 100 % от всех запланированных решений на основе нескольких технологий ИИ с подтверждением запланированных эффектов по проектам – Соответствие – в отчетном году внедрены в промышленную эксплуатацию от 90 до 100 % запланированных решений на основе какой-либо одной технологии ИИ с подтверждением запланированных эффектов – Недостижение – в отчетном году внедрены в промышленную эксплуатацию менее 90 % из запланированных решений на основе какой-либо одной технологии ИИ с подтверждением

№ п/п	Аналитические данные	Показатель	Порядок сравнения	Критерий сравнения
3.	В 2020 году CIO планируют развернуть на 14 % больше решений на основе ИИ в своих компаниях, чем по итогам предыдущего года (gartner.com)	Количество развернутых за год решений на основе технологий ИИ в сравнении с количеством развернутых решений ИИ за предыдущий год	– По результатам отчетного года устанавливается количество развернутых в ОАО «РЖД» решений на основе технологий ИИ – Производится сравнение с количеством развернутых в ОАО «РЖД» решений на основе технологий ИИ в предыдущем году	– Превышение – в отчетном году развернуто решений на основе технологий ИИ больше, чем в предыдущем году на 14 % и более – Соответствие – в отчетном году развернуто на 10-14 % решений на основе технологий ИИ больше, чем в предыдущем году – Недостижение – в отчетном году развернуто решений на основе технологий ИИ больше, чем в предыдущем году только на 10 % и менее

№ п/п	Аналитические данные	Показатель	Порядок сравнения	Критерий сравнения
4.	92 % руководителей компаний видят позитивные эффекты от ИИ-проектов в новых трансформационных возможностях и высокой динамике развития бизнеса (newvantage.com, bcg.com)	Доля ИИ-проектов, результаты которых направлены на расширение трансформационных возможностей и рост динамики развития бизнеса, от всех ИИ-проектов за отчетный год	– По результатам отчетного года актуализируется количество ИИ-проектов в ОАО «РЖД» в период с 2020 года по отчетный год – Устанавливается доля ИИ-проектов, результаты которых направлены на расширение трансформационных возможностей и рост динамики развития бизнеса	– Превышение – более чем в 92 % ИИ-проектов запланированы или достигнуты результаты, направленные на расширение трансформационных возможностей и рост динамики развития бизнеса – Соответствие – в 85-92 % ИИ-проектов запланированы или достигнуты результаты, направленные на расширение трансформационных возможностей и рост динамики развития бизнеса – Недостижение – менее чем в 85 % ИИ-проектов запланированы или достигнуты результаты, направленные на расширение трансформационных возможностей и рост динамики развития бизнеса

№ п/п	Аналитические данные	Показатель	Порядок сравнения	Критерий сравнения
5.	90 % CIO Российских компаний выражают желание получить профессиональную поддержку для более эффективной работы с технологиями ИИ (microsoft.com)	Факты использования профессиональной поддержки (консультанты, производители ИТ-решений для технологий ИИ) в ИИ-проектах за отчетный год	– По результатам отчетного года актуализируется количество ИИ-проектов в ОАО «РЖД» в период с 2020 года по отчетный год – Устанавливается доля ИИ-проектов, в которых используется (использовалась) профессиональная поддержка	– Превышение – более чем в 90 % ИИ-проектов используется профессиональная поддержка – Соответствие – в 80-90 % ИИ-проектов используется профессиональная поддержка – Недостижение – менее чем в 80 % ИИ-проектов используется профессиональная поддержка

Приложение 5.

Информационная безопасность в области искусственного интеллекта

1. Нормативное регулирование Российской Федерации в области искусственного интеллекта

№ п/п	Документ	Описание и вопросы безопасности
1.	**Указ Президента Российской Федерации от 10 октября 2019 г. № 490** (утверждает Национальную стратегию развития искусственного интеллекта на период до 2030 года (далее – Стратегия))	**Первые два принципа Стратегии:** **защита прав и свобод человека**: обеспечение защиты гарантированных российским и международным законодательством прав и свобод человека; **безопасность**: недопустимость использования искусственного интеллекта в целях умышленного причинения вреда гражданам и юридическим лицам, а также предупреждение и минимизация рисков возникновения негативных последствий использования технологий ИИ. **Одна из основных задач в Стратегии:** Формирование комплексной системы безопасности при создании, развитии, внедрении и использовании технологий ИИ. **Одним из основных направлений разработки и развития ПО:** Разработка единых стандартов в области безопасности (в том числе отказоустойчивости) и совместимости программного обеспечения, эталонных архитектур вычислительных систем и программного обеспечения, а также определение критериев сопоставления программного обеспечения и критериев эталонных открытых тестовых сред (условий) в целях определения качества и эффективности программного обеспечения.

№ п/п	Документ	Описание и вопросы безопасности
		Констатировано: Требуется создание нормативно-правовой базы, предусматривающей обеспечение защиты данных, полученных при осуществлении экономической и научной деятельности, в том числе их хранение преимущественно на территории РФ, а также установление приоритетного доступа российских государственных органов и организаций к таким данным в рамках требований законодательства.
2.	**Федеральный закон от 24 апреля 2020 года № 123-ФЗ** (устанавливает экспериментальный правовой режим, а также регулирует отношения, возникающие в связи с его установлением, для создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в г. Москве. Экспериментальный правовой режим (далее –	**Один из основных принципов ЭПР:** Защита прав и свобод человека и гражданина, обеспечение безопасности личности, общества и государства. **Условия безопасности информации в рамках ЭПР:** 1. Циркуляция информации конфиденциального характера в среде участников ЭПР и обработка персональных данных. 2. Обезличивание ПДн как основной механизм защиты прав субъекта персональных данных в рамках ЭПР. 3. Регламентация правил обработки, хранения и уничтожения ПДн. 4. Хранение персональных данных, полученных в результате обезличивания, только на территории г. Москвы.

№ п/п	Документ	Описание и вопросы безопасности
	ЭПР) устанавливается на 5 лет)	
3.	**Федеральный закон от 31 июля 2020 года № 258-ФЗ** (определяет цели, принципы и круг участников экспериментальных правовых режимов в сфере цифровых инноваций, а также регулирует отношения, связанные с их установлением и реализацией в Российской Федерации по направлениям: медицинская деятельность; проектирование, производство и эксплуатация транспортных средств; продажа товаров, работ,	**Первые два принципа ЭПР:** 1. Недопустимость ограничения конституционных прав и свобод граждан, нарушения единства экономического пространства на территории РФ или иного умаления гарантий защиты прав граждан и юридических лиц, предусмотренных нормативными правовыми документами. 2. Обеспечение безопасности личности, общества и государства. **Условия безопасности информации в рамках ЭПР:** 1. Информационное взаимодействие участников ЭПР осуществляется с учетом требований законодательства РФ об обращении со сведениями, составляющими государственную и иную охраняемую законом тайну, конфиденциальную и иную информацию, отнесенную в соответствии с законодательством РФ к информации ограниченного доступа, а также законодательства РФ о защите персональных данных. 2. Предметом специального регулирования не могут быть правоотношения, возникшие при осуществлении деятельности, связанной с защитой государственной тайны, обеспечением безопасности КИИ РФ. 3. Действие ЭПР может быть прекращено при выявлении непредвиденных рисков нарушения прав и свобод гражданина, причинения вреда жизни, здоровью или имуществу человека либо имуществу юридического лица, причинения вреда интересам государства, ущерба обороне и (или) безопасности государства, в том

№ п/п	Документ	Описание и вопросы безопасности
	услуг дистанционным способом; архитектурно-строительное проектирование, строительство и эксплуатация зданий, сооружений)	числе рисков нарушения надежного и устойчивого функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, электроэнергетической системы, сетей связи, критической информационной инфраструктуры.
4.	**Распоряжение Правительства РФ от 19 августа 2020 года № 2129-р** (об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г.)	**Цель Концепции:** Определение основных подходов к трансформации системы нормативного регулирования в РФ для обеспечения возможности создания и применения технологий ИИ в различных сферах экономики с соблюдением прав граждан и обеспечением безопасности личности, общества и государства. **Приоритетная цель регулирования:** Стимулирование разработки, внедрения и использования технологий, создание систем ИИ в доверенном и безопасном исполнении. **Один из принципов регулирования:** Применение риск-ориентированного междисциплинарного подхода и принятие ограничительных норм в случае, если применение технологий несет объективно высокий риск причинения вреда участникам общественных отношений, правам человека и интересам общества и государства. Развитие технологий ИИ должно основываться на базовых этических нормах и предусматривать проектируемое

№ п/п	Документ	Описание и вопросы безопасности
		соответствие закону, в том числе требованиям безопасности (применение систем ИИ не должно заведомо для разработчика приводить к нарушению правовых норм). **Концептуальная проблема регулирования:** Соблюдение баланса между требованиями по защите ПДн и необходимостью их использования для обучения систем ИИ. **Необходимо:** 1. Создание специального механизма для обеспечения: своевременного и эффективного внедрения ИИ без соблюдения избыточных административных процедур и с обеспечением необходимого уровня безопасности. 2. Адаптировать законодательство РФ для обеспечения: - правовых условий для безопасного доступа разработчиков систем ИИ к данным; - особых режимов для доступа к данным, включая ПДн, в целях проведения научных исследований, обучения ИИ и разработки технологических решений; - нормативного расширения перечня и типов открытых данных; - максимального использования потенциала «больших данных» и изменения существующих подходов к регулированию обезличенных персональных данных. - применения и оборота данных, полученных в результате обезличивания сведений, составляющих профессиональную и коммерческую тайну; - решения вопросов целесообразности и возможности определения условий, при которых субъекты профессиональной тайны вправе привлекать для обработки соответствующих сведений сторонние организации;

№ п/п	Документ	Описание и вопросы безопасности
		- условий получения согласия на обработку ПДн, когда она осуществляется при проведении научных исследований в сфере ИИ, а также использования систем ИИ, обеспечивающих необходимый уровень защиты персональных данных; - определения случаев и условий страхования ответственности за вред, как альтернативы иным инструментам регулирования; - создания современной системы нормативно-технического регулирования в области ИИ с целью обеспечения надежности, достоверности, безопасности и интероперабельности решений в этой области; - процедур обязательного и добровольного подтверждения соответствия; - использования мер, ограничивающих степень использования систем ИИ, вместо требований обязательного подтверждения соответствия при необходимости. **В разделе Концепции по ИБ констатировано:** 1. обеспечение необходимого уровня безопасности систем ИИ является ключевым условием внедрения таких технологий; 2. для отдельных категорий систем ИИ в зависимости от степени риска их использования могут быть установлены специфические требования безопасности; 3. развитие правового регулирования в сфере обеспечения ИБ должно происходить с учетом целей, задач и содержания законодательства РФ об информационной безопасности, включая правовое регулирование развития КИИ и защиту ПДн. 4. необходимо обеспечить учет национальных интересов РФ, ее граждан и отечественных компаний при формировании международного регулирования в сфере систем ИИ, а также интегрировать РФ в международный рынок ИИ с точки

№ п/п	Документ	Описание и вопросы безопасности
		зрения универсальности правового регулирования и использования базовых международных принципов.
5.	**Федеральный проект «Искусственный интеллект» Национальной программы «Цифровая экономика Российской Федерации»** (разработан паспорт федерального проекта «Искусственный интеллект» Национальной программы «Цифровая экономика Российской Федерации»)	Паспорт, раздел 3 «Задачи и результаты федерального проекта», пункт 2 «Поддержка научных исследований в целях опережающего развития ИИ»: - проведение научных исследований не менее шестью исследовательскими центрами в сфере ИИ, в том числе в области доверенного системного программного обеспечения (подпункт 2.1); - проведение научных исследований Академией криптографии РФ для ГИС в области обеспечения информационной безопасности при применении ИИ, разработка требований по обеспечению информационной безопасности в системах ИИ (подпункт 2.3).

2. Стандартизация Российской Федерации в области искусственного интеллекта

№ п/п	Документ	Описание и вопросы безопасности
1.	**ГОСТ Р 58776-2019 «Средства мониторинга поведения и прогнозирования намерений людей. Термины и определения»**	Вопросы обеспечения информационной безопасности не рассматриваются. Стандарт создает основу для развития интеллектуальных систем, эффективность функционирования которых напрямую зависит от возможности прогнозирования поведения людей. Стандарт разработан с целью обеспечения эффективной коммуникации с человеком интеллектуальных робототехнических систем, включая беспилотные транспортные средства, способные анализировать поведение участников дорожного движения. Кроме этого прогноз поведения может быть использован, например, для выявления людей с девиантными и преступными намерениями, что важно при решении задач безопасности.
2.	**ГОСТ Р 58777-2019 «Воздушный транспорт. Аэропорты. Технические средства досмотра. Методика определения показателей качества распознавания незаконных вложений по теневым рентгеновским изображениям»**	Вопросы обеспечения информационной безопасности не рассматриваются. Стандарт устанавливает единые требования к системам и алгоритмам распознавания незаконных вложений в багаже и ручной клади по теневым рентгеновским изображениям.

№ п/п	Документ	Описание и вопросы безопасности
3.	**ГОСТ Р ИСО/МЭК 20546-2019 «Информационные технологии. Большие данные. Обзор и словарь»**	В рамках предложенного проекта стандарта даются понятия «Безопасность данных» и «Требования по защите конфиденциальности» и соответствующие пояснения к этим понятиям. На общественное обсуждение вынесена первая редакция стандарта. Национальный стандарт входит в серию национальных стандартов, гармонизирующих международные документы в области больших данных, и идентичен положениям действующего международного стандарта ISO/IEC 20546:2019 Information technology – Big data – Overview and vocabulary.
4.	**Приказ Росстандарта от 25 июля 2019 года № 1732.** (о создании Технического комитета по стандартизации ТК 164 «Искусственный интеллект», который представляет собой зеркальное отражение на национальном уровне профильного международного подкомитета ISO/IEC JTC 1 SC 42 «Artificial Intelligence»)	Проведение плановых работ по следующим направлениям: Направление № 2 «Качество технологий»: - Доверенность систем ИИ (тех. отчет) - Управление рисками (стандарт) Направление № 3 Большие данные: - Большие данные. Безопасность и конфиденциальность (стандарт) Направление № 4 Информационная безопасность и этические аспекты применения систем ИИ: - Особенности использования ПДн (отчет) Направление № 7 Требования к технологиям ИИ в системах безопасности: - Автоматическая идентификация по биометрическим признакам и ее качество (стандарты)

3. Зарубежная практика

№ п/п	Документ	Описание и вопросы безопасности
1.	**Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Конвенция 108+)**	**Общий регламент о защите данных (General Data Protection Regulation – GDPR)** Конвенция о защите физических лиц при автоматизированной обработке персональных данных, является в настоящее время единственным глобальным международным договором в сфере защиты персональных данных, носящим юридически обязывающий характер. Россия подписала и ратифицировала протокол о внесении изменений в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data). **Последствия ратификации Конвенции:** С учетом того, что РФ берет на себя обязательства по гармонизации национального законодательства в сфере персональных данных с учетом положений обновленной Конвенции, необходимо в будущем учитывать ее положения и положения европейского Общего регламента о защите данных (General Data Protection Regulation - GDPR). Европейский регламент GDPR рассматривает правовой режим обработки персональных данных в странах, присоединившихся к Конвенции, как адекватный. Это значит, что европейские регуляторы в рамках GDPR не будут применять к российским компаниям, работающим на рынках ЕС, дополнительные меры защиты персональных данных. Обновленная Конвенция сохраняет суверенность подходов, связанных с

№ п/п	Документ	Описание и вопросы безопасности
		защитой прав субъектов персональных данных. Принятие мер защиты на территории РФ рассматривается в рамках национального законодательного поля и является исключительной компетенцией российского надзорного органа. **Главные изменения:** Изменения в определении новых прав, предоставляемых гражданам для управления своими персональными данными при их обработке на основе математических алгоритмов, искусственного интеллекта и т.д. Вводится обязанность операторов персональных данных уведомлять уполномоченный надзорный орган об утечках, устанавливается четкий режим трансграничных потоков данных. Положения документа требуют соблюдения принципа «проектируемой конфиденциальности», то есть интеграции мер защиты персональных данных на этапе проектирования систем их обработки. Расширяется состав типов конфиденциальных сведений, обработка которых отнесена к «специальной категории» и может быть осуществлена только в том случае, если законом установлены соответствующие гарантии. Теперь к ним отнесены генетические данные, биометрические данные, персональные данные, касающиеся правонарушений, уголовного судопроизводства, а также данные о членстве в профсоюзах и этническом происхождении. **Область действия Конвенции:** Вопросы обработки персональных данных, относящихся к сведениям, составляющим государственную тайну, фактически выведены за скобки новой редакции Конвенции.

№ п/п	Документ	Описание и вопросы безопасности
		Конвенция допускает исключения и ограничения своего действия в случаях защиты национальной безопасности, обороны, общественной безопасности, общественных интересов, важных экономических и финансовых интересов государства, обеспечения беспристрастности и независимости судебной власти, предотвращения, расследования и наказания преступлений, исполнения наказания по уголовным делам, а также для защиты субъекта данных или прав и основных свобод других лиц. **Принципы Конвенции:** Ключевыми принципами являются: законность, справедливость, точное обозначение целей, пропорциональность обработки данных, конфиденциальность по проекту и по умолчанию, ответственность и демонстрация соответствия (подотчетность), прозрачность, безопасность данных и управление рисками.
2.	**Руководящие принципы по искусственному интеллекту и защите данных** Комитет Конвенции о защите физических лиц при автоматической обработке персональных данных подготовил Руководящие принципы, которые представляют собой набор	**Руководящие указания для разработчиков, производителей и поставщиков услуг ИИ:** - должны придерживаться ценностно-ориентированного подхода при разработке своих продуктов и услуг; - должны оценивать возможные неблагоприятные последствия применения ИИ для прав и основных свобод человека; - на всех этапах обработки, включая сбор данных, должны придерживаться подхода, основанного на соблюдении прав человека; - должны критически оценивать качество, характер, происхождение и объем используемых персональных данных;

№ п/п	Документ	Описание и вопросы безопасности
	базовых мер, которым должны следовать правительства, разработчики, производители и поставщики услуг ИИ, чтобы его применения не умаляли человеческое достоинство, права человека и основные свободы каждого физического лица, в частности в отношении права на защиту данных.	- учитывать при разработке и использовании применений ИИ риск неблагоприятного воздействия на отдельных лиц и общество в результате использования взятых вне контекста данных и алгоритмических моделей; - создавать независимые комитеты экспертов в различных областях; - поощрять коллективные формы оценки рисков, основанные на активном участии отдельных лиц и групп, которых потенциально могут затрагивать применения ИИ; - обеспечить право отдельных лиц не подвергаться существенному влиянию решений, затрагивающих их интересы, на основе исключительно автоматизированной обработки без учета их мнений; - гарантировать пользователям свободу выбора в отношении использования ИИ путем предоставления реальных альтернатив применениям ИИ; - применять такие формы бдительности в отношении алгоритмов ИИ, которые способствуют подотчетности всех соответствующих заинтересованных сторон; - субъекты данных должны информироваться о том, что они взаимодействуют с ИИ; - должно быть обеспечено право возражения в связи с обработкой на основе технологий ИИ. Кроме приведенных указаний документ содержит Руководящие указания для законодателей и политиков.
3.	**Руководящие принципы по защите физических лиц при**	**Цель Руководящих принципов:** Содействие защите субъектов персональных данных при обработке ПДн в

№ п/п	Документ	Описание и вопросы безопасности
	обработке персональных данных в мире больших данных Комитет Конвенции о защите физических лиц при автоматической обработке персональных данных подготовил Руководящие принципы, которые обеспечивают сторонам общую основу для применения соответствующей политики и мер для введения в действие принципов и положений Конвенции 108 в контексте больших данных.	контексте больших данных путем изложения применимых принципов защиты данных и соответствующих методов для ограничения рисков для прав субъектов данных. Эти риски в основном связаны с потенциальной необъективностью анализа данных, недооценкой правовых, социальных и этических последствий использования больших данных для процессов принятия решений и маргинализацией эффективного и осознанного участия отдельных лиц в этих процессах. **Основные принципы:** - этическое и социально ответственное использование данных; - превентивная политика и оценка рисков; - ограничение целей и прозрачность; - индивидуальный подход; - свободное, конкретное, информированное и недвусмысленное согласие; - обезличивание; - вмешательство человека в решения с использованием больших данных; - политики открытых данных; - обучение.