

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ДРАЙВЕР ЦИФРОВОЙ ТРАНСФОРМАЦИИ И ИСТОЧНИК ЭКОНОМИЧЕСКИХ УГРОЗ

Александр Сергеевич МИКУЛЕНКОВ^{1,2}

¹Отдел приоритетных исследований и разработок, Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (национальный исследовательский университет)», Москва, Россия

²Научный стажер АНО ВО «Международный банковский институт имени Анатолия Собчака», Санкт-Петербург, Россия

Адрес для корреспонденции: А.С. Микуленков, 141701, Институтский переулок, 9,
г. Долгопрудный, Россия

Т.: +7 (498) 713-91-81, доб. 63-03. E-mail: mikulenkov.as@mipt.ru

Аннотация

Стремительная цифровизация хозяйственных процессов способствует повышению эффективности функционирования предприятий из разных отраслей экономики. Использование технологий искусственного интеллекта для анализа и обработки больших данных, принятия на их основе управленческих решений способствует более глубокому пониманию бизнес-процессов как внутри предприятия, так и за его пределами – в тесной взаимосвязи с динамичным миром контрагентов и стейкхолдеров. Несмотря на явные преимущества технологий искусственного интеллекта, их использование может иметь и негативные последствия, подвергающие риску экономическую безопасность предприятия, целостность и непрерывность его технологических циклов. В работе проанализированы различные направления применения технологий искусственного интеллекта на предприятии. Выявлены и сгруппированы основные риски, связанные с использованием искусственного интеллекта на предприятии, представлены меры по их смягчению. В заключение предлагается набор факторов, необходимых для успешного внедрения и использования искусственного интеллекта на предприятии. Сделан вывод о необходимости трансформации корпоративных стратегий риск-менеджмента и их адаптации к рискам цифровизации.

Ключевые слова

Искусственный интеллект, цифровая трансформация, экономическая безопасность, риски, риск-менеджмент.

ARTIFICIAL INTELLIGENCE: THE DRIVER OF DIGITAL TRANSFORMATION AND THE SOURCE OF ECONOMIC THREATS

Alexander Sergeevich MIKULENKOV^{1,2}

¹Department of Priority Research and Development, Federal State Autonomous Educational Institution of Higher Education «Moscow Institute of Physics and Technology (National Research University)», Moscow, Russia

²Scientific intern Autonomous non-profit organization of higher education «International banking Institute named after Anatoliy Sobchak»,
St. Petersburg, Russia

Address for correspondence: A.S. Mikulenkov, 141701, Institutsky lane, 9, Dolgoprudny, Russia
T.: +7 (498) 713-91-81, add. 63-03. E-mail: mikulenkov.as@mipt.ru

Abstract

The rapid digitalization of economic processes contributes to improving the efficiency of the functioning of enterprises from different sectors of the economy. The use of artificial intelligence technologies for analyzing and processing big data, making management decisions based on them contributes to a deeper understanding of business processes both inside and outside the enterprise - in close relationship with the dynamic world of counterparties and stakeholders. Despite the obvious advantages of artificial intelligence technologies, their use can also have negative consequences that jeopardize the economic security of the enterprise, the integrity and continuity of its technological cycles. The paper analyzes various areas of application of artificial intelligence technologies in the enterprise. The main risks associated with the use of artificial intelligence in the enterprise are identified and grouped, and measures to mitigate them are presented. At the conclusion of the work, a set of factors necessary for the successful implementation and use of artificial intelligence in the enterprise is proposed. It is concluded that it is necessary to transform corporate risk management strategies and adapt them to the risks of digitalization.

Keywords

Artificial intelligence, digital transformation, economic security, risks, risk management.

Введение

Согласно Указу Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации», искусственный интеллект (далее – ИИ) представляет собой «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» [1]. К технологиям ИИ относятся: технологии компьютерного зрения, обработки естественного языка, распознавания и синтеза речи, интеллектуальной поддержки принятия решений, а также перспективные методы ИИ.

ИИ активно используется в ходе цифровой трансформации предприятий – процессе имплементации современных технологий в производственные процессы и бизнес-операции с целью повышения их эффективности. К основным фундаментальным драйверам развития технологий ИИ можно отнести гиперперсонализацию рынка, увеличение количества накопленных больших данных, развитие методов обработки и анализа больших данных.

Пандемия COVID стала еще одним драйвером, который положительно повлиял на развитие и распространение систем ИИ, усилил влияние сформировавшихся до этого фундаментальных драйверов. Она ускорила развитие интеллектуальных ассистентов, голосовых и текстовых роботов, речевой аналитики, бесконтактных систем безопасности, систем бесконтактной оплаты и распознавания лиц. Активно развивались системы интеллектуального видеонаблюдения, происходили процессы конвергенции систем безопасности [2]. Данная тенденция, в частности, нашла отражение в увеличении объема рынка видеонаналитики в 2020 г. на 14,2% по сравнению с 2019 г. [2]. ИИ определил новые возможности и стал центральным инструментом в построении инновационных бизнес-моделей [3]. Согласно исследованию McKinsey, 61% компаний, связывавших в 2019 г. значительную часть своей прибыли с внедрением ИИ-решений, увеличили инвестиции в этой сфере в период пандемии [4].

Во время пандемии также снизился уровень недоверия к системам ИИ [5]. Гиперперсонализация рынка услуг стимулировала развитие ИИ-решений: чат-боты, голосовые ассистенты, видеоролики, рекламные стратегии, баннеры, контекстная реклама³⁰.

Увеличение денежных вложений в программы финансирования разработок в области ИИ также можно отнести к драйверам развития ИИ-решений. С каждым годом размер вложений в программы финансирования разработок в области ИИ в мире возрастает. По данным портала Statista, объем финансирования стартапов в области ИИ в мире с 2011 по 2020 гг. увеличился в 5 раз (см. Рисунок 1) [6]. Объем инвестиций за два квартала 2021 г. превысил суммарные инвестиции за весь 2020 г., что свидетельствует о стремительном росте интереса со стороны инвесторов к ИИ-решениям.

³⁰ Гиперперсонализация – это маркетинговая стратегия, в основе которой лежит использование данных о клиентах для улучшения качества их обслуживания.

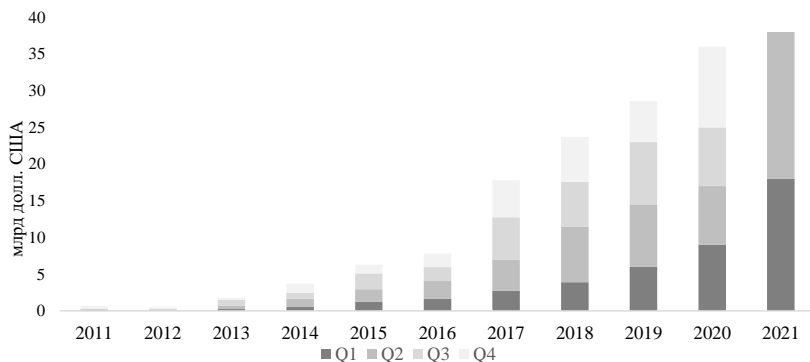


Рисунок 1 – Финансирование стартапов в области ИИ в мире с 2011 по 2021 гг., поквартально, в млрд долл. США

Источник: портал Statista

Применение ИИ, с одной стороны, способствует нивелированию существующих экономических рисков, с другой – создает качественно новые угрозы, обусловленные особенностями функционирования интеллектуальных технологических систем [7; 8]. Исследователи отмечают, что предварительная классификация «провалов» ИИ позволяет более точно и эффективно выявлять ключевые источники неопределенности и рисков функционирования автономных систем, способствует более эффективному контролю рисков [9; 10; 11].

Таким образом, разработка и реализация стратегий и мер цифровой защиты предприятия должна сопровождаться выявлением угроз и управлением рисками, где риск – это вероятностное наступление неблагоприятных последствий в результате влияния внешних или внутренних факторов на функционирование интеллектуальных систем [12].

Цель исследования

Целью данного исследования является анализ рисков, связанных с использованием ИИ на предприятии, выявление факторов, необходимых для смягчения «цифровых» рисков и успешной реализации проектов по внедрению и дальнейшему использованию технологий ИИ в масштабах бизнес-единицы. Для достижения заявленной цели были поставлены следующие задачи:

- проанализировать ключевые тенденции внедрения и использования ИИ;
- оценить эффекты от внедрения и использования ИИ;
- определить и классифицировать риски внедрения и использования технологий на базе ИИ, предложить меры по их смягчению.

Материалы и методы исследования

В ходе исследования был проведен анализ направлений экономической деятельности, в которых применение ИИ наиболее востребовано. Теоретическая основа исследования – это аналитические, консалтинговые исследования, экспертные оценки, статистическая документация. В работе использован следующий исследовательский инструментарий: абстрактно-логические методы исследования, методы обобщения, группировки, анализа и синтеза информации, метод экспертных оценок, кейс-анализ.

Объектом исследования является ИИ. Предметом исследования являются тенденции внедрения и использования ИИ для повышения эффективности хозяйственных процессов, оптимизации технологических циклов предприятий (трансформация бизнес-процессов), а также риски, обусловленные выявленными тенденциями.

Результаты исследования

В качестве ключевых тенденций развития ИИ были выделены:

- автоматизация производственных операций и бизнес-процессов;
- развитие механизмов прогнозирования с использованием ИИ;
- разработка и применение инструментов аналитики и первичного исследования;
- интеграция с иными сквозными цифровыми технологиями;
- разработка и применение человеко-машинных интерфейсов.

1) Автоматизация производственных операций и бизнес-процессов

Промышленность является одним из наиболее значимых сегментов рынка ИИ, что обуславливается вариативностью направлений применения подобных технологий в целях автоматизации производственных процессов. Направления применения ИИ в промышленной сфере охватывают весь цикл производства продукции. ИИ также активно применяется на рынке логистических услуг с целью автоматизации трудоемких действий, экономии средств, повышения эффективности использования ресурсов предприятия, оптимизации функционирования дорожно-транспортной инфраструктуры. По оценкам журнала *The Economist*, совокупная выгода от применений ИИ в логистике оценивается в пределах от 1,3 до 2 трлн долл. США в год [13]. ИИ используется для автоматизации складских операций, управления транспортом без участия человека, а также для управления инфраструктурой «умных дорог» как части экосистемы «умного города».

Системы ИИ активно используются в сфере услуг при взаимодействии с клиентом, его идентификации и оценки информации в соответствии с определенными критериями и алгоритмами. В финансовых сервисах ИИ применяется для автоматического расчета персонализированных предложений

конкретным клиентам на основе доступного объема персональных данных, включая потребительские предпочтения.

2) Развитие механизмов прогнозирования с использованием ИИ

Системы ИИ нашли широкое применение в предиктивной аналитике: от финансовых рынков до ритейла и медицины. Механизмы прогнозирования, используемые в этих сферах, базируются на методиках прогностического анализа, в основе которых лежат входящие в режиме реального времени потоки больших данных. ИИ выполняет анализ в автоматическом режиме со скоростью, превышающей скорость выполнения той же работы человеком.

Объединение прогностических способностей ИИ с функционалом торговых роботов позволяет повысить скорость и точность биржевой торговли, что является особенно важным в электронной биржевой торговле, на долю которой, по состоянию на 2020 г., приходится почти 45% от совокупных доходов торговли акциями [14].

Использование ИИ в ритейле позволяет с большей точностью прогнозировать объемы продукции. Применение ИИ в ритейле повышает эффективность работы магазинов, что выражается в увеличении прибыли, снижении времени нахождения товара на складах и на витрине, а также в минимизации возврата купленных товаров. В будущем ИИ может помочь дистрибьютерам и ритейлерам полностью автоматизировать принятие решений в режиме реального времени.

Использование ИИ в медицине позволяет заблаговременно предсказывать острые критические заболевания. Обучение ИИ на основе популяционных данных о заболеваемости позволяет определять отличия каждого конкретного случая болезни от среднего, выявлять индикаторы, сигнализирующие о состоянии организма, нарушении его нормального функционирования. Несмотря на точность и быстрдействие, применение подобных систем зачастую сопряжено со сложностью интерпретации полученных данных лечащими врачами [15].

3) Разработка и применение инструментов аналитики и первичного исследования

Применение ИИ в качестве инструмента аналитики и первичного исследования обосновано возможностью делегировать «умной» системе рутинные процедуры, которые, с одной стороны, не требуют интеллектуальных усилий человека, с другой – необходимы в рамках определенных технологических и хозяйственных процессов. ИИ используется для визуального или звукового распознавания категорий объектов. В рамках указанного направления применения алгоритмов ИИ значимую роль играют SVM-

системы³¹, основной задачей которых является классификация данных по изначально заданным параметрам. Например, типовой задачей SVM-систем является идентификация и отделение спама в потоке электронных писем.

ИИ-инструменты аналитики и первичного исследования нашли свое применение в сфере транспорта. Беспилотные автомобили, летающие дроны, железнодорожные составы и водные суда используют распознавание препятствий для адекватного позиционирования транспортного средства в пространстве, его корректного движения, реакции на изменение внешних условий, помощи человеку-водителю. Так, робот-помощник «Cognitive Agro Pilot» управляет движением комбайна, снижая нагрузку на человека-механизатора, и дает тому возможность, не отвлекаясь на управление сельскохозяйственной техникой, сконцентрироваться на уборке урожая [16].

4) Интеграция с иными сквозными цифровыми технологиями

Технология ИИ активно интегрируется с другими инновационными технологиями (VR/AR, группы новых производственных технологий – НПП – в т.ч. сенсоры, «умные» датчики и проч.) с целью повышения доступности и полноты сбора информации и ускорения ее обработки в режиме реального времени. Так, приложения дополненной реальности с элементами ИИ Vuforia Expert Capture (совмещение VR/AR и ИИ) обладают информацией о наборе технических инструментов и сведений об окружающей и производственной среде, что позволяет сотрудникам в режиме реального времени визуально осмотреть объект (в трехмерной плоскости), внести необходимые изменения в процесс его функционирования [17].

Применение ИИ вместе с «умными» датчиками происходит в системах промышленного интернета в процессе упаковки, перевозки, разгрузки и хранения грузов. Установленные на груз датчики позволяют собирать совокупность информации об условиях хранения и перевозки, целостности упаковки и сохранности ее содержимого. Дальнейшая передача этой информации ИИ позволяет анализировать грузовую логистику и информировать клиентов о статусе их груза в режиме реального времени. Для гарантии систематизации и точности информации в подобных случаях уместно использование систем распределенных реестров, способных гарантировать неизменность информации о грузе и ее четкую привязку ко времени. В качестве примера можно привести систему автоматизированного контроля качества погрузки руды, внедренную на производственных мощностях ПАО «Новолипецкий металлургический комбинат»: система контролирует процесс

³¹ Support Vector Machine – метод опорных векторов – метод обучения, использующийся в рамках задач классификации и регрессии.

загрузки, не допуская попадания в вагоны слишком больших валунов, не подлежащих дроблению на фабрике [18].

Технологические компании предлагают клиентам услуги по интеграции бытовых приборов в единую систему управления жилым пространством, которая будет обеспечивать безопасность и комфорт при проживании, а также позволит экономить на энергопотреблении, минимизируя участие человека. «Умный дом» «Xiaomi Smart Home» – один из примеров реализации данной технологии в виде технологичного пакетного решения [19].

5) Разработка и применение человеко-машинных интерфейсов

Применение алгоритмов ИИ направлено на разработку человеко-машинного интерфейса в целях повышения эффективности процессов обмена информацией между людьми и машинами. Управление подобными системами должно осуществляться за счет обеспечения связи между искусственными нейронами и мозгом человека. Мысленное управление большинством устройств, возможность реализации прямого подключения человека к интернету – лишь некоторые из возможных эффектов от имплементации человеко-машинных интерфейсов в жизнь общества.

В рамках данного исследования были выделены 5 укрупненных групп рисков, обусловленных использованием технологий ИИ в хозяйственной деятельности предприятия:

- риск конфиденциальности и безопасности данных;
- риск статистической дискриминации;
- риск принятия некорректных управленческих решений;
- риск критического сбоя в производстве/ инфраструктурный риск/ риск уязвимости технологических систем;
- риск кадрового дисбаланса.

1) Риск конфиденциальности и безопасности данных

Благодаря накоплению и анализу массивов больших данных, технологии ИИ активно используются в различных отраслях экономики. Данные, собираемые и используемые ИИ, зачастую являются персональными, в т.ч. биометрическими. Угрозы при работе с такими данными во многом исходят из уязвимости баз данных и цифровых хранилищ информации, которые могут быть подвержены взломам, похищены посредством кибератак. Цифровым кражам подвергается также интеллектуальная собственность предприятий, которая фактически является их технологическим активом.

Обеспечение безопасности пользователя и его данных – одна из основных и первостепенных задач, требующих решения при внедрении и использовании технологий ИИ. В ноябре 2020 г. была запущена информационная база данных

инцидентов ИИ (АИД), состоящая из сообщений о сбоях ИИ, которые стали причиной причинения вреда [20]. Данная база инцидентов, фиксируя «провалы» ИИ, предоставляет разработчикам и пользователям возможность учесть потенциальные риски и проблемы до введения системы в эксплуатацию.

2) Риск статистической дискриминации

Качество данных определяется их структурой, размерностью, наличием случайных выбросов, недостающих данных и дисбалансом классов данных [21]. На качество данных также влияет достоверность источника. Одним из последствий некачественных данных является появление пристрастной системы, т.е. системы, которая может быть несправедлива к какой-либо исследуемой группе, способствовать статистической дискриминации.

Система ИИ, подверженная внутренним предубеждениям конкретного источника данных, подвержена и риску принятия решений, которые могут привести к несправедливым, некорректным результатам [22].

3) Риск принятия некорректных управленческих решений

Чем глубже цифровые решения интегрированы в хозяйственные процессы компании, пользующейся некачественными данными, тем выше риски принятия неверного управленческого решения, которое повлечет за собой множество негативных последствий для функционирования предприятия, его технологической и финансово-экономической устойчивости. Некачественные данные являются причиной некорректной работы системы, что снижает эффективность ее использования и вызывает недоверие потребителя.

4) Риск критического сбоя в производстве, инфраструктурный риск, риск уязвимости технологических систем

Некорректная работа системы ИИ может способствовать сбоям в функционировании связанной с ней инфраструктуры, в т.ч. критически важной для реализации и поддержания хозяйственной деятельности предприятия. К подобным сбоям может приводить множество факторов: ограниченность вычислительных мощностей, относительно низкая скорость интернет-соединения, сложность поддержания функционирования системы ИИ, ее обслуживания, дороговизна энергопотребления.

После сбоя в работе алгоритмов ИИ, повлекшего за собой смерть человека, Uber Technologies полностью остановил тестирование автопилотируемых машин в Питтсбурге, Сан-Франциско и Торонто [23]. Помимо внутренних технологических сбоев в хозяйственных процессах предприятия, инфраструктурный риск может быть спровоцирован и реализован извне посредством кибератак. Так, миллионные убытки стали результатом кибератаки на металлургическое предприятие в Германии: внедрение

вредоносной программы в программное обеспечение привело к перегреву и выходу оборудования из строя доменной печи компании – критическому сбою в производственном процессе [23].

5) Риск кадрового дисбаланса

Кадровая проблема обусловлена сложностью интеллектуальных систем, с одной стороны, и низким уровнем «цифровой» квалификации сотрудников предприятия, с другой. Привлечение квалифицированных специалистов со стороны для решения нетиповых технико-технологических задач часто может быть невозможно силами и средствами компании в данный момент времени.

В рамках исследования описанные выше риски были сгруппированы, а также представлены меры по их снижению (см. Таблицу 1).

Таблица 1 – Риски и меры по их снижению

Риск	Митигирование
	Правовые
Риск конфиденциальности и безопасности данных	<p><i>Превентивные меры:</i></p> <ul style="list-style-type: none"> - «обезличивание» данных - децентрализованное хранение баз данных <p><i>В случае наступления риска:</i></p> <ul style="list-style-type: none"> - выявление «провалов» интеллектуальных систем - развитие и усиление систем кибербезопасности
	Аналитические
Риск статистической дискриминации	<p><i>Превентивные меры:</i></p> <ul style="list-style-type: none"> - анализ возможных направлений дискриминации - выявление предвзятости во входных данных <p><i>В случае наступления риска:</i></p> <ul style="list-style-type: none"> - снижение предвзятости системы - повышение качества данных - поиск более достоверных источников данных - замена источников
	Управленческие
Риск принятия некорректных управленческих решений	<p><i>Превентивные меры:</i></p> <ul style="list-style-type: none"> - подготовка данных, поступающих в систему - совмещение ручных и автоматических методов обработки - критический анализ выводов и расчетных оценок системы <p><i>В случае наступления риска:</i></p> <ul style="list-style-type: none"> - пересмотр подходов к сбору и анализу данных - модернизация аналитических систем - корректировка корпоративных стратегий
	Технологические
Инфраструктурный риск	<p><i>Превентивные меры:</i></p> <ul style="list-style-type: none"> - подготовка существующего оборудования - модернизация материально-технической базы <p><i>В случае наступления риска:</i></p> <ul style="list-style-type: none"> - снижение уязвимости интеллектуальных систем - повышение устойчивости и мощности вычислительных систем
	Кадровые
Кадровый дисбаланс	<p><i>Превентивные меры:</i></p> <ul style="list-style-type: none"> - выявление кадровых потребностей - подготовка и обучение персонала <p><i>В случае наступления риска:</i></p> <ul style="list-style-type: none"> - дополнительный найм компетентных специалистов - переобучение и перепрофилирование работников

Источник: составлено автором

При оценке рисков и разработке стратегий по их нивелированию важно оценить величину наступления конкретного риска, которая может быть получена путем перемножения значения вероятности на оценку степени влияния риска (см. Таблицу 2).

Таблица 2 – Оценка величины риска

Вероятность	Величина риска = вероятность × влияние				
	0,9	0,045	0,09	0,15	0,36
0,7	0,035	0,07	0,14	0,28	0,56
0,5	0,025	0,05	0,1	0,2	0,4
0,3	0,015	0,03	0,06	0,12	0,24
0,1	0,005	0,01	0,02	0,04	0,08
	0,05	0,1	0,2	0,4	0,8
			Влияние		

Источник: составлено автором

Согласно экспертным оценкам, критическими рисками считаются те, для которых расчетное значение величины влияния больше 0,18, умеренными – в диапазоне от 0,04 до 0,18, незначительными – до 0,04.

Вероятность наступления, степень влияния и величина рисков зависит от различных внутренних и внешних факторов: размера предприятия, отрасли функционирования, качества оборудования и программных систем и проч. В рамках разработки и реализации стратегий риск-менеджмента каждый риск необходимо оценивать, как минимум, дважды: на начальном этапе и по результатам реализации мер по его предотвращению.

Выводы

Вариативность направлений использования ИИ обуславливает проблемы применения соответствующих программных продуктов и алгоритмов. Внедрение технологий на базе ИИ в хозяйственную деятельность предприятий и социальную жизнь общества сопровождается возникновением ряда юридических и технических проблем, связанных с конфиденциальностью данных, безопасностью и ответственностью пользователей, вопросами интеллектуальной собственности.

На базе проведенного исследования автором предложен набор двухэтапных факторов, которые в совокупности позволят митигировать риски на предприятии, внедряющем и использующем ИИ. Так, успешное внедрение ИИ в деятельность организаций зависит от ряда первичных взаимодополняющих факторов (см. Рисунок 2):

- «цифровой» опыт и квалификация сотрудников, взаимодействующих с технологиями на базе ИИ;
- достаточные материально-технические возможности организации в совокупности с предварительной подготовкой и/или обновлением инфраструктуры для внедрения ИИ;

- разработка стратегий, дорожных карт развития систем ИИ в рамках предприятия и его структурных подразделений (прозрачное и объективное экономическое и управленческое обоснование применения ИИ на предприятии, оценка эффектов от внедрения и дальнейшего использования ИИ);

- желание и мотивация руководства совершать последовательные шаги на пути цифровой трансформации предприятия.

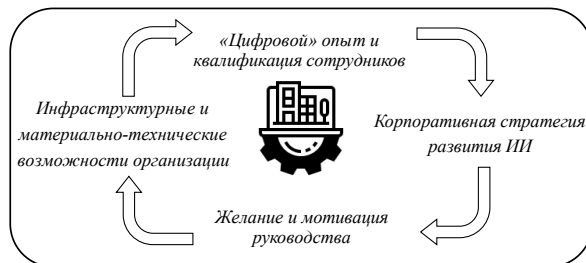


Рисунок 2 – Факторы успешного внедрения ИИ на предприятии

Источник: составлено автором

Данный набор факторов можно назвать первичным, поскольку он необходим для успешной реализации проектов по *внедрению* технологий ИИ на отдельном предприятии. Далее будет рассмотрен набор вторичных факторов, сформулированных в виде конкретных действий, выполнение которых способствует успешному *использованию* и обеспечению бесперебойного функционирования систем ИИ в ходе оптимизации хозяйственной деятельности предприятия (см. Рисунок 3).

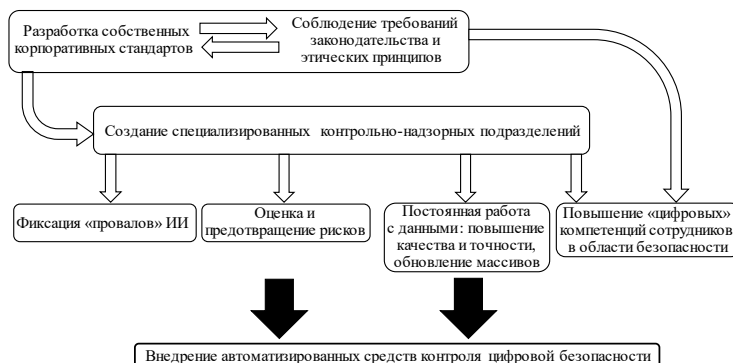


Рисунок 3 – Схема предпосылок для успешного использования ИИ на предприятии

Источник: составлено автором

Более подробно представленную совокупность вторичных факторов как набор последовательных и взаимодополняющих действий можно сформулировать следующим образом:

- разработка корпоративной нормативной и технической документации, устанавливающей принципы и требования к использованию систем ИИ в рамках данного предприятия, взаимодействию с подобными системами;

- соблюдение действующих требований законодательства в области ИИ, следование отраслевым и надотраслевым принципам кодексов этики ИИ при использовании систем ИИ и использовании результатов их функционирования;

- создание специализированных контрольно-надзорных подразделений внутри компаний, фиксирующих инциденты «провалов» ИИ и разрабатывающих оперативные стратегии реагирования на подобные провалы, способы их превентивного нивелирования, порядок действий персонала в случае выхода интеллектуальных систем из строя;

- обеспечение постоянной работы с массивами поступающих в интеллектуальные системы данных с целью их обновления, повышения качества и точности как самих данных, так и системы в целом;

- обучение сотрудников методам противодействия провалам ИИ, предотвращения масштабирования выявленной проблемы, контроль и повышение «цифровой» квалификации сотрудников;

- оценка рисков использования интеллектуальных систем, вероятности их наступления в текущих условиях инфраструктурных ограничений и кадровой подготовки специалистов предприятия;

- внедрение автоматизированных средств контроля безопасности при использовании ИИ.

Представленный набор факторов является общим для всех предприятий. Он может отличаться в зависимости от специфики производственной деятельности, особенностей технологических процессов.

Процесс цифровой трансформации современного предприятия подразумевает управление рисками на всех этапах его функционирования – от целеполагания до имплементации практических моделей риск-менеджмента [24], а также пересмотра самой корпоративной системы управления рисками. Помимо выработки общей корпоративной стратегии риск-менеджмента на уровне предприятия в целом, необходимо реализовывать стратегии на уровне конкретных проектов и подразделений, учитывая их специфику и уникальность [24].

Накопление опыта цифровой трансформации бизнеса будет способствовать теоретическому осмыслению значимости риск-менеджмента и

необходимости технической формализации процессов управления инновациями на уровне конкретного предприятия и его структурных подразделений.

Список источников

1. Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Официальный сайт Администрации Президента [Электронный ресурс]. URL: <http://www.kremlin.ru/acts/bank/44731> (дата обращения 08.03.2022).

2. Видеоаналитика (российский рынок) // Официальный сайт Tadviser [Электронный ресурс]. URL: <https://www.tadviser.ru/index.php/> Статья:Видеоаналитика_(российский_рынок) (дата обращения 08.03.2022).

3. The rise of the AI-powered company in the postcrisis world // Официальный сайт Boston Consulting Group BCG [Электронный ресурс]. URL: <https://www.bcg.com/publications/2020/business-applications-artificial-intelligence-post-covid> (дата обращения 22.02.2022).

4. The state of AI in 2020 // Официальный сайт McKinsey [Электронный ресурс]. URL: <https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-survey-the-state-of-ai-in-2020> (дата обращения 22.02.2022).

5. Итоги 2020: пандемия как драйвер искусственного интеллекта // Официальный сайт ICTMoscow [Электронный ресурс]. URL: <https://ict.moscow/news/itogi-2020-ai/> (дата обращения 22.02.2022).

6. Финансирование стартапов в области искусственного интеллекта (ИИ) // Официальный сайт Statista [Электронный ресурс]. URL: <https://www.statista.com/statistics/943151/ai-funding-worldwide-by-quarter/> (дата обращения 22.02.2022).

7. **Лапаев Д.Н., Морозова Г.А.** Искусственный интеллект: за и против. Развитие и безопасность. 2020. № 3. С. 70–77.

8. **Першина И.С.** Направления использования расширенного интеллекта в борьбе с COVID-19: риски и возможности. XV всероссийская научно-практическая конференция / МЦНС «Наука и просвещение» // Результаты современных научных исследований и разработок. 2021. С. 127–130.

9. **Burton S., Habli I., Lawton T., McDermid J., Morgan F.** Mind the gaps: Assuring the safety of autonomous systems from an engineering, ethical, and legal perspective. Artificial Intelligence, Volume 279, 2020. p. 1–16.

10. **Вислова А.Д.** Современные тенденции развития искусственного интеллекта // Известия Кабардино-Балкарского научного центра РАН. № 2 (94). 2020. С. 14–28.

11. **Карцхия А.А.** Искусственный интеллект как средство управления в условиях глобальных рисков // Мониторинг правоприменения. № 1 (34). 2020. С. 45–50.

12. **Карцхия А.А., Макаренко Г.И., Сергин М.Ю.** Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях

цифровизации системы права // Вопросы кибербезопасности. № 3 (31). 2019. С. 18–23.

13. How AI is spreading throughout the supply chain // Официальный сайт The Economist [Электронный ресурс]. URL: <https://www.economist.com/special-report/2018/03/28/how-ai-is-spreading-throughout-the-supply-chain> (дата обращения 22.02.2022).

14. How AI trading technology is making stock market investors smarter // Официальный сайт Built In [Электронный ресурс]. URL: <https://builtin.com/artificial-intelligence/ai-trading-stock-market-tech> (дата обращения 22.02.2022).

15. Explainable artificial intelligence model to predict acute critical illness from electronic health records // Официальный сайт Nature [Электронный ресурс]. URL: <https://www.nature.com/articles/s41467-020-17431-x> (дата обращения 22.02.2022).

16. Робот-помощник для автономного управления комбайном // Официальный сайт AI Russia [Электронный ресурс]. URL: <https://ai-russia.ru/library/cognitive-agro-pilot> (дата обращения 22.02.2022).

17. Vuforia Expert Capture: Scale Expert Knowledge to Your Frontline Workers // Официальный сайт PTC [Электронный ресурс]. URL: <https://www.ptc.com/en/products/vuforia/vuforia-expert-capture> (дата обращения 22.02.2022).

18. Контроль погрузки железной руды // Официальный сайт AI Russia [Электронный ресурс]. URL: <https://ai-russia.ru/library/nlmc-redmadrobot> (дата обращения 22.02.2022).

19. Умный дом Xiaomi Smart Home // Официальный сайт Xiaomi [Электронный ресурс]. URL: <https://xiaomi-smarhome.ru/> (дата обращения 07.03.2022).

20. Artificial Intelligence Incident Database // Официальный сайт AI Incident Database [Электронный ресурс]. URL: <https://incidentdatabase.ai/?lang=en> (дата обращения 22.02.2022).

21. Transforming Paradigms. A Global AI in Financial Services Survey // Официальный сайт EY [Электронный ресурс]. URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/innovation/ey-why-a-i-will-redefine-the-financial-services-industry-in-two-years.pdf (дата обращения 22.02.2022).

22. PwC's Responsible AI // Официальный сайт PwC [Электронный ресурс]. URL: <https://www.pwc.com/us/en/services/consulting/analytics/artificial-intelligence/what-is-responsible-ai.html> (дата обращения 22.02.2022).

23. Восстание машин. Какие риски искусственный интеллект создает для экономики // Официальный сайт Forbes [Электронный ресурс]. URL: <https://www.forbes.ru/finansy-i-investicii/363499-vosstanie-mashin-kakie-riski-iskusstvennyu-intellekt-sozdaet-dlya> (дата обращения 22.02.2022).

24. **Пашенко Д.С., Комаров Н.М.** Риск-менеджмент – ключевой элемент в цифровой трансформации промышленного предприятия // Мир новой экономики. 2021. 15 (1). С. 14–27.

25. **Sigova M.V.** Big data in digital-banks / Klioutchnikov, I.K., Sigova, M.V., Klioutchnikova, A.I. // Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020, 2019, стр. 9594–9601.

26. **Sigova M.V.** Adaptive analysis of merchant big data / Surnin, O., Sigova, M., Sitnikov, P., Ivaschenko, A., Stolbova, A. // Communications in Computer and Information Sciencethis, 2019, 1083, стр. 105–117.

27. **Sigova M.V.** The impact of the digitisation of the financial industry on the modelling and pricing of financial assets / Sigova, M., Klyuchnikov, I., Vasilev, S., Zatevakhina, A. // International Journal of Risk Assessment and Managementthis, 2020, 23(1), стр. 14–26.

28. **Iakovlev A.I., Kruglova I.A.** How the foundations of the crypto-economy methodology were formed / Alexander I. Iakovlev, Inna A. Kruglova // 2021 International Conference Engineering Technologies and Computer Science (EnT) EnT 2021 - 2021. - P. 77-82.

References

1. Ukaz Prezidenta Rossijskoj Federacii ot 10.10.2019 № 490 «O razvitii iskusstvennogo intellekta v Rossijskoj Federacii» // Oficial'nyj sajt Administracii Prezidenta [Elektronnyj resurs]. URL: <http://www.kremlin.ru/acts/bank/44731> (data obrashcheniya 08.03.2022).

2. Videoanalitika (rossijskij rynek) // Oficial'nyj sajt Tadviser [Elektronnyj resurs]. URL: [https://www.tadviser.ru/index.php/Stat'ya:Videoanalitika_\(rossijskij_rynek\)](https://www.tadviser.ru/index.php/Stat'ya:Videoanalitika_(rossijskij_rynek)) (data obrashcheniya 08.03.2022).

3. The rise of the AI-powered company in the postcrisis world // Oficial'nyj sajt Boston Consulting Group BCG [Elektronnyj resurs]. URL: <https://www.bcg.com/publications/2020/business-applications-artificial-intelligence-post-covid> (data obrashcheniya 22.02.2022).

4. The state of AI in 2020 // Oficial'nyj sajt McKinsey [Elektronnyj resurs]. URL: <https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-survey-the-state-of-ai-in-2020> (data obrashcheniya 22.02.2022).

5. Itogi 2020: pandemiya kak drajver iskusstvennogo intellekta // Oficial'nyj sajt ICTMoscow [Elektronnyj resurs]. URL: <https://ict.moscow/news/itogi-2020-ai/> (data obrashcheniya 22.02.2022).

6. Finansirovanie startapov v oblasti iskusstvennogo intellekta (II) // Oficial'nyj sajt Statista [Elektronnyj resurs]. URL: <https://www.statista.com/statistics/943151/ai-funding-worldwide-by-quarter/> (data obrashcheniya 22.02.2022).

7. **Lapaev D.N., Morozova G.A.** Iskusstvennyj intellekt: za i protiv // Razvitie i bezopasnost'. 2020. № 3. S. 70–77.

8. **Pershina I.S.** Napravleniya ispol'zovaniya rasshirennogo intellekta v bor'be s COVID-19: riski i vozmozhnosti. XV vserossijskaya nauchno-

prakticheskaya konferenciya / MCNS «Nauka i prosveshchenie» // Rezul'taty sovremennyh nauchnyh issledovaniy i razrabotok. 2021. S. 127–130.

9. **Burton S., Habli I., Lawton T., McDermid J., Morgan F.** Mind the gaps: Assuring the safety of autonomous systems from an engineering, ethical, and legal perspective // Artificial Intelligence. Volume 279. 2020. p. 1–16.

10. **Vislova A.D.** Sovremennye tendencii razvitiya iskusstvennogo intellekta. Izvestiya Kabardino-Balkarskogo nauchnogo centra RAN. № 2 (94). 2020. S. 1–28.

11. **Karckhiya A.A.** Iskusstvennyj intellekt kak sredstvo upravleniya v usloviyah global'nyh riskov // Monitoring pravoprimeneniya. №1 (34). 2020. S. 45–50.

12. **Karckhiya A.A., Makarenko G.I., Sergin M.YU.** Sovremennye trendy kiberugroz i transformaciya ponyatiya kiberbezopasnosti v usloviyah cifrovizacii sistemy prava // Voprosy kiberbezopasnosti. № 3 (31). 2019. S. 18–23.

13. How AI is spreading throughout the supply chain // Oficial'nyj sajt The Economist [Elektronnyj resurs]. URL: <https://www.economist.com/special-report/2018/03/28/how-ai-is-spreading-throughout-the-supply-chain> (data obrashcheniya 22.02.2022).

14. How AI trading technology is making stock market investors smarter // Oficial'nyj sajt Built In [Elektronnyj resurs]. URL: <https://builtin.com/artificial-intelligence/ai-trading-stock-market-tech> (data obrashcheniya 22.02.2022).

15. Explainable artificial intelligence model to predict acute critical illness from electronic health records // Oficial'nyj sajt Nature [Elektronnyj resurs]. URL: <https://www.nature.com/articles/s41467-020-17431-x> (data obrashcheniya 22.02.2022).

16. Robot-pomoshchnik dlya avtonomnogo upravleniya kombajnom // Oficial'nyj sajt AI Russia [Elektronnyj resurs]. URL: <https://ai-russia.ru/library/cognitive-agro-pilot> (data obrashcheniya 22.02.2022).

17. Vuforia Expert Capture: Scale Expert Knowledge to Your Frontline Workers // Oficial'nyj sajt PTC [Elektronnyj resurs]. URL: <https://www.ptc.com/en/products/vuforia/vuforia-expert-capture> (data obrashcheniya 22.02.2022).

18. Kontrol' pogruzki zheleznoj rudy // Oficial'nyj sajt AI Russia [Elektronnyj resurs]. URL: <https://ai-russia.ru/library/nlmc-redmadrobot> (data obrashcheniya 22.02.2022).

19. Umnyj dom Xiaomi Smart Home // Oficial'nyj sajt Xiaomi [Elektronnyj resurs]. URL: <https://xiaomi-smarthome.ru/> (data obrashcheniya 07.03.2022).

20. Artificial Intelligence Incident Database // Oficial'nyj sajt AI Incident Database [Elektronnyj resurs]. URL: <https://incidentdatabase.ai/?lang=en> (data obrashcheniya 22.02.2022).

21. Transforming Paradigms. A Global AI in Financial Services Survey // Oficial'nyj sajt EY [Elektronnyj resurs]. URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/innovation/ey-

why-a-i-will-redefine-the-financial-services-industry-in-two-years.pdf (data obrashcheniya 22.02.2022).

22. PwC's Responsible AI // Oficial'nyj sajt PwC [Elektronnyj resurs]. URL: <https://www.pwc.com/us/en/services/consulting/analytics/artificial-intelligence/what-is-responsible-ai.html> (data obrashcheniya 22.02.2022).

23. Vosstanie mashin. Kakie riski iskusstvennyj intellekt sozdaet dlya ekonomiki // Oficial'nyj sajt Forbes [Elektronnyj resurs]. URL: <https://www.forbes.ru/finansy-i-investicii/363499-vosstanie-mashin-kakie-riski-iskusstvenny-intellekt-sozdaet-dlya> (data obrashcheniya 22.02.2022).

24. **Pashchenko D.S., Komarov N.M.** Risk-menedzhment – klyuchevoj element v cifrovoj transformacii promyshlennogo predpriyatiya // Mir novoj ekonomiki. 2021. 15 (1). S. 14–27.

25. **Sigova M.V.** Big data in digital-banks / Klioutchnikov, I.K., Sigova, M.V., Klioutchnikova, A.I. // Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020, 2019, стр. 9594–9601.

26. **Sigova M.V.** Adaptive analysis of merchant big data / Surnin, O., Sigova, M., Sitnikov, P., Ivaschenko, A., Stolbova, A. // Communications in Computer and Information Sciencethis, 2019, 1083, стр. 105–117.

27. **Sigova M.V.** The impact of the digitisation of the financial industry on the modelling and pricing of financial assets / Sigova, M., Klyuchnikov, I., Vasilev, S., Zatevakhina, A. // International Journal of Risk Assessment and Managementthis, 2020, 23(1), стр. 14–26.

28. **Iakovlev A.I., Kruglova I.A.** How the foundations of the crypto-economy methodology were formed / Alexander I. Iakovlev, Inna A. Kruglova // 2021 International Conference Engineering Technologies and Computer Science (EnT) EnT 2021 - 2021. - P. 77-82.