ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

П Р Е Д В А Р И Т Е Л Ь Н Ы Й
Н А Ц И О Н А Л Ь Н Ы Й
С Т А Н Д А Р Т
Р О С С И Й С К О Й
Ф Е Д Е Р А Ц И И

ПНСТ

(проект)

Информационные технологии

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИТ

Последствия влияния стратегического управления при использовании искусственного интеллекта организациями

(ISO/IEC 38507:2022, MOD)

Издание официальное

Настоящий проект стандарта не подлежит применению до его утверждения

Москва

Российский институт стандартизации

2023

Предисловие

1 ПОДГОТОВЛЕН Научно—образовательным центром компетенций в области цифровой экономики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова» (МГУ имени М.В.Ломоносова) и Обществом с ограниченной ответственностью «Институт развития информационного общества» (ИРИО) на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 164 «Искусственный интеллект»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 202 г. № —ст

4 Настоящий стандарт является модифицированнным по отношению к к международному стандарту ИСО/МЭК 38507:2022 «Информационные технологии. Стратегическое управление ИТ. Последствия влияния стратегического управления при использовании искусственного интеллекта организациями» (ISO/IEC 38507:2022 «Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations», MOD). В настоящий стандарт включены дополнительные по отношению к международному стандарту ISO/IEC 38507:2022 годы выпуска стандартов для учета текущего статуса международных стандартов, на которые приведены ссылки в ISO/IEC 38507:2022.

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном операционном документе, приведены в дополнительном приложении ДА.

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТР 1.16—2011 (разделы 5 и 6).

Национальный орган Российской Федерации по стандартизации собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее, чем за девять месяцев до истечения срока его действия, разработчику

настоящего стандарта по адресу: 119991, Российская Федерация, Москва, Ленинские горы, д. 1 и в национальный орган Российской Федерации по стандартизации по адресу: 123112, город Москва, Пресненская набережная, дом 10, строение 2.

В случае отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемых информационном указателе «Национальные стандарты» и журнале «Вестник технического регулирования». Уведомление будет размещено также на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет.

© ISO, 2023
© IEC, 2023
© Оформление. ФГБУ «РСТ», 2023

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

Предисловие II
Введение VI
1 Область применения 1
2 Нормативные ссылки 2
3 Термины и определения 2
3.1 Термины, связанные с искусственным интеллектом 2
3.2 Термины, связанные со стратегическим управлением 3
4 Последствия влияния стратегического управления при использовании ИИ организациями 4
4.1 Общие положения 4
4.2 Поддержание стратегического управления при внедрении ИИ 5
4.3 Сохранение подотчётности при внедрении ИИ 7
5 Обзор ИИ и систем ИИ 9
5.1 Общие положения 9
5.2 Отличия систем ИИ от других информационных технологий 11
5.2.1 Автоматизация принятия решений 11
5.2.2 Решение задач, под влиянием данных 12
5.2.3 Адаптивные системы 12
5.3 Экосистема ИИ 13
5.4 Преимущества использования ИИ 16
5.5 Ограничения на использование ИИ 18
6 Политика в отношении использования ИИ 20
6.1 Общие положения 20
6.2 Надзор за стратегическим управлением ИИ 22
6.3 Стратегическое управление процессом принятия решений 22
6.4 Стратегическое управление использованием данных 25
6.5 Культура и ценности 27
6.6 Соответствие требованиям 28
6.6.1 Принятые обязательства 28
6.6.2 Менеджмент соответствия 30
6.7 Риск 31
6.7.1 Аппетит к риску и управление рисками 31
6.7.2 Управление рисками 32

6.7.3 Цели ... 33

6.7.4 Источники риска ... 35

6.7.5 Средства управления ... 38

Приложение А (обязательное)
Стратегическое управление и принятие организационных решений ... 40

А.1 Обзор соответствующих стандартов стратегического управления ... 40

А.1.1 Общие положения ... 40

А.1.2 Направление ... 40

А.1.3 Подотчетность ... 41

А.1.4 Надзор ... 42

А.2 Руководство руководящего органа в отношении управленческих решений ... 43

А.3 Стратегическое управление использованием данных ... 44

Приложение ДА (справочное)
Сведения о соответствии ссылочных национальных стандартов ссылочным международным стандартам, использованным в качестве ссылочных в примененном международном документе ... 45

Библиография ... 46

Введение

Целью настоящего стандарта является предоставление руководства для руководящего органа организации, которая использует или рассматривает возможность использования искусственного интеллекта (ИИ).

Этот документ содержит руководство по роли руководящего органа в отношении использования ИИ в своей организации и призывает организации использовать соответствующие стандарты в качестве основы для стратегического управления использованием ИИ.

В этом документе рассматриваются природа и механизмы ИИ в той степени, которая необходима для понимания последствий их использования с точки зрения стратегического управления: каковы дополнительные возможности, риски и ответственность, которые несет использование ИИ. Акцент делается на стратегическом управлении (которое осуществляется людьми) использованием ИИ в организации, а не на технологиях, составляющих любую систему ИИ. Однако такое стратегическое управление требует понимания последствий использования технологий.

Искусственный интеллект (ИИ)

ИИ охватывает семейство технологий, которые объединяют вычислительную мощность, масштабируемость, сетевые технологии, подключенные устройства и интерфейсы, а также огромные объемы данных. Упоминание «ИИ» в данном документе следует понимать как ссылку на целое семейство технологий и методов, а не на какую—либо конкретную технологию, метод или приложение. Концепция и терминология ИИ представлены в *ISO/IEC 22989:2022*.

Использование ИИ

«Использование ИИ» определяется в данном документе в самом широком смысле как разработка или применение системы ИИ на любом этапе ее жизненного цикла для достижения целей и создания ценности для организации. Это включает взаимоотношения с любой из сторон, предоставляющей или использующей такие системы.

Последствия влияния стратегического управления при использовании искусственного интеллекта

Сфера применения настоящего стандарта касается последствий использования ИИ для организации. Использование ИИ, как и любого другого мощного инструмента,

влечет за собой новые риски и ответственность, которые следует учитывать организациям, использующим его. ИИ не является по своей сути «добрым» или «злым», «справедливым» или «предвзятым», «этичным» или «неэтичным», хотя его использование может быть или казаться таковым.

Цель организации, этические нормы и другие руководящие принципы отражены, официально или неофициально, в ее политике. В данном документе рассматриваются как политика стратегического управления и политика организации, так и их применение, а также даются рекомендации по их адаптации для использования ИИ. Аспекты политики, связанные с оперативной деятельностью, реализуются через систему оперативного управления. Настоящий стандарт содержит ссылки на другие стандарты для получения подробной информации по смежным темам, включая социальную ответственность, надежность (например, менеджмент рисков, менеджмент смещенности и качества) и менеджмент соответствия требованиям.

В настоящий стандарт включены дополнительные по отношению к международному стандарту ISO/IEC 38507:2022 годы выпуска стандартов для учета текущего статуса международных стандартов, на которые приведены ссылки в ISO/IEC 38507:2022, выделенные курсивом, а именно:

- изменен раздел Введение;
- изменен раздел 2, удалено примечание о статусе ISO/IEC 22989;
- изменен раздел 3, удалено примечание о статусе ISO/IEC 22989;
- изменен раздел 5.3, названия Рисунка 1, Рисунка 2, удалены примечания о статусе ISO/IEC 22989:2022;
- изменен раздел 6.2, удалено примечание о статусе ISO/IEC 23894;
- изменен раздел 6.7.4, удалено примечание о статусе ISO/IEC TR 24027:2021, ISO 31050.

ПНСТ
(проект)

П Р Е Д В А Р И Т Е Л Ь Н Ы Й Н А Ц И О Н А Л Ь Н Ы Й С Т А Н Д А Р Т
Р О С С И Й С К О Й Ф Е Д Е Р А Ц И И

Информационные технологии
СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИТ
Последствия влияния стратегического управления при использовании искусственного интеллекта организациями

Information technology. Governance of IT. Governance implications of the use of artificial intelligence by organizations

Дата введения –

1 Область применения

Настоящий стандарт содержит руководство для членов руководящего органа организации по обеспечению и регулированию использования ИИ с целью обеспечения его эффективного, действенного и приемлемого использования в организации.

Настоящий стандарт также является руководством для более широкого круга лиц, включая следующие категории:

- высшее руководство;
- внешние коммерческие организации и специалисты—профессионалы, такие как юристы и бухгалтеры; ассоциации розничной торговли, отраслевые ассоциации и профессиональные организации и ассоциации;
- представители органов государственной власти;
- внутренние и внешние поставщики услуг (включая консультантов);
- оценщики и аудиторы.

Настоящий стандарт применим к стратегическому управлению настоящим и будущим использованием ИТ, а также к последствиям такого использования для самой организации.

Настоящий стандарт применим к любой организации, включая общественные и частные организации, государственные структуры и некоммерческие организации.

Издание официальное

Этот документ применим к организациям любого размера, несмотря на их зависимость от данных или информационных технологий.

2 Нормативные ссылки

Следующие стандарты упоминаются в тексте таким образом, что часть или все их содержание представляют собой требования настоящего стандарта. Для датированных ссылок применяется только указанное издание. Для недатированных ссылок применяется последнее издание стандарта, на который дана ссылка (включая любые поправки).

ISO/IEC 22989:2022, Информационные технологии — Искусственный интеллект — Концепции искусственного интеллекта и терминология

ISO/IEC 38500:2015, Информационные технологии — Стратегическое управление ИТ в организации

3 Термины и определения

Для целей настоящего документа применяются термины и определения, приведенные в ISO/IEC 22989, ISO/IEC 38500, а также следующие.

ИСО и МЭК поддерживают терминологические базы данных для использования в стандартизации, расположенные по следующим адресам:

- платформа ИСО для онлайн—просмотра материалов по стандартам (Online Browsing Platform, OBP) доступна по адресу https://www.iso.org/obp/ui;
- Электропедия МЭК (IEC Electropedia) доступна по адресу http://www.electropedia.org/.

3.1 Термины, связанные с искусственным интеллектом

3.1.1 **использование ИИ** (use of AI): разработка или применение системы ИИ на любом этапе ее жизненного цикла для достижения целей организации

Примечание 1 — Этот термин относится к любым действиям или деятельности, связанным с ИИ, которые могут иметь последствия для стратегического управления.

3.2 Термины, связанные со стратегическим управлением

3.2.1 **надзор** (oversight): отслеживание реализации организационной политики, политики стратегического управления и управления соответствующими задачами, услугами и продуктами, установленными организацией, с целью адаптации к изменениям внутренних или внешних обстоятельств

Примечание 1 – Эффективный надзор требует общего понимания ситуации. Надзор является одним из «принципов стратегического управления», подробно рассмотренных в ISO 37000:2021, 6.4.

3.2.2 **риск** (risk): Следствие влияния неопределенности на достижение поставленных целей

Примечания

1 Следствие влияния неопределенности — это отклонение от ожидаемого. Оно может быть положительным, отрицательным или и тем, и другим, и может устранять, создавать или приводить к возможностям и угрозам.

2 Цели могут иметь различные аспекты и категории и могут применяться на разных уровнях.

3 Риск обычно выражается в терминах источников риска, потенциальных событий, их последствий и вероятности.

[ИСТОЧНИК: ISO 31000:2018, 3.1]

3.2.3 **риск-аппетит** (risk appetite): Величина и тип соответствующего риска (3.2.2), который организация готова поддерживать или достичь

[ИСТОЧНИК: ISO Guide 73:2009, 3.7.1.2]

3.2.4 **принятые обязательства** (compliance obligations): требования, которые организация должна соблюдать в обязательном порядке, а также требования, которые организация выбирает добровольно

[ИСТОЧНИК: ISO 37301:2021, 3.25]

3.2.5 **соответствие** (compliance): выполнение всех принятых обязательств организации (3.2.4)

[ИСТОЧНИК: ISO 37301:2021, 3.26]

4 Последствия влияния стратегического управления при использовании ИИ организациями

4.1 Общие положения

Стратегическое управление организаций обеспечивается применением принципов, которые помогают организации выполнять свою организационную цель и при этом создавать ценность для организации и ее заинтересованных сторон. Согласно ISO 31000:2018, п. 5.3, в рамках стратегического управления определяется курс организации, ее внешние и внутренние взаимоотношения, а также правила, процессы и практики, необходимые для достижения ее цели. Структуры оперативного управления отражают направления стратегического управления в стратегии и соответствующих целях, необходимых для достижения желаемых уровней устойчивой производительности и долгосрочной жизнеспособности.

Обзор концепций стратегического управления и принятия организационных решений (и, в частности, ссылки на существующие стандарты), которым необходимо следовать, приведен в Приложении А.

Ответственность руководящего органа за постановку целей в традиционном контексте распространяется как на финансовые цели, так и на нефинансовые результаты, включая культуру, ценности и этические результаты. Разработка и исполнение политики организации, включая политику стратегического управления обычно обеспечиваются посредством сочетания средств управления, бизнес-планов, стратегий, должностных инструкций, принятой профессиональной практики, нормативных документов, обучения, ключевых показателей деятельности и различных форм коммуникаций с руководством.

Руководящий орган несёт ответственность за всю деятельность организации.

Руководящий орган организации несет постоянную ответственность за рассмотрение последствий внедрения любого нового инструмента, техники или технологии для организации.

Членам руководящего органа следует убедиться самим и быть в состоянии продемонстрировать заинтересованным сторонам что их политика (совместно с реализацией данной политики) является достаточной для организации, ее продукции

и взаимодействий, а также человеческих ресурсов, процессов и технологий, которые использует организация. В этом отношении ответственность за внедрение ИИ и за результат его внедрения не является чем-то новым. Однако ИИ обладает потенциалом, способствующим появлению у организации новых целей, а также более результативному и эффективному достижению и/или расширению существующих целей.

4.2 Поддержание стратегического управления при внедрении ИИ

Руководящий орган устанавливает цель организации и утверждает стратегии, необходимые для достижения этой цели. Однако, возможно, что существующее стратегическое управление уже не соответствует своему назначению, когда в организации используется ИИ. Следует, чтобы конкретный выбор инструментов, например систем ИИ, был решением руководства, принятым с учетом и в соответствии с указаниями руководящего органа. Для того чтобы выработать такое руководство, руководящему органу следует ознакомиться с ИИ в общих чертах, поскольку его использование может принести:

- значительную выгоду для организации в стратегическом плане;
- значительный риск для организации, чреватый нанесением ущерба ее заинтересованным сторонам;
- возникновение у организации дополнительных обязательств.

Руководящему органу следует оценить предполагаемое использование ИИ в рамках своего риск-аппетита. Риск может быстро меняться. Новые знания и проактивный подход дают организации возможность реагировать на риск. Поэтому организации следует продемонстрировать готовность к изменению или отмене проектов, если это будет сочтено необходимым. Дополнительное руководство см. в ISO/IEC 38506.

Использование ИИ приводит к новым последствиям, включая, но не ограничиваясь следующими:

- повышенная зависимость от технологий и систем для комплектования данных и обеспечения их качества;
- необходимость обеспечить прозрачность и объяснимость систем ИИ (включая понимание целей, предположений и включенных в них правил), когда частично или полностью автоматизированные системы используются

для решения задач и проблем, которые ранее выполнялись людьми (например, оценка кредитоспособности), совместно с адекватными процессами изменения и обновления этих алгоритмов;

- возможность того, что существующие направления и средства управления не подходят для обеспечения требуемых результатов (и снижения риска нежелательных последствий) или даже могут быть скомпрометированы. Это связано с различиями в допущениях, которые могут быть сделаны при делегировании полномочий человеку, в отличие от использования или получения поддержки от ИИ.

Пример 1. Инструкция «отложить погашение кредита до окончания праздников» достаточно понятна в контексте для другого человека-оператора, но недостаточно точна для правильного выполнения системой ИИ.

- конкурентное давление из-за продаж и деятельности организации, не использующей ИИ;
- принятие решения использования систем ИИ без осознания или рассмотрения потенциальной смещенности, ошибок или вреда, или последствий внедрения ИИ в существующие сложные системы;
- растущее несоответствие между скоростью изменений в автоматизированных системах обучения и связанных с ними человеко—ориентированных мер и средств обеспечения исполнения законодательно—нормативных требований;
- влияние ИИ на рабочую силу, включая опасения по поводу дискриминации, ущерба фундаментальным правам работников, увольнения в результате автоматизации или снижения требований к квалификации и переподготовке, возможной потери организационных знаний, а также использование ИИ для повышения творческого потенциала человека, повышения качества работы за счет делегирования повторяющихся, тривиальных или опасных задач системе ИИ;
- влияние на коммерческую деятельность и репутацию бренда.

Использование ИИ также может снизить или устранить некоторые существующие риски, и руководящему органу следует пересмотреть и соответствующим образом скорректировать свою оценку рисков.

Пример 2. Система ИИ может снизить риск ошибок, когда она используется в дополнение к персоналу, выполняющему повторяющиеся задачи, или когда персонал должен постоянно отслеживать системы в поисках редких отклонений (например, охранники).

4.3 Сохранение подотчётности при внедрении ИИ

Члены руководящего органа несут ответственность за контроль / надзор над деятельностью организации и за результаты этой деятельности, а также за системы и методы работы, позволяющие обеспечить уверенность в них. Они несут ответственность за решения, принимаемые в организации, включая решения, которые принимаются с использованием ИИ, а также за адекватность стратегического управления и средств управления в местах внедрения ИИ. Таким образом, они несут ответственность за использование ИИ, которое организация считает приемлемым.

Руководящему органу следует взять на себя ответственность за использование ИИ, а не возлагать ответственность на саму систему ИИ. Члены руководящего органа несут ответственность за свою осведомлённость о возможностях и рисках, связанных с использованием систем ИИ. Членам руководящего органа следует осознавать риск антропоморфизации ИИ — явления, при котором человеческие характеристики (например, мышление, эмоции, суждения, морализация) неоправданно приписываются системам ИИ, не пропорционально или несоответствующим образом по сравнению с тем, что необходимо для понимания роли, которую играет использование ИИ.

Члены руководящего органа могут быть привлечены к ответственности за неправильные действия организации в случаях, когда недостаточное проявление должной осмотрительности, недостаточные забота, руководство, обучение, надзор и принуждение в организации позволяют возникнуть проблемам. Такая ответственность может быть обеспечена самим руководящим органом, продиктована заинтересованными сторонами или установлена другими способами. Члены руководящего органа могут быть наказаны, отстранены от должности или привлечены к удовлетворению требований в суда.

Поэтому руководящему органу следует убедиться в том, что его практика соответствует конкретным целям, для которых ИИ применяется в организации. Это может включать пересмотр и, при необходимости, совершенствование следующего:

- Направление: через политику, стратегию, распределение ресурсов, кодексы этики, заявления о ценностях, цели или другие документы, касающиеся использования ИИ в организации;
- Надзор: посредством оценки ИИ, оценивания его ценности для организации и риск—аппетита организации, а также обеспечения внедрения, отслеживания, измерения, обеспечения принятия решений и других механизмов, связанных с использованием ИИ в организации;
- Оценка: рассмотрение различных элементов, например, внутренних и внешних факторов, относящихся к организации, текущих и будущих угроз и возможностей, достигнутых результатов, результативности и эффективности действующих механизмов стратегического управления, а также суждений о принятых решениях и вариантах.
- Отчетность: демонстрация заинтересованным сторонам того, что использование ИИ результативно регулируется ответственными лицами (сравните это с задачами «оценивать», «направлять» и «отслеживать» в ISO/IEC 38500:2015, 4.2).

Руководящему органу также следует убедиться, что он обладает достаточными возможностями для решения проблем, связанных с последствиями использования ИИ. Действия по решению проблем могут включать:

- совершенствование навыков, связанных с ИИ, среди своих членов;
- увеличение частоты проверки использования организацией ИТ и, в частности, ИИ;
- изучение и обновление критериев, используемых для отслеживания как внутренней, так и внешней среды;
- обеспечение представления интересов и проблем персонала (например, безопасность на рабочем месте, обучение персонала, качество работы);
- усиление надзора путем создания или усиления подкомитетов, занимающихся вопросами стратегии, рисков, оценки или аудита, а также этики.

Ответственность руководящего органа следует установить по всем аспектам предполагаемого или фактического использования ИИ и таким образом, чтобы обеспечить достижение намеченных результатов, а именно:

- при рассмотрении потенциальных последствий использования ИИ;
- при разработке бизнес—стратегий, включающих использование ИИ;

- на этапах приобретения, внедрения, конфигурации, развертывания, тестирования и других этапах проекта на протяжении всего жизненного цикла системы ИИ;
- изменения в среде, которой подвергается ИИ, обучение и действия, решения и результаты работы системы ИИ, а также ее воздействие на заинтересованные стороны;
- наличие соответствующих методов обеспечения безопасности для защиты организации, ее заинтересованных сторон и ее данных;
- при выводе из эксплуатации, включая знания и данные, которые содержатся в системе ИИ.

Наряду с проблемами, связанными с самим ИИ, существуют и другие проблемы, связанные с новыми технологиями, которые могут повлиять на организацию и ее заинтересованные стороны, в том числе:

- неправильное понимание природы технологий;
- принятие неадекватных стратегических управленческих решений;
- отсутствие надлежащего стратегического управленческого надзора за ИИ;
- неспособность включить ИИ в область распространения существующего стратегического управления;
- неуместное или повсеместное применение технологий без учета контекста, соответствующего планирования, политики или обучения;
- неспособность защитить и обезопасить информацию и активы от автоматизированных атак, использующих ИИ для выявления уязвимостей;
- неспособность рассмотреть последствия возникающих связей между людьми и системами ИИ.

5 Обзор ИИ и систем ИИ

5.1 Общие положения

Системы ИИ существуют в различных формах и требуют разной степени надзора со стороны руководящего органа. Таким образом, следует чтобы руководящий орган понимал, какие последствия влечёт за собой «использование ИИ» и на каком этапе

его использования следует вовлечь руководящий орган либо напрямую, либо через соответствующие механизмы стратегического управления.

Системы ИИ опираются на существующие возможности ИТ, включая сетевые технологии, устройства Интернета вещей, например, датчики и исполнительные механизмы, большие данные и облачные вычисления.

Большинство последних достижений в области технологий ИИ относятся к области машинного обучения (МО). МО — это технология ИИ, которая дает компьютерам возможность «учиться» без явного программирования. Данные являются ключевым фактором: они могут представлять собой, например, текст, числа, картинки, символы, формулы, графики, изображения, речь, звук или видео. С учетом существующего набора (обучающих) данных создается (настраивается) модель, которая применяется к новым данным для решения конкретной задачи, прогнозирования результата или классификации новых входных данных.

Характер систем ИИ, основанных на МО, включая цель их использования, выбор алгоритмов, подход, основанный на данных, методологии обучения и результаты, основанные на вероятности, таков, что существует потенциал дополнительного риска для организации и возможностей для нее (см. также 6.7).

Системы ИИ могут автоматизировать процесс принятия решений, анализируя данные для получения потенциального вероятностного результата и, во многих случаях, действуя в соответствии с этим результатом. Системы ИИ могут изменить характер продуктов, процессов и отношений, а также методы работы организации. Это может оказать существенное влияние на большинство отраслей.

Как и в случае с любым другим мощным инструментом, наряду с возможностью получения полезной отдачи также существует потенциал для причинения вреда, поэтому использование ИИ должно охватываться проводимой организацией оценкой риска.

Использование ИИ может привести к появлению у организации новых обязательств, как вытекающих из требований законодательства, так и являющихся следствием внедрения организацией добровольных кодексов практики, — что может происходить как непосредственно в ходе автоматизации системой ИИ процессов принятия решений, так и косвенно посредством использования данных или иных ресурсов и процессов. Основным вопросом, на который следует обратить внимание руководящему органу, является потенциальная возможность пересечения системой ИИ границы между демонстрацией вариантов выполнения действий и самостоятельным выполнением действий без участия человека.

От других технологий ИИ отличают огромный объём и сложность обрабатываемых данных, собираемых из разнообразных источников, которые могут быть слишком сложны для того, чтобы человек мог ими манипулировать или адекватно обрабатывать; а с точки зрения последствий для стратегического управления, технологии ИИ отличают:

- возможность автоматизации принятия решений;
- использование для решения проблем анализа данных, понимания и обучения, а не явным образом запрограммированной человеком логики решения задач;
- способность адаптироваться по мере изменения окружения системы ИИ, причем такими способами, которые не запрограммированы в явном виде и не обязательно известны заранее.

Эти три элемента имеют самые разнообразные последствия для организации и ее стратегического управления.

5.2 Отличия систем ИИ от других информационных технологий

5.2.1 Автоматизация принятия решений

Системы ИИ обычно выдают результаты на основе исторических и текущих данных, выбранных для задач, для которых система ИИ предназначена. В современных системах ИИ, в частности, основанных на МО, итоговый прогноз обычно даётся как возможный с определённой вероятностью.

Например:

- вероятность того, что эта деталь не соответствует требованиям качества, составляет 97 %;
- вероятность того, что этот маршрут будет самым быстрым, составляет 92 %;
- с вероятностью 98 % лицо перед камерой принадлежит «Барри Джонсу».

На основе этих вероятностей система ИИ может предпринять различные действия (действия, которые могут меняться со временем в результате переобучения). В некоторых случаях автоматические решения могут приниматься за доли секунды.

Скорость принятия таких решений является ключевым элементом систем ИИ, что делает их мощными инструментами для использования организациями. Процесс автоматизированного принятия решений может учитывать большие объёмы и разнообразие входных данных.

5.2.2 Решение задач, под влиянием данных

Системы ИИ, в частности, основанные на МО, обычно изучают большие объемы данных, выявляют и уточняют закономерности, обнаруженные в этих данных. Эта способность позволяет таким системам решать определенные типы задач, которые слишком сложны или трудоемки для самостоятельного решения человеком или с помощью классических методов программирования.

Вместо управления каждым логическим шагом и программирования решения задач человеком, на этот процесс влияют данные, например:

- распознавание лица — это то, что люди делают очень хорошо, но описать, как именно это достигается, очень сложно. Системы ИИ достигают этого путем изучения тысяч изображений лиц, изучения закономерностей в этих данных и применения этих закономерностей к новым изображениям лиц;
- процесс поиска раковой клетки среди миллионов здоровых клеток очень сложен, но методы МО для распознавания изображений оказались применимы для диагностики рака.

Все более широкое использование МО вместе (в случае, если система развивается благодаря переобучению и непрерывному обучению) с постоянно меняющимися данными значительно ускоряет решение задач и несет в себе огромный потенциал, а также вызовы для стратегического управления.

5.2.3 Адаптивные системы

Некоторые системы ИИ на этапе эксплуатации проходят переобучение либо обучаются постоянно. Входные данные, полученные во время работы, используются системой ИИ для улучшения и оптимизации своих внутренних моделей. Таким образом, со временем такие системы ИИ могут генерировать различные результаты на основе одних и тех же входных данных. Такая адаптация может развиваться как реакция на внешние стимулы, такие как изменения в окружающей среде или обратная связь, поступающая в систему ИИ. В качестве примера рассмотрим рекомендательную систему, которая отслеживает реакцию пользователя на свои

рекомендации и адаптируется для повышения коэффициента их принятия. Это и есть «непрерывное обучение» (ISO/IEC 22989:—, 3.1.10).

Адаптация также может быть результатом самосовершенствования, например, в системе ИИ, играющей в шахматы, которая способна обучаться, просто играя сама с собой.

Такие адаптивные системы также имеют следующие последствия для стратегического управления:

- Потенциально от системы ИИ может потребоваться наличие средств, позволяющих понять её функционирование, например, при проведении оценки или аудита.
- Поскольку функциональность системы ИИ со временем меняется, для обеспечения уверенности в том, что система по—прежнему работает в приемлемых границах, могут потребоваться дополнительные оценки или другие механизмы контроля.
- Адаптивность системы ИИ может повысить маневренность организации и обеспечить ей стратегическое преимущество.
- Системы ИИ могут непреднамеренно обходить требования и ограничения, установленные существующими инструментами стратегического управления. Руководству следует обеспечить, чтобы системы ИИ явным образом соответствовали таким требованиям и ограничениям.

5.3 Экосистема ИИ

Понимание многочисленных компонентов системы ИИ и того, как они могут быть связаны с организацией, требует многослойного подхода к экосистеме ИИ.

Как показано на рисунке 1, экосистема ИИ обширна и включает в себя спектр различных технологий. Более подробная версия этого рисунка доступна в *ISO/IEC 22989:2022*, Рисунок 6, где более подробно описаны элементы МО и вычислительные ресурсы. Если используются средства реализации ИИ, некоторые из других компонентов этой экосистемы становятся функциональной частью общей системы ИИ и их следует рассматривать как таковые с точки зрения стратегического управления.

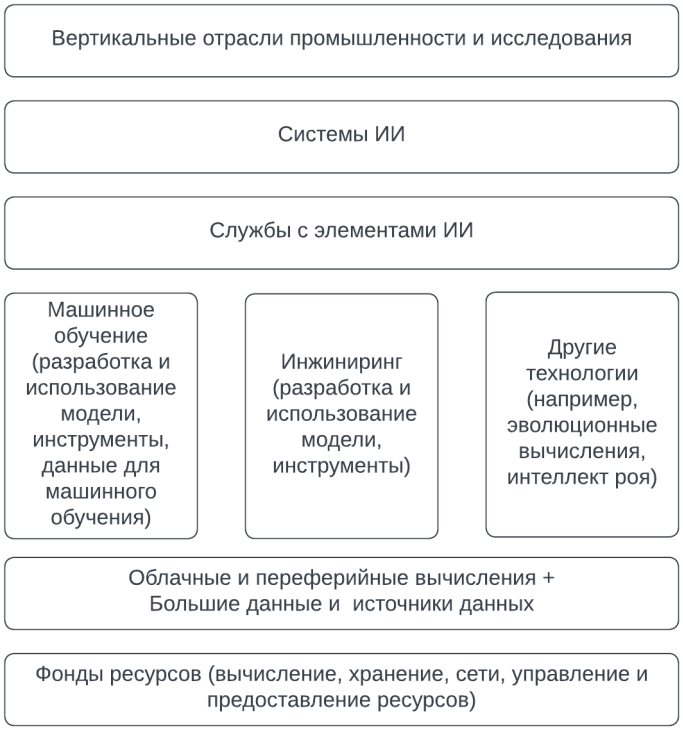

Рисунок 1 — Упрощенная версия экосистемы ИИ из *ISO/IEC 22989:2022*, Рисунок 6

Такое многослойное представление экосистемы ИИ может помочь определить уровень и объем подотчетности в зависимости от роли организации в экосистеме, а также соответствующий уровень подотчетности руководящего органа.

Сложная природа экосистем ИИ означает, что объем надзора будет сильно варьироваться в зависимости от нескольких факторов, включая:

- целевое назначение системы ИИ;
- тип используемого ИИ;
- функциональный слой используемой экосистемы ИИ;
- потенциальную пользу, которую принесет система ИИ;
- новые риски, которые могут сопровождать систему ИИ;
- этап внедрения системы ИИ;
- роль, которую играет организация в цепочке создания ценности ИИ (например, роль поставщика, производителя, потребителя ИИ).

См. *ISO/IEC 22989:2022*, 5.17).

На эти факторы влияют цель и задачи организации, а также решение об использовании системы ИИ в предпочтение другим информационным технологиям.

Эти факторы в основном учитываются в начале разработки и развертывания системы ИИ. Однако существуют и другие организационные соображения, которые следует учитывать на протяжении всего жизненного цикла.

На рисунке 2 показан жизненный цикл системы ИИ с момента зарождения до вывода из эксплуатации. После того как организация приняла решение об использовании ИИ, это может помочь руководящим органам определить точки или «ворота», на которых могут возникнуть ключевые вопросы стратегического управления, требующие решения со стороны руководящего органа.

Рисунок 2 — Модель жизненного цикла системы ИИ из *ISO/IEC 22989:2022*, Рисунок 3

С учетом жизненного цикла системы ИИ организация может начать понимать, как развивать существующие механизмы стратегического управления. Жизненный цикл может помочь определить, где требуется дополнительное стратегическое управление, учитывая зависимость системы ИИ от данных. Стратегическое управление данными рассматривается в стандартах серии ISO/IEC 38505. Жизненный цикл также может помочь руководящему органу определить на каждом этапе, где организация может быть подвержена дополнительным рискам, а затем принять решения о том, как управлять такими рисками. В разделах 5.4 и 5.5 более подробно

описаны дополнительные особенности по стратегическому управлению, возникающие при использовании ИИ.

5.4 Преимущества использования ИИ

Руководящий орган может рассмотреть вопрос о внедрении ИИ для реализации конкретных возможностей, выявленных организацией, включая будущий рост организации или более эффективное достижение целей и задач организации. В таких случаях руководящему органу необходимо сопоставить эти возможности с риском и другими последствиями использования. Ему следует обеспечить наличие и использование механизмов надзора для проверки того, соответствует ли развертывание стратегическому замыслу, целям и ценностям организации. ИИ можно использовать для достижения целей и создания ценности для организации. Это может привести к следующему:

- снижение операционных расходов,
- появлению новых продуктов и услуг, которые значительно изменят существующие способы ведения деятельности, или
- преобразование организаций, таких как государственные структуры или некоммерческие организации.

Сегодня практически все организации уже так или иначе используют ИИ в своей повседневной деятельности, порой даже не осознавая этого. Примерами такого использования могут служить:

- использование спутниковой навигационной системы, которая находит наиболее эффективный маршрут для грузоперевозок;
- большинство поисковых запросов в интернете используют ИИ для ответа на запрос, поиска схожей картинки или документа;
- офисные приложения используют ИИ, чтобы предложить лучший дизайн слайда в презентации или улучшить грамматику в документе.

Дальнейшее применение можно найти в различных областях (например, сельское хозяйство, оборона, образование, здравоохранение, производство, транспорт) и использовать различные модели развертывания (например, облачные услуги или системы на объектах, киберфизические системы). Обширная коллекция примеров использования включена в ISO/IEC TR 24030, охватывая эти и другие области и модели развертывания.

Система ИИ может, например:

- изменить характер продуктов, процессов и услуг;
- автоматизировать данных об обратной связи сбор, сравнение, перевод, проверку или анализ, оставляя за человеком деятельность, приносящую наибольшую полезную отдачу (например, выводы, которые нужно сделать, или решения, которые нужно принять);
- повысить уровень обслуживания клиентов, производительность и качество продукции;
- изменить отношения с клиентами и поставщиками (а значит, и между сотрудниками, клиентами и цепочками поставок) с помощью интеллектуальных агентов, таких как чат—боты, для сбора необходимой информации, сортировки и маршрутизации запросов, помощи в вопросах, связанных с продуктами, услугами или выставлением счетов, или решения задач;
- повысить эффективность в промышленности и сельском хозяйстве путем перехода от «автоматизированной помощи» к «полностью автоматической поддержке»;
- определить наиболее вероятное намерение говорящего на основе образцов разговорного языка;
- прогнозировать распространение болезней на основе исторических данных о подобных вспышках заболеваний;
- предположить возможный случай рака на основе изучения клеток;
- рекомендовать предоставление или отказ в предоставлении кредита.

Такое использование ИИ может принести пользу организации, но также может создать новые или обострить существующие проблемы, такие, например, как возникновение дополнительных риском или смещенность, вопросы, которые более подробно рассматриваются в п. 6.

Вооружившись искусственным интеллектом, организация может изменить свою стратегию и применить модели, подходящие для ее сектора. Организация может изменить то, каким образом она приносит пользу своим заинтересованным сторонам, и способы получения этой пользы. Использование ИИ также создает возможности для рабочей силы, например повышение творческого потенциала, мобилизуемого с помощью ИИ, повышение конкурентоспособности и различные возможности работы, исключающие повторяющиеся, тривиальные или небезопасные задачи. Таким

образом, технологии ИИ могут принести глубокие преобразования в организации. Руководящему органу следует узнать о возможностях, которые ИИ открывает для организации, и способствовать их внедрению, когда это целесообразно.

Используя ИИ для решения таких задач, организация может сосредоточить усилия и ресурсы на задачах, в которых полезная отдача зависит от усилий человека и не может быть автоматизирована или воспроизведена ИИ.

5.5 Ограничения на использование ИИ

Хотя организация может легко определить преимущества использования ИИ, руководящему органу следует понимать ограничения и обязательства, которые накладывает на организацию такое использование. Чтобы адекватно регулировать эти ограничения и обязательства, организации следует предпринять некоторые из следующих действий:

- Усилить надзор за соответствием требованиям. В отсутствие надлежащего контроля и надзора использование ИИ для автоматизации процессов может приводить к нестабильным результатам, которые сложно объяснить и воспроизвести, и которые могут противоречить политикам организации (см. 6.6).
- Рассмотреть сферу использования. Убедитесь, что сфера автоматизации контролируется руководящим органом и что автоматизация осуществляется соответствующим образом уполномоченным квалифицированным персоналом (см. 6.3). Руководящему органу следует обеспечить наличие необходимых полномочий, ответственности и подотчетности, а также изучить и понять последствия такой автоматизации до ее внедрения.
- Оценить воздействие на заинтересованные стороны и принять меры в случае необходимости. Хотя некоторые решения будут негативно влиять на заинтересованные стороны (например, отказ в банковском кредите клиенту), организации следует убедиться, что такое влияние не усугубится в результате использования ИИ. Следует позаботиться о сохранении как актуальности существующих оценок рисков и воздействий (см. 6.7), так и эффективности процессов их смягчения, таких как процессы защиты законных прав или обеспечения правовой определённости.
- Определить требования законодательства или обязательства по использованию такой технологии. Растёт вероятность того, что применение

ИИ и взаимосвязанных с ним таких решений, как распознание лиц или для автоматического управления транспортными средствами, может быть оспорено или же стать предметом новых требований законодательства. Руководящий орган должен продемонстрировать, как исполняются такие обязательства, и показать, что применение ИИ соответствует требованиям, а его результаты, где это требуется, должным образом объясняются.

- Согласовать использование ИИ с целями организации. Инновационное использование новых технологий имеет решающее значение для жизнеспособности и здоровья многих организаций, и в таких случаях политика стратегического управления будет поощрять такие инновации. Не каждый проект будет стратегически важным (например, некоторые только сократят расходы), но в целом следует то, чтобы использование ИИ помогало организации в достижении ее целей.
- Привести использование ИИ в соответствие с культурой и ценностями организации. Следует чтобы решения, предлагаемые системой ИИ, учитывали политику организации, ожидания (включая последствия использования) и этические нормы.
- Убедиться, что при решении задачи должным образом учитывается контекст. Организации необходимо обеспечить, чтобы элементы контекста, важные для понимания поведения, ценностей и культуры, не были потеряны или пропущены в данных, которые она использует для решения задач.
- Изучить дополнительный риск, который может принести организации использование ИИ. Изучив цель и задачи организации и рассмотрев возможные источники риска, выявленные в случае принятия решения об использовании ИИ, а также меры по обработке этих рисков, организации следует оставаться в рамках своего риск—аппетита (см. 6.7).

Помимо этих общих ограничений на использование ИИ организацией (и любых других, применимых к организации или ее заинтересованным сторонам), сами системы ИИ будут иметь технологические ограничения. Руководящему органу, занимающемуся вопросами стратегического управления, следует также получить от руководителей, отвечающих за оперативную деятельность, заверения в том, что обеспечивается адекватное управление такими ограничениями.

6 Политика в отношении использования ИИ

6.1 Общие положения

Системы ИИ используют данные для построения моделей и прогнозирования, а также потенциальной автоматизации решений и действий. Как и при любом использовании человеческих ресурсов, процессов или технологий, руководящий орган остается ответственным за эти решения и действия. Некоторое использование ИИ может непреднамеренно привести к несоответствию политике или к результатам, которые не были предусмотрены существующей политикой.

Выбор и утверждение направлений и средств управления, которые подходят для организации, не использующей ИИ, потенциально не подходят для организации, использующей ИИ.

Сохранение постоянного результативного стратегического управления требует проверки и возможного усиления существующих механизмов стратегического управления и средств управления для обеспечения их надежности, четкости и адекватности для учета дополнительных соображений стратегического управления (а также указаний руководству), которые системы ИИ привносят в организацию и ее заинтересованные стороны.

Руководящему органу и менеджерам следует дополнительно привлекать заинтересованные стороны, на которые может повлиять использование систем ИИ, такие как персонал и его представители, на протяжении всего процесса внедрения систем ИИ в организациях с помощью процедур информирования, консультаций и участия.

Руководящие указания в этом пункте призваны помочь руководящему органу понять и пересмотреть политику, которую ему следует рассмотреть, чтобы уменьшить возникновение предотвратимых и непреднамеренных последствий использования организацией ИИ. Оно не является и не может быть всеобъемлющим.

Согласно ISO/IEC TR 38502:2017, 4.1.3, менеджеры отвечают за обеспечение достижения целей организации в рамках стратегий и политики, установленных руководящим органом. Задача стратегического управления решается в тесном сотрудничестве между руководящим органом и менеджерами, как показано на рисунке 3.

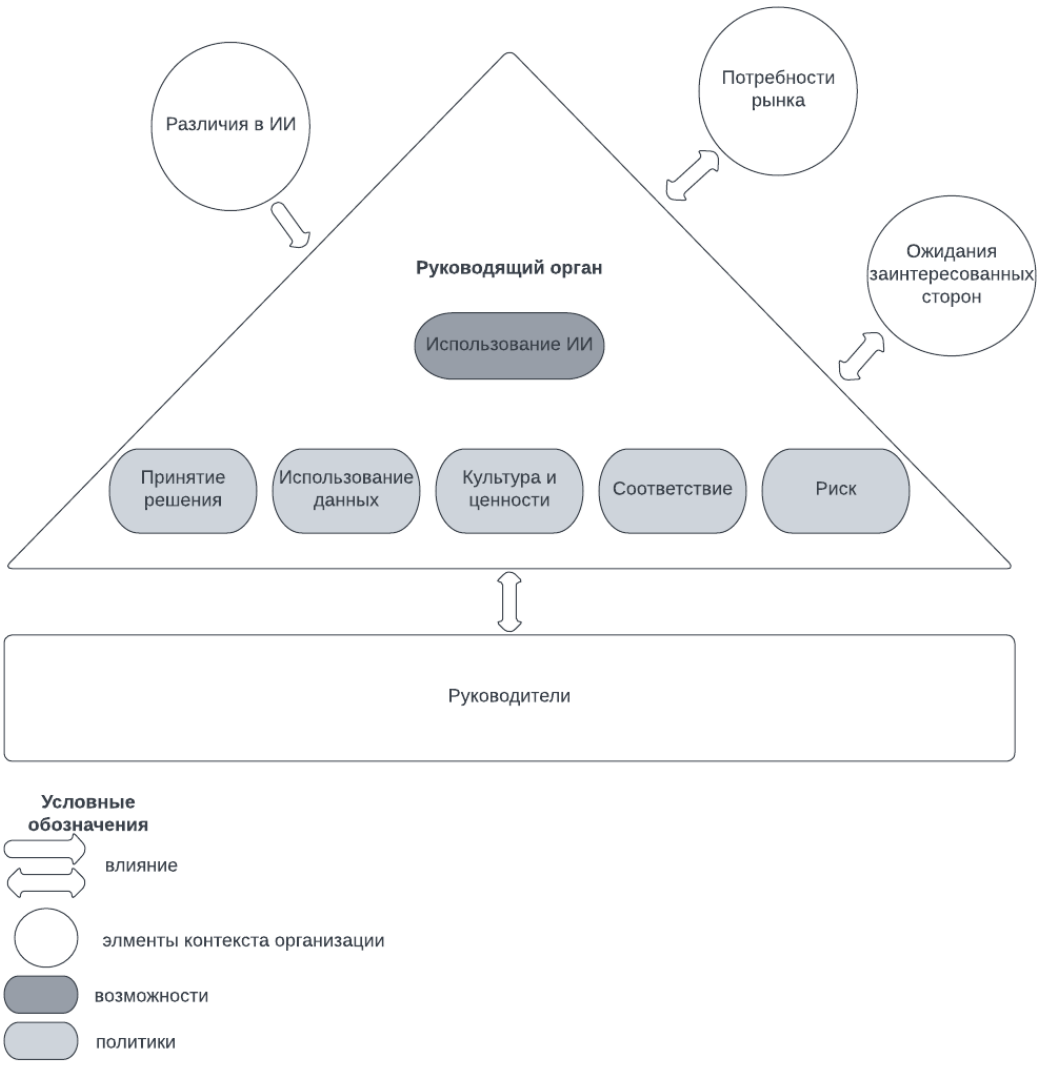

Рисунок 3 — Последствия влияния стратегического управления при использовании ИИ

Рисунок 3 основан на «Модели стратегического управления ИТ» в ISO/IEC 38500:2015, Рисунок 1, и модифицирует ее (воспроизведено на рисунке А.1).

Независимо от использования какой-либо технологии, руководящему органу следует устанавливать и контролировать достижение результатов, которые соответствуют его принципам. Такие принципы могут возникнуть внутри организации, быть предложены или навязаны внешними организациями (например, в [18], [19], [20] и [21]).

Следует чтобы скорость технологических инноваций и постоянно меняющиеся требования законодательства побуждали организацию активно поддерживать набор принципов использования ИИ и следить за тем, чтобы они оставались подходящими для использования ИИ в организации.

6.2 Надзор за стратегическим управлением ИИ

Руководящему органу следует обеспечить создание механизмов надзора за ИИ и их соответствие рискам, связанным с использованием ИИ в организации.

Следует чтобы надзор за стратегическим управлением, основанный на политике, установленной организацией, определял индивидуальную и коллективную подотчетность в цепи ответственности. Надзор за надлежащим стратегическим управлением следует основывать на общем понимании использования (и контекста использования) системы. См. «Внешний и внутренний контекст» в *ISO/IEC 23894:2023*, 6.3.33) и ISO 31000:2018, 6.3.3.

В рамках надзора за стратегическим управлением ИИ руководящему органу следует обеспечить то, что:

- разработаны политики, обеспечивающие надлежащее использование ИИ;
- обязанности, цепочка ответственности, подотчетность, полномочия и потенциальное делегирование полномочий четко определены и согласованы как внутри организации, так и, где это применимо, между различными сторонами в любой цепочке создания ценности;
- имеется адекватный контроль со стороны человека при использовании ИИ;
- любой человек, использующий ИИ или ответственный за использование ИИ:
  - имеет соответствующее представление об используемой системе ИИ;
  - надлежащим образом информирован и обучен, в том числе знает, как и кому эскалировать проблемы;
  - имеет полномочия принимать решения (или знает, к кому обратиться с запросом о принятии решения) и знает, перед кем отчитываться;
  - имеет достаточный контроль над системой ИИ, включая возможность вмешательства в случае необходимости.

6.3 Стратегическое управление процессом принятия решений

Стратегическое управление процессом принятия решений является частью общего стратегического управления организацией.

Полномочия и ответственность делегируются персоналу организации, чтобы распределить нагрузку от выполненной работы и принятых решений. Где бы ни находились такие делегированные полномочия или ответственность, подотчетность за всю проделанную работу и принятые решения остается за руководящим органом (см. 4.3). Некоторые из этих решений и часть этой работы могут все чаще приниматься и выполняться системами ИИ, но руководящий орган остается подотчетным таким же образом, как и в случае, когда человек принимает решения или выполняет работу.

Пересмотр политики принятия решений в отношении использования ИИ призван обеспечить, чтобы человек или группа людей несли и сохраняли четкую ответственность за решения, на принятие которых они делегировали полномочия и ответственность. Это происходит независимо от того, было ли решение частично или полностью автоматизировано.

Руководящему органу следует отслеживать типы решений и результатов, генерируемых автоматизированными системами, и направлять руководство на обеспечение того, чтобы такие системы были настроены на работу в приемлемых пределах путем внедрения соответствующих средств управления. Следует чтобы такие средства управления обеспечивали руководящему органу надлежащую видимость соответствия процесса принятия решений политике организации, а также любых исключений из нее.

Управляющему органу следует убедиться в том, что активный надзор за такими средствами управления делегирован сотруднику с соответствующими ресурсами, который имеет полномочия принимать или инициировать ответные меры на выявленные проблемы. Использование автоматизированного принятия решений, осуществляемого системой ИИ, не меняет подотчетности руководящего органа (или ответственности любого делегированного органа) за такие решения.

Важные факторы, связанные с принятием решений в организации, включают:

- Соответствие целям. Следует чтобы решения соответствовали целям организации, не выходя за рамки выделенных ресурсов, определенного риска и других средств управления, установленных организацией.
- Уровень ответственности. Обеспечение соответствия уровня принятия решений предоставленным полномочиям и ответственности, связанной с принятием решения, является важнейшим элементом надлежащего

стратегического управления. Определение масштабов и последствий возможных решений и соответствие их уровням ответственности необходимо для того, чтобы дать сотрудникам возможность действовать надлежащим образом и тем самым сделать всю организацию более гибкой. Подотчетность человека за действия и решения, выполняемые системой ИИ, следует четко определить и возложить на сотрудников, имеющих соответствующие полномочия и инструменты для выполнения поставленных перед ними задач (например, возможность визуального контроля, надзор, контроль качества) и для принятия достаточных корректирующих действий в случае выявления проблем.

- Способность принимать решения. Лицам, принимающим решения, следует иметь достаточные навыки и подготовку для принятия решений, за которые они отвечают. Должны быть внедрены средства управления для обеспечения адекватности систем ИИ поставленной перед ними задаче. См. ISO/IEC TR 24028.
- Процесс принятия решений. Заинтересованные стороны предъявляют все более высокие требования к прозрачности процесса принятия решений. Эта прозрачность включает требования к отчетности, стратегическое направление и взаимодействие со всеми внутренними и внешними пользователями. Вместе с повышением прозрачности растет и ожидаемый уровень вовлеченности и внимательности при принятии решений. Поэтому процессы принятия решений (вместе с действиями, необходимыми для смягчения последствий плохо принятых решений) являются важным механизмом стратегического управления и будут приобретать все большее значение по мере расширения использования ИИ.
- Надзор за принятием решений. Руководящему органу следует обеспечить надлежащий надзор, внедрение средств управления для обеспечения результативных возможностей принятия решений и надлежащую возможность визуального контроля как соответствия принимаемых решений политике организации, так и любых исключений. Для исключений в принятии решений, связанных с соответствием, следует определить необходимость в дополнительной прозрачности и подотчетности. Всем заинтересованным сторонам следует предоставлять соответствующие средства для выявления и сообщения о несоответствующем поведении или результатах принятия

решений в целом (независимо от того, включают ли они системы ИИ или нет), а также для получения значимого, своевременного и адекватного ответа.

6.4 Стратегическое управление использованием данных

Некоторые системы ИИ опираются на данные для построения и обучения модели, поэтому стратегическое управление использованием данных имеет решающее значение для ответственного использования ИИ. Руководящему органу следует на ранней стадии убедиться в том, что существующее стратегическое управление и руководство адекватны целям использования данных и что конфиденциальные данные защищены и обеспечены (см. ISO/IEC 38505—1). Это включает, например, документирование того, как организация соблюдает свои обязательства, в том числе в отношении закупок и продажи, конфиденциальности и безопасности, хранения и удаления данных, а также надзор за собственной политикой в отношении управления данными (см. также 6.7.4).

Дополнительные соображения по стратегическому управлению при использовании данных для систем ИИ включают:

- соответствующие проектные решения, принятые для системы ИИ;
- сбор данных;
- соответствующие операции по обработке подготовки данных, например, разметка, маркировка, очистка, обогащение и структурирование;
- формулирование соответствующих предположений, в частности, в отношении информации, которую данные, как предполагается, измеряют и представляют;
- предварительная оценка наличия, качества, количества и пригодности данных;
- экспертизы с учетом возможной смещенности;
- выявление любых возможных пробелов или недостатков данных, а также способов устранения этих пробелов и недостатков.

Одно из основных отличий систем ИИ (в частности, систем МО) от других ИТ-систем заключается в том, что они полагаются на вывод данных для получения результата с определенным уровнем достоверности. Вторым важным отличием является наличие и использование обучающих данных, которые, в зависимости от их качества, могут улучшить или ухудшить качество любого результата. Это отличается

от разработки программного обеспечения, которое рассчитано на людей, задумывающих и программирующих конкретные логические шаги, необходимые для получения результата. В подпунктах 5.2.2 и 5.2.3 описывается, чем отличаются такие системы. Поскольку качество данных имеет решающее значение для работы систем ИИ, руководящему органу следует получить от руководства заверения в том, что данные имеют необходимое качество для их предполагаемого использования в системах ИИ.

В зависимости от области применения, использование исторических данных для обучения системы ИИ может привести к:

- повторению предыдущих ошибок;
- принятию «необоснованных» решений в отношении результатов, не зафиксированных в данных;
- принятию решений в отношении новых комбинаций обстоятельств или данных, которые трудно понять человеку, например, связывание различных наборов данных, которые явно не связаны между собой;
- информации о наблюдении и поведении, которая не обязательно раскрывается добровольно;

Эти результаты лучше всего понимать как ошибки или погрешности, возникающие из—за использования неполных, ошибочных или несоответствующих данных. Иногда (и часто неверно) это называют «смещенностью ИИ». Однако смещенность вносится или усиливается людьми, а не самими системами ИИ (см. также 6.7.4).

В тех случаях, когда данные используются в системах ИИ, следует проверить существующие методы стратегического управления использованием данных и практики управления данными. Кроме того, для совместно используемых систем ИИ, например, для анализа отраслевой деятельности, может потребоваться дополнительная политика стратегического управления и средства управления со стороны руководства.

Другие технологические активы (например, алгоритмы, нейронные сети и системы обработки естественного языка) также могут потребовать аналогичных усовершенствований в существующих организационных и стратегических управленческих политиках.

Организации следует рассмотреть возможность применения положений ISO/IEC 38505—1, касающихся использования данных, к этим аспектам стратегического управления использованием ИИ:

- Ценность: качество и количество данных, их своевременность, контекст и стоимость их использования.
- Риск: безопасность данных, неправомерное использование и конфиденциальность, а также конкурентные риски, связанные с неэффективным использованием данных.
- Ограничения: требования законодательства, договорные обязательства, авторские или коммерческие интересы. См. также А.3 о стратегическом управлении использованием данных.

Данные и их использование организациями становятся все более важным вопросом для всех организаций и их заинтересованных сторон. В соответствии с принципами, моделями и специфическими для данных аспектами стратегического управления, изложенными в ISO/IEC 38505—1, руководящим органам следует предпринимать действия, обеспечивающие результативное стратегическое управление и инвестиции в использование данных организацией, а также учитывать риски, связанные с этим использованием. Это включает в себя обеспечение того, что правильные данные используются для правильных целей.

6.5 Культура и ценности

Руководящий орган отвечает за определение желаемой культуры и ценностей организации в отношении заинтересованных сторон, рынков и регулирующих органов, а также изменений в ожиданиях общества в отношении деятельности и воздействия организации. Руководящим органам следует знать о появляющихся рекомендациях и международных нормах поведения, таких как те, что отражены во Всеобщей декларации прав человека [22], Йоханнесбургской декларации по устойчивому развитию [23] и других документах. Более подробную информацию можно найти в ISO 26000:2010, 3.3.2.

Любому решению или действию организации следует соответствовать ее культуре и ценностям. Однако большая часть культуры и ценностей организации неявно заложена в поведении ее сотрудников и процессах. Система ИИ не имеет эквивалента человеческого понимания контекста, здравого смысла, морали или

знаний, чтобы направлять свои действия. Вместо этого система ИИ полагается на модели, алгоритмы или обучающие данные для достижения сопоставимых результатов.

По этим причинам руководящему органу следует четко определить свою культуру и ценности и иметь соответствующие механизмы и политику стратегического управления, чтобы обеспечить отслеживание и корректировку такого поведения системы ИИ в случае необходимости. В некоторых случаях следует чтобы масштабы и воздействие системы ИИ были ограничены и дополнены действиями человека, чтобы можно было обеспечить соблюдение политики стратегического управления. Как этого добиться, будет зависеть от обстоятельств. В равной степени система ИИ может помочь выявить, где в принятии решений человеком есть недостатки (например, неуместная смещенность или дискриминация, или плохое рассуждение или дедукция) и таким образом дать представление для организации, которое руководящий орган может впоследствии рассмотреть. Это поднимает будущие проблемы стратегического управления организациями.

В зависимости от характера и цели предполагаемой к использованию системы ИИ, возможно, что организации потребуется осуществлять явный надзор за этими системами, чтобы обеспечить их соответствие культуре и ценностям организации. Механизмы стратегического управления могут принимать форму «Совета по культуре и ценностям» или «Совета по рассмотрению вопросов этики». Надзор может заключаться в том, что перед утверждением чувствительных или высокорискованных проектов систем ИИ или при соблюдении определенных критериев эскалации необходимо провести проверку. Дополнительные политики организации в этой области могут требовать использования технических средств управления в системе ИИ для обеспечения соответствия этим политикам. Более подробную информацию об этике и общественных проблемах, связанных с использованием ИИ, см. в ISO/IEC TR 24368.

6.6 Соответствие требованиям

6.6.1 Принятые обязательства

Для обеспечения выполнения организацией принятых ей обязательств организация устанавливает постоянный процесс обеспечения соответствия

требованиям. Чтобы быть результативным, процесс обеспечения соответствия формируется руководством организации и внедряется в культуру организации. Система менеджмента соответствия, подобная описанной в стандарте ISO 37301, отвечает этим требованиям и помогает организации продемонстрировать свою приверженность выполнению обязательств и соответствовать ожиданиям заинтересованных сторон.

Руководящему органу следует получить гарантии того, что руководство настраивает и обслуживает любую систему ИИ, используемую организацией, для выполнения принятых организацией обязательств и во избежание нарушения соответствия требованиям. Примерами нарушений являются механизмы ценообразования, нарушающие антимонопольные требования законодательства, или использование данных для обучения, нарушающее гражданские права или носящее дискриминационный характер.

Соответствие требованиям касается поведения операционного персонала. ИИ может уменьшить влияние человеческого поведения в определенных ситуациях, тем самым снижая риск несоответствия, которое является результатом человеческого поведения. Как следствие, влияние человеческого фактора теперь повышается или смещается в сторону тех, кто проектирует, разрабатывает и внедряет системы ИИ. Такое изменение ставит совершенно новую задачу в плане осведомленности, обучения и отслеживания.

При рассмотрении роли ИИ в контексте организации и ее принятых обязательств руководящему органу следует рассмотреть эти вопросы:

- ожидания заинтересованных сторон относительно использования и влияния ИИ (убедитесь, что они соответствуют существующим политикам и принятым обязательствам);
- культурные последствия использования ИИ в организации, такие как повышенная сложность системы ИИ, которая может заставить сотрудников считать, что она не содержит ошибок. Организации следует установить соответствующие процессы для проверки результатов работы системы ИИ;
- степень использования ИИ в организации;
- влияние ИИ на соблюдение требований организации;
- изменения в риск—аппетите организации, возникающие в результате использования ИИ;

- степень, с которой существующие надзорные процессы, структуры и средства управления учитывают конкретные аспекты ИИ;
- влияние использования ИИ на структуры подотчетности в организации;
- следует, чтоб существующая система менеджмента соответствия была оценена с учетом последствий, связанных с использованием ИИ (когда, например, проекты и решения могут быть трудно объяснимы и подвержены частым изменениям), что может включать, например, расширение политики соответствия или расширение периодической оценки рисков;
- затрагиваются ли физические лица в результате использования или создания персональных данных системой ИИ, которая ограничена, например, законом или политикой организации.

6.6.2 Менеджмент соответствия

Использование стандарта системы менеджмента соответствия позволяет организации интегрированно совместить в своей системе менеджмента специфические требования к менеджменту, например, к безопасности, качеству и конфиденциальности. Это облегчает добавление дополнительных мер по обеспечению соответствия в систему менеджмента, возникающих в результате использования ИИ.

На уровне менеджмента соответствия особое внимание следует уделять следующему:

- расширение процессов обеспечения соответствия с учетом скорости, масштаба или сложности системы ИИ (например, для повышения уровня или частоты отслеживания);
- запросы на повторную оценку человеком решений, принятых системой ИИ;
- дополнительные средства управления для обеспечения того, чтобы системы ИИ оставались в требуемых условиях соответствия;
- обеспечение соответствия политике использования данных для построения моделей или обучения;
- использование ИИ для отслеживания других систем ИИ и дополнительное отслеживание или оповещение, которые могут потребоваться.

Организации следует оценить влияние любого запланированного использования ИИ с помощью системы менеджмента соответствия. Следует чтобы возможные

варианты использования ИИ в рамках системы менеджмента были частью этой оценки.

6.7 Риск

6.7.1 Аппетит к риску и управление рисками

Стратегическое управление организацией, каким бы образом оно ни осуществлялось, включает в себя определение цели и задач организации, а также стратегии их достижения. При рассмотрении своей стратегии руководящий орган организации принимает решение о риск-аппетите, преследуя свои цели. Чтобы оставаться в рамках этого риск-аппетита и помочь руководящему органу в принятии решений относительно риск-аппетита организация устанавливает процесс управления рисками.

Управление рисками предполагает сбор соответствующей информации для принятия организацией решений в отношении рисков. Хотя руководящий орган определяет общий риск-аппетит и цели организации, он делегирует процесс принятия решений по выявлению, оценке и учету риска руководству организации. Различные роли стратегического управления и менеджмента в решении проблемы риска обсуждаются в следующих документах:

- настоящий стандарт, в котором описаны дополнительные соображения по стратегическому управлению организацией в отношении разработки, приобретения или использования системы ИИ. Такие соображения включают новые возможности, потенциальные изменения в риск-аппетите, а также новые политики стратегического управления для обеспечения ответственного использования системы ИИ в организации;
- ISO/IEC 23894, который описывает процессы управления, которые следует выполнять в организации для устранения дополнительных рисков для организации в результате внедрения системы ИИ.

В работе с рисками участвуют как руководящий орган, который определяет риск-аппетит и несет за него ответственность, так и руководство, которое работает над поддержанием риска в пределах согласованного риск-аппетита.

В ходе проверки текущих процессов управления рисками следует особенно тщательно изучить, хорошо ли понимаются и управляются риски, связанные с

принятием решений, использованием данных, культурой и ценностями, а также с соответствием нормативным требованиям. Таким образом, можно прояснить контекст дополнительных рисков, которые системы ИИ привносят в организацию. Как только эти дополнительные риски будут определены, руководящий орган окажется в более выгодном положении для того, чтобы:

- обеспечить адекватный учет рисков при постановке целей организации;
- понимать риски, с которыми сталкивается организация при достижении своих целей;
- обеспечить внедрение и результативное функционирование систем управления такими рисками;
- обеспечить, чтобы такие риски находились в рамках риск—аппетита организации;
- обеспечить результативное распространение информации о таких рисках и управлении ими (используя, например, ISO 31000:2018, 5.2).

6.7.2 Управление рисками

Управление рисками является неотъемлемой частью всей деятельности организации. Хотя системы ИИ могут принести пользу организации, цели организации, связанные с надлежащим стратегическим управлением процессом принятия решений, использованием данных, а также с желаемой культурой и ценностями организации, следует пересмотреть с учетом возможных последствий использования ИИ.

Организация стремится защитить свои принципы и ценности, свою идентичность и репутацию, своих заинтересованных лиц, свой рынок, свою окружающую среду и, кроме того, защитить свою свободу действий, чтобы добиться успеха.

Для устранения рисков, связанных с ИИ, руководящему органу следует создать:

- соответствующие внутренние правила и политики;
- соответствующие конкретные структурные подразделения, процессы и инструменты, призванные гарантировать или обеспечить соблюдение ценностей, принципов и внутренних средств управления, которые являются основой надлежащего стратегического управления.

Кроме того, руководящему органу следует обеспечить то, чтобы подрядчики и субподрядчики организации соблюдали те же кодексы практики и политики.

Эти меры дают возможность любой заинтересованной стороне выявлять и сообщать о несоответствующем поведении системы ИИ и получать конструктивные и адекватные ответы. Они особенно важны там, где задействованы сложные цепочки поставок и где репутационный, финансовый или иной риск может быть возложен на ведущего подрядчика или закупщика. Организации следует получить четкое представление о последствиях использования ИИ в рамках договорных отношений, в которых задействованы риск-аппетиты различных организаций.

Рисунок 4 демонстрирует следующие примеры:

- цели, которые преследует организация (например, защита репутации);
- дополнительные источники риска, которые может привнести в организацию использование ИИ;
- некоторые технические и организационные средства управления, которые могут быть использованы для устранения рисков.

Рисунок 4 — Управление рисками при использовании ИИ

6.7.3 Цели

Цели, которые организация хочет защитить с помощью процессов управления рисками, включают в себя не только защиту активов, таких как данные, информационные системы, код приложений, алгоритмы и оборудование, но и ее обязанности проявления заботы культуру и ценности, репутацию и стратегию.

На рисунке 4 показаны примеры целей, которые преследует организация:

- Подотчетность и ответственность. Руководящему органу следует поддерживать подотчетность, а также надзор за выполнением организацией своих обязанностей как внутри, так и за пределами организации в отношении использования ИИ.
- Репутация и доверие. Рассматриваемый здесь риск относится к самой организации. Однако организация не существует изолированно, поэтому должны быть рассмотрены ее заинтересованные стороны и среда, в которой она работает. Следует чтобы последствия и вероятность рисков, влияющих на заинтересованные стороны, такие как клиенты и поставщики, были ключевыми соображениями с точки зрения риска для организации.
- Обязанность проявлять заботу. Организация несет ответственность и, возможно, законодательную обязанность заботиться о своих заинтересованных сторонах, как внутренних, так и внешних. Это может включать обязательство (с нормативными или правовыми последствиями, в зависимости от юрисдикции) обеспечить благополучие всех заинтересованных сторон и защиту их прав, например, доступ к значимым финансовым, медицинским или жилищным услугам, а также прав человека (включая свободу передвижения или неприкосновенность частной жизни).
- В ситуациях, когда существует значительный риск, связанный с обязанностью проявлять заботу, руководящему органу следует потребовать дополнительные организационные средства управления для результативного отношения к таким рискам и обеспечения того, чтобы они не превышали риск—аппетит организации (примеры см. в разделе 6.7.5).
- Безопасность. В тех случаях, когда использование системы ИИ сопряжено со значительным риском причинения физического или эмоционального вреда, организации следует быть особенно внимательна к характеру и последствиям такого вреда. При необходимости организации следует внедрить соответствующие системы для постоянного управления безопасностью, а также рассмотреть вопрос о том, как использование ИИ может снизить подверженность людей опасным видам деятельности.
- Безопасность и конфиденциальность. Организации следует обеспечивать безопасность своей операционной деятельности, особенно в тех случаях, когда необходима конфиденциальность и важна неприкосновенность частной жизни. Эти цели не следует менять при использовании ИИ, особенно

учитывая способность систем ИИ производить новую информацию из закономерностей в данных.

- Данные. Данные являются важным ресурсом для организации, и их защите и целостности следует быть целью организации.
- Прозрачность. Прозрачность принятия решений организацией, вероятно, будет целью, которую руководящий орган желает поддерживать. Заинтересованные стороны ожидают понимания хотя бы некоторых важных исходных данных и переменных, которые объясняют, как организация принимает решения. Это происходит независимо от того, насколько автоматизировано принимается решение.

Некоторые из этих целей подробно рассматриваются в ISO/IEC TR 24368 и ISO/IEC TR 24028, а также в ISO 31050.

6.7.4 Источники риска

Организации следует ожидать появления дополнительных источников риска в зависимости от масштаба и характера области, к которой применяется система ИИ, и типа развернутой системы ИИ. Некоторые виды использования ИИ будут сдерживаться и контролироваться, что приведет к незначительному или отсутствию дополнительного риска для организации. Другие виды использования будут нести значительные риски, которых раньше в организации не было.

Кроме того, как указано в ISO/IEC 23894, менее зрелые технологии, например, используемые при разработке и применении систем ИИ, могут создавать риски, которые неизвестны организации или которые трудно оценить. С другой стороны, для зрелых технологий может быть доступно большее разнообразие данных об опыте, что облегчает выявление и оценку рисков. Набор «уровней готовности», характеризующих зрелость системы ИИ, может быть полезен для оценивания и отслеживания рисков.

Прямое сопоставление активов, ценностей и целей с источниками риска или средствами управления рисками невозможно, поскольку влияние любого из этих элементов может повлиять на любой другой элемент.

Примеры источников риска, показанные на рисунке 4, относятся к использованию ИИ, хотя эти источники могут быть применимы и ко многим другим технологиям или процессам. Организации следует ожидать появления дополнительных источников

риска в зависимости от масштаба и характера используемых систем ИИ. Приведенные примеры включают:

- Поиск источников данных. Поскольку данные используются для построения и обучения модели в системе МО, качество и адекватность данных имеют решающее значение и им следует соответствовать предполагаемому использованию и целям системы. Данные, подвергнутые манипуляциям, могут допустить состязательные атаки, что приведет к отравлению модели и неправильной классификации.
- Неясные условия. При традиционной разработке программного обеспечения характер задачи и ее решение тесно связаны, поскольку люди, вовлеченные в процесс, используют схожие подходы для решения обеих задач. Однако система ИИ может прийти к решению совершенно другим способом спустя долгое время после того, как система была первоначально спроектирована и разработана, поэтому точность, ясность и объем условий задачи, системные требования, цели системы и границы поведения могут играть важную роль.
- Цепочка создания ценности. Поставка и распространение систем ИИ может включать риски, так же как и использование систем ИИ теми, кто находится за пределами организации. Следует чтобы подотчетность была четко определена и согласована между различными сторонами в цепочке создания ценности.
- Нежелательная смещенность. Алгоритм, обучающие и тестовые данные, а также модель МО, используемые в системах ИИ, часто нацелены на отражение и предсказание ситуаций реального мира. По своей природе эти системы представляют собой лишь небольшую выборку или перспективу и могут давать результаты, которые отражают выборку, а не реальный мир. Это может привести к усилению нежелательной смещенности. См. *ISO/IEC TR 24027:2021*.
- Отсутствие объяснимости МО. Риск возникает из—за сложности систем ИИ. Это может сделать очень трудным объяснение того, как система ИИ пришла к определенному выводу. Это отличается от традиционных ИТ—систем, где человек определяет алгоритмическую процедуру для определения ответа. Человека можно опросить, перепроверить, оценить его положение и репутацию, привлечь к ответственности и протестировать любой код, чтобы убедиться, что он дал предсказанные ответы.

- Отсутствие опыта в области ИИ. Использование ИИ требует навыков, отличных от традиционной разработки программного обеспечения, хотя эти навыки также необходимы. Дополнительные навыки включают в себя понимание аналитики данных и статистики, моделирования, разработки и тестирования алгоритмов, а также навыков работы с людьми, таких как этика и эмпатия.
- Киберугрозы. Внедрение некоторых систем ИИ может быть уязвимо для отдельных и трудно распознаваемых киберугроз, которые оставляют после себя мало заметные следы или вообще не оставляют их.

Другие источники риска связаны с использованием ИИ и его косвенным воздействием на человека. Например:

- Утрата навыков. Все более широкое использование ИИ в рутинных ролях по принятию решений означает, что люди со временем все меньше подвергаются воздействию опыта. Сокращение опыта сотрудников («атрофия агентов») лишает человека возможности совершенствовать свои навыки, способности принимать решения и опыт. Такое вытеснение развития человеческих навыков представляет собой риск для организаций и общества в целом.
- Договорные вопросы. Руководящему органу следует обеспечить то, чтобы применимые договоры, законы и передовая практика оставались в силе при использовании систем ИИ. Во многих приложениях системы ИИ учатся на основе данных и практики принимающей их организации, на начальном и потенциально постоянном уровне. Это уникальным образом делает системы ИИ отражением организации, которую они обслуживают, что может повлиять на применимость договоров, законов и передовой практики.
- Экологические вопросы. Руководящему органу следует рассмотреть риск выбросов углекислого газа в результате потребления энергии для обучения ИИ и обработки данных. Ему также следует учитывать риск загрязнения окружающей среды и истощения ресурсов из—за ускоренного устаревания аппаратного обеспечения в пользу более новых облачных и переферийных устройств с поддержкой ИИ.
- Личная автономия. Использование ИИ все чаще может определять диапазон выбора, с которым сталкиваются люди в плане новостей, развлечений, взаимодействий, продуктов и услуг. Несмотря на то, что по отдельности эти

решения незначительны, растущая частота и повсеместное распространение этих решений означает, что руководящему органу следует рассмотреть влияние использования ИИ на автономию человека как личности, так и в составе сообщества.

- Упущенные возможности. Руководящие органы иногда слишком консервативны, чтобы воспользоваться новыми возможностями. Если руководящий орган не использует возможности, которые открывает использование ИИ, организация может столкнуться с усилением конкуренции со стороны организаций, которые используют такие возможности.

6.7.5 Средства управления

Средства управления направлены на поддержание или изменение рисков таким образом, чтобы они оставались в пределах риск—аппетита организации. Эти средства управления могут быть организационными средствами управления, например, осуществляемыми через управленческие структуры, наблюдательные советы или процессы управления, или техническими средствами управления, которые реализуются с помощью таких мер, как ограничения доступа к базе данных, программному коду или фильтрации данных.

Средства управления, показанные на рисунке 4, — это лишь небольшая часть тех, которые могут быть связаны с системами ИИ.

На рисунке 4 приведены следующие примеры средств управления рисками:

- Применимость. Следует чтобы описание системы ИИ, включая, например, ее алгоритмы, данные и модели, были достаточно прозрачным, чтобы обеспечить ее применимость для предполагаемого использования.
- Экспертный совет по этике. Для приложений, для которых организация определила высокий риск, высокое воздействие на заинтересованные стороны или другие пороговые значения, общим средством управления рисками является использование экспертного совета по этике, который может обеспечить соответствие культуре и ценностям организации.
- Процессы управления. Разработка и внедрение процессов управления является обычной практикой для решения таких требований, как качество, безопасность, конфиденциальность и соответствие. Аналогичные процессы могут быть разработаны для требований, связанных с системой ИИ.

- Технические средства управления. Технические средства управления, встроенные в программное обеспечение, могут осуществлять действия, помогающие справиться с некоторыми рисками. См., например, ISO/IEC TR 24029—1.
- Обучение и подготовка. Каждому человеку, участвующему на всех этапах использования ИИ, следует пройти соответствующую подготовку, чтобы обеспечить приобретение и применение необходимых навыков.

Приложение А
(обязательное)
Стратегическое управление и принятие организационных решений

А.1 Обзор соответствующих стандартов стратегического управления

А.1.1 Общие положения

ISO 37000 описывает стратегическое управление организациями как систему, с помощью которой организация направляется, контролируется и отвечает за достижение своей цели.

В его основе лежат:

- определение цели, миссии, видения, организационного духа, организационных ценностей и культуры, чтобы задать организации направление;
- следование стратегии и надлежащее распределение ресурсов для достижения этой цели;
- осуществление надзора за деятельностью организации, обеспечение соответствия и жизнеспособности;
- взаимодействие с заинтересованными сторонами и ведение отчетности перед ними.

В области информационных технологий «стратегическое управление» определено в ISO/IEC 38500:2015 как «система управления и контроля» организации через три основные задачи оценки, управления и отслеживания использования ИТ.

А.1.2 Направление

ISO/IEC 38500:2015 содержит руководящие указания для руководящих органов по распределению ответственности за стратегии и политику, которые определяют направление инвестиций в ИТ и то, чему ИТ следует достичь. Им следует поощрять культуру надлежащего стратегического управления ИТ в своей организации и

руководить подачей предложений на утверждение для удовлетворения выявленных потребностей (см. рисунок А.1).

Рисунок А.1 — Модель стратегического управления ИТ (из ISO/IEC 38500:2015)

А.1.3 Подотчетность

Руководящий орган организации несет ответственность за решения, действия и бездействие всей организации и подотчетен заинтересованным сторонам организации. Эта подотчетность не может быть делегирована.

Организация использует людей, процессы и технологии для достижения своей цели, и, независимо от используемых ресурсов, руководящий орган остается ответственным за результаты деятельности организации. Например, руководящий орган может нести ответственность и быть привлечен к ответственности за неправомерное использование сотрудниками ИТ—оборудования, если считается, что

в организации не было достаточного руководства, обучения, надзора и правоприменения для предотвращения такого неправомерного использования. Руководящий орган может подвергнуться аналогичному риску в результате недостаточного стратегического управления использованием ИИ.

«Приемлемое использование ИИ» определяется заинтересованными сторонами организации в различных контекстах, в которых они работают, и это «приемлемое использование» может варьироваться в разных контекстах. Именно в процессе взаимодействия с заинтересованными сторонами организация может понять, что означает «приемлемое использование», и воплотить эти требования в организационной политике. Такая политика будет отражать не только применимые требования законодательства, но и ожидания общества.

Взаимодействие с заинтересованными сторонами, являющееся ключевым принципом стратегического управления организациями, требует, чтобы организация поддерживала разумное взаимодействие с заинтересованными сторонами для обеспечения того, чтобы организация создавала выгоду в течение длительного времени и делала это способом, приемлемым для этих заинтересованных сторон. Эти отношения могут требовать законодательных или моральных обязательств, а также соответствия нормам или ожидаемому поведению общества, экономики и окружающей среды, в которых работает организация.

А.1.4 Надзор

ISO 37000:2021, 6.4.1 гласит, что руководящему органу следует осуществлять надзор за деятельностью организации, чтобы гарантировать, что она соответствует намерениям руководящего органа и ожиданиям от организации, ее этическому поведению и принятым обязательствам.

Организационная политика отражает применимые законодательные и общественные обязательства. Они также включают политику, которая настраивает и стимулирует организацию к достижению ее целей. Для того чтобы оставаться ответственным перед своими заинтересованными сторонами, руководящий орган использует соответствие организационной политики как средство сохранения результативного контроля над организацией.

Руководящий орган также несет ответственность за определение характера и степени рисков, с которыми организация готова столкнуться при достижении своих целей. После определения риск-аппетита он осуществляет надзор за надлежащим

управлением этим риском и любым смягчением, необходимым для того, чтобы риск-аппетит не был превышен.

Надлежащий надзор также гарантирует, что руководящий орган обеспечивает надлежащий организационный потенциал для выполнения своих задач, защиты интересов организации и заинтересованных сторон и выявления новых возможностей.

А.2 Руководство руководящего органа в отношении управленческих решений

Руководящий орган устанавливает цель и другие параметры организации и несет ответственность за всю организацию. Руководящий орган решает, какие параметры установить, и они будут разными в разных организациях. Как правило, такие параметры могут включать (формально или неформально) следующее:

- Стратегические решения, включая рынки для обслуживания, продукты и услуги для предоставления.
- Вовлечение заинтересованных сторон для определения инвестиций, ожидаемого поведения, культуры и ценностей.
- Риск-аппетит, определяющий характер и степень рисков, которые организация готова принять на себя для достижения своих целей.

Роль руководства заключается в эффективном и результативном достижении целей организации в рамках этих параметров.

Разграничение и прозрачность ролей руководства и стратегического управления имеют решающее значение для успеха организации. Эти роли предполагают разную ответственность и требуют разного набора навыков. Их разделение дает им четко определенную свободу для инноваций и предпринимательства. Взаимодействие между ролями обеспечивает необходимые средства управления для защиты организации. Например, если руководство видит новые возможности или риски, которые выходят за рамки стратегии или риск—аппетита, ему следует предложить изменить соответствующие параметры. Затем руководящий орган решает, соответствует ли изменение этих параметров наилучшим интересам организации и ее заинтересованных сторон.

Хотя каждая из этих ролей является отдельной, несколько ролей могут выполняться одним и тем же лицом, при условии, что между ними нет конфликта

интересов и что это лицо осознает отдельную ответственность, которую влечет за собой каждая роль. Например, член высшего руководства может также быть членом руководящего органа. Однако важно, чтобы эти роли оставались отдельными, и чтобы человек в любой момент времени осознавал, какую роль он выполняет.

А.3 Стратегическое управление использованием данных

ISO/IEC 38505—1:2017, пункт 5, выделяет следующие аспекты стратегического управления, специфичные для данных:

- Ценность. Данные — это сырье для получения полезной информации. Некоторые данные потенциально бесполезны, в то время как другие данные чрезвычайно ценны для организации. Однако эта ценность неизвестна до тех пор, пока она не используется организацией, поэтому все данные представляют интерес для руководящего органа, который в конечном итоге несет за них ответственность. Термин «ценность» в данном случае также включает в себя качество и количество данных, их своевременность, контекст (который сам по себе является данными) и стоимость их хранения, обслуживания, использования и утилизации.
- Риск. Различные классы данных и типы обработки влекут за собой различные уровни риска, и руководящему органу следует понимать риски, связанные с данными, и то, как руководителям управлять этими рисками. Риски проявляются не только в нарушениях данных, но и в неправильном использовании данных и возникающих в связи с этим репутационных рисках.
- Ограничения. Большинство данных сопровождается ограничениями на их использование. Некоторые из них накладываются на организацию извне через законодательство, нормативные акты или договорные обязательства и включают вопросы, например, конфиденциальности, авторского права, коммерческих интересов. Другие соображения включают этические или общественные обязательства, или политику организации, которая ограничивает использование данных. Стратегии и политики должны учитывать эти ограничения при любом использовании данных организацией.

Приложение ДА
(справочное)
Сведения о соответствии ссылочных национальных стандартов ссылочным международным стандартам, использованным в качестве ссылочных в примененном международном документе

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального и межгосударственного стандарта
ISO/IEC 22989:2022, Information technology — Artificial intelligence — Artificial intelligence concepts and terminology	NEQ*	ПНСТ 553–2021** Информационные технологии. Искусственный интеллект. Концепции искусственного интеллекта и терминология (ISO/IEC DIS 22989, NEQ)
ISO/IEC 38500:2015, Information technology — Governance of IT for the organization	IDT	ГОСТ Р ИСО/МЭК 38500—2017 Информационные технологии. Стратегическое управление ИТ в организации

* В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:

- IDT — идентичный стандарт;
- NEQ — неэквивалентный стандарт.

** В России принят предварительный национальный стандарт, основанный на ранней редакции международного стандарта

Библиография

[1] ISO Guide 73:2009, Risk management — Vocabulary

[2] ISO/IEC 23894:2023, Information technology — Artificial intelligence — Risk management

[3] ISO/IEC TR 24027, Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making

[4] ISO/IEC TR 24028, Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence

[5] ISO/IEC TR 24029—1, Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview

[6] ISO/IEC TR 24030, Information technology — Artificial intelligence (AI) — Use cases

[7] ISO/IEC TR 24368:2022, Information technology — Artificial intelligence — Overview of ethical and societal concerns

[8] ISO 26000:2010, Guidance on social responsibility

[9] ISO 31000:2018, Risk management — Guidelines

[10] ISO 31050, Guidance for managing emerging risks to enhance resilience

[11] ISO 37000:2021, Governance of organizations — Guidance

[12] ISO 37301:2021, Compliance management systems — Requirements with guidance for use

[13] ISO/IEC TR 38502:2017, Information technology — Governance of IT — Framework and model

[14] ISO/IEC 38505—1:2017, Information technology − Governance of IT − Governance of data − Part 1: Application of ISO/IEC 38500 to the governance of data

[15] ISO/IEC TR 38505—2, Information technology − Governance of IT − Governance of data − Part 2: Implications of ISO/IEC 38505—1 for data management

[16] ISO/IEC TS 38505—3, Information technology — Governance of IT — Governance of data — Part 3: Data Classification

[17] ISO/IEC 38506, Information technology — Governance of IT — Application of ISO/IEC 38500 to the governance of IT enabled investments

[18] Secretariat J.C. Social Principles of Human—Centric AI, March 2019 [viewed January 2021]. Available from: https://www8.cao.go.jp/cstp/english/humancentricai.pdf

[19] OECD The OECD Principles on AI, May 2019 [viewed January 2021]. Available from https://www.oecd.org/going-digital/ai/principles/

[20] European Commission. Ethics Guidelines for Trustworthy Artificial Intelligence (AI), April 2019 viewed January 2021]. Available from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

[21] Government of Singapore. Model Artificial Intelligence Governance Framework, Second Edition, January 2020 [viewed January 2021]. Available from https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf

[22] United Nations Universal Declaration of Human Rights [viewed October 2021]. Available from https://www.un.org/en/about-us/universal-declaration-of-human-rights

[23] United Nations Johannesburg Declaration on Sustainable Development, World Summit on Sustainable Development, 2002 [viewed October 2021]. Available from http://www.un-documents.net/jburgdec.htm

ПНСТ
(проект)

УДК 004.01:006.354 ОКС 35.020

Ключевые слова: ИИ, искусственный интеллект, руководящий орган, стратегическое управление

Руководитель разработки

Председатель совета директоров
Института развития информационного общества,
академик Российской инженерной академии

Ю.Е. Хохлов

Исполнитель

П.В. Степанов