Impact Factor: 9.9 ISSN-L: 2544-980X

Критерии Оценки Эффективности Искусственного Интеллекта, Внедренного В Корпоративное Управление

Ж. И. Юлдашев [1]

Аннотация: в данной статье были раскрыты положительные и отрицательные ситуации, возникающие при внедрении искусственного интеллекта в корпоративное управление, и правовая сторона их мониторинга. В статье дана правовая оценка критериям оценки эффективности применения искусственного интеллекта в корпоративном управлении. В то же время по этому вопросу автор также высказал свое мнение.

Ключевые слова: корпоративное управление, искусственный интеллект, современные технологии, проведение собраний, голосование, принятие решений, информация о личности, информационная безопасность, мониторинг, общественный контроль.

Внедрение искусственного интеллекта в корпоративное управление и применение эффективных современных технологий в корпоративной деятельности имеет важное значение. Он помогает в анализе данных, автоматизации процессов и принятии решений. Сущность этой новой технологии оценивается рядом факторов. Во-первых, она обладает способностью быстро и точно анализировать большие объемы данных. Это связано с предоставлением руководителям ценной информации для анализа принятия решений. Во-вторых, автоматизация отрасли крайне важна для решения трудоемких процессов с помощью алгоритмических возможностей, экономии ресурсов и снижения вероятности ошибок. Правовые процессы в корпоративном управлении (проведение собраний, голосование, принятие решений) также связаны с оптимизацией управления, что предоставляет глубокие рекомендации для повышения эффективности и снижения затрат через интеллектуальные алгоритмы.

Еще один важный аспект корпоративного управления заключается в том, что искусственный интеллект может хорошо анализировать рынок и давать рекомендации по принятию оптимальных решений. Точнее говоря, преимущества в конкуренции можно достичь путем наблюдения за клиентами и рынком, определения желаний и потребностей клиентов. Искусственный интеллект, применяемый в корпоративном управлении, также играет роль в инновациях и стратегическом планировании: он помогает определить возможности создания новых продуктов и услуг, а также является лучшим инструментом для подготовки и реализации стратегических планов.

Правовое значение оценки и контроля систем ИИ очень важно. Это регулируется на основе национального законодательства каждой страны и международных нормативных документов. Например, законы об электронном правительстве, о персональных данных, об информационной безопасности оцениваются как правовая основа для регулирования вышеуказанных отношений. Недостаточно контроля со стороны уполномоченных государственных органов за искусственным интеллектом, применяемым в корпоративном управлении. В этом отношении следует особо отметить роль общественного контроля и мониторинга, осуществляемого международными организациями. С помощью этих методов можно легко оценить эффективную работу искусственного интеллекта.

По мнению авторов, для надежной оценки систем искусственного интеллекта необходимы четко определенные количественные и качественные показатели, соответствие этическим

[1] Заведующий кафедрой Ташкентского государственного юридического университета. к.ю.н. профессор.

корпоративным принципам[1]. Оценка деятельности программного обеспечения искусственного интеллекта, внедренного в корпоративное управление, осуществляется с технической, экономической и правовой точек зрения.

Например, выявленные в ходе мониторинга случаи неправомерного использования персональных данных приводят к оценке соблюдения прав участников на неприкосновенность частной жизни. Общественный контроль в этой области опирается на мнения, собранные путем проведения опросов о справедливости, надежности и прозрачности искусственного интеллекта. Также могут применяться внутренние правила информирования о нарушениях в управлении и внешние телефоны доверия для конфиденциального информирования о проблемах.

По нашему мнению, комбинированный подход к методам даст положительный эффект при оценке деятельности искусственного интеллекта, внедренного в корпоративное управление.

Некоторые авторы считают, что для строгого и ответственного управления искусственным интеллектом необходимы многогранные протоколы, уравновешивающие внутренний, внешний, экспертный и общественный контроль[2]. Мы считаем, что это мнение охватывает множество методов мониторинга, имеющих свою истину. Протоколы мониторинга должны включать проверку внедренных моделей искусственного интеллекта, анализ правил, требующих периодического обновления и пересмотра данных в программном обеспечении, приведение стандартов мониторинга в соответствие с национальным и международным законодательством и стандартами.

С развитием науки и техники роль общественного контроля может также занять искусственный интеллект. Однако чрезмерное доверие к возможностям роботов также не даст положительного эффекта. Поскольно естественно, что правила корпоративной этики с человеческим фактором в корпоративном управлении будут отличаться от установленных правил этики в результате полного доверия управления искусственному интеллекту. Существует разница между искусственным интеллектом и техническими устройствами компании. Поэтому технический мониторинг может быть связан в основном с исправной работой устройств и различными мерами кибербезопасности.

В целом правовые критерии оценки деятельности искусственного интеллекта зависят от качества внутренних документов компании.

Однако, по нашему мнению, основное внимание в деятельности искусственного интеллекта должно быть обязательно направлено на защиту персональных данных. Вопрос безопасности данных требует особого внимания при использовании систем искусственного интеллекта. Согласно требованиям законодательства GDPR Европейского Союза, компании должны соблюдать строгие ограничения при обработке персональных данных[3]. Персональные данные – это информация, которая индивидуализирует личность или служит для определения его отличия от других лиц. В современном информационном обществе, когда данные стали важным источником, определяющим взаимоотношения с технологиями, компьютерами и другими, очень важно собирать, определять, определять их конфиденциальность и секретность этих данных. Персональные данные играют решающую роль в различных сферах нашей жизни. Сегодня, когда онлайн-виртуальные действия стали более активными, онлайн-покупки, взаимодействие в социальных сетях и обмен информацией, интеграция межведомственных данных, увеличение цифрового обмена данными повысили актуальность этого вопроса и его значение как объекта защиты. Также уместно отметить вышеизложенное в вопросе безопасности медицинских, финансовых, профессиональных, семейных данных.

Персональные данные являются важной информацией, которая должна быть защищена и уважаема. Сбор, обработка и использование такой информации должны осуществляться прозрачно и удобно для использования.

Сегодня ни для кого не секрет, что все сферы общества цифровизируются, оборот информации усиливается, расширяется процесс оценки, продажи и иного распоряжения информацией как

товаром. Действительно, поскольку информационные технологии играют все более важную роль в нашей повседневной жизни в цифровом мире, персональные данные становятся "ценным богатством", но обеспечение их безопасности, конфиденциальности становится главной заботой для их владельца и обработчиков. В связи с этим необходимо собирать, обрабатывать, хранить персональные данные не только государственными органами, но и компаниями, защищать эти данные от угроз и злоумышленников.

Важность защиты персональных данных следует понимать не только из вышеперечисленного, но и из того, что это важно для жизни и деятельности человека, является отдельным фактором в его защите. Персональные данные – это совокупность деликатной информации о каждом человеке. Поэтому важно всегда осознавать важность этой информации для ее владельца.

Обычно, когда персональные данные собираются и обрабатываются уполномоченными государственными органами и некоторыми компаниями, их защита является их обязанностью. Если персональные данные будут раскрыты третьим лицам, это может привести к мошенничеству, клевете и другим серьезным проблемам.

Необходимость защиты персональных данных определяется рядом факторов. В частности:

Риски и угрозы. Сбор и обработка персональных данных включает риски и угрозы. Киберпреступники могут использовать уязвимости систем безопасности для получения персональных данных, захвата источников их сбора или доступа к памяти компьютеров, где они хранятся, и использования их в преступных целях. Утечки данных, вирусы и другие кибератаки стали повсеместной проблемой в интернете.

Шифрование персональных данных. Шифрование персональных данных – это метод защиты данных, при котором данные преобразуются в зашифрованную форму и доступ к ним возможен только авторизованным пользователям с помощью ключа. Это важный механизм защиты данных при передаче и хранении.

Идентификация персональных данных. Важно регистрировать и идентифицировать персональные данные в компьютерной системе. Это может быть строка чисел или символов, присваивающая имена субъектам отношений, связанных с защитой персональных данных. Эта информация называется идентификатором субъекта. Если пользователь имеет зарегистрированный в сети идентификатор, он считается легальным (законным), в противном случае – нелегальным (незаконным) пользователем. Перед использованием компьютерных ресурсов пользователь должен пройти процесс идентификации и аутентификации компьютерной системы.

Целью гражданско-правовой защиты персональных данных граждан является предоставление и обеспечение неприкосновенности частной жизни для того, чтобы гражданин обладал определенной независимостью от общества, его социальных и государственных структур.

Одной из важных правовых проблем является вопрос об ответственности за ущерб, возникший в результате решений, принятых системами искусственного интеллекта. Во многих странах специальная законодательная база в этой области еще не сформирована[4].

Однако недостаточно правовых оснований для определения стоимости ущерба и решения вопроса об ответственности в результате утечки персональных данных, кибератак именно при использовании искусственного интеллекта. Поскольку вопрос определения искусственного интеллекта как субъекта права еще не решен.

Использование автономных продуктов искусственного интеллекта поднимает вопрос о том, как проектировать и создавать такие системы для строгого соблюдения закона[5]. По мнению С.Бозарова, для признания распространения персональных данных в качестве ущерба персональным данным требуются достаточные основания и доказательства. Действительно, персональные данные стали товаром, так как пользователи обычно соглашаются предоставлять свои персональные данные в обмен на другие услуги. В обычной бизнес-модели для интернета

эти данные используются онлайн-платформами (социальные сети, поисковые системы, контент и другие) для предложения целевой рекламы других продуктов или услуг. Хотя органы по защите данных не хотят рассматривать персональные данные как обычный товар, хотя данные трудно оценить, новая система защиты данных в определенной степени подтверждает идею о том, что персональные данные являются частью рыночного обмена и "договорной практики", рассматривая информацию как собственность. Поэтому каждый раз при несанкционированном использовании персональных данных субъект информации должен требовать возмещения ущерба в форме роялти на основании необоснованного обогащения. Однако следует помнить заранее, что не всякое несанкционированное использование персональных данных может привести к ущербу[6].

Применение технологий искусственного интеллекта в корпоративном управлении значительно повышает эффективность компаний. Однако для правильной организации этого процесса, оценки деятельности, регулярного мониторинга необходимо создать соответствующую правовую базу. Необходимо совершенствовать национальное законодательство с учетом международного опыта, в частности, четко определить вопросы безопасности данных и ответственности.

Использованная Литература

1. Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L.. "The ethics of algorithms: Mapping the debate." Big Data & Society, 2016. 3(2).
2. Fjeld, Jessica and Achten, Nele and Hilligoss, Hannah and Nagy, Adam and Srikumar, Madhulika, Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI (January 15, 2020). Berkman Klein Center Research Publication No. 2020-1, Available at SSRN

   //https://ssrn.com/abstract=3518482 or http://dx.doi.org/10.2139/ssrn.3518482
3. Anderson, M. Data Protection in the Age of AI: A Comprehensive Analysis of GDPR Requirements. European Journal of Law and Technology, 2023. 14(2), 45-67.
4. Lee, J., & Wilson, R. Legal Frameworks for AI Liability in Corporate Governance. Harvard Business Law Review, 2024. 12(1), 78-95.
5. Prakken H. On how AI & law can help autonomous systems obey the law: a position paper // AI4J – Artificial Intelligence for Justice. – 2016. P. 42–46, 264

   //https://www.ai.rug.nl/~verheij/AI4J/papers/AI4J_paper_12_prakken.pdf
6. Bozarov Sardor Soxibjonovich. Sun’iy intellekt doirasida huquqiy javobgarlik. Yuridik fanlar doktori (Doctor of Science) ilmiy darajasini olish uchun tayyorlangan DISSERTATSIYA. –T. 2023.