отношении которого поступило заявление или сообщение, смещение сроков со дня обнаружения на более позднее время, что непосредственно затрагивает его интересы.

Аналогичным образом можно проанализировать ситуацию со стороны органа. Ни ПИКоАП, ни КоАП не содержат конкретных сроков, до истечения которых поступившее заявление или сообщение подлежит оценке должностным лицом. В действительности можно столкнуться с ситуацией, когда в связи с перегруженностью должностных лиц оценка конкретного материала откладывается, что, исходя из формулировки оснований для начала административного процесса и отсутствия формы фиксации, может повлечь освобождение лиц от административной ответственности в связи с истечением сроков со дня обнаружения административного правонарушения и не позволит достичь целей административной ответственности, предусмотренных ст. 4.1 КоАП.

Таким образом, целесообразным видится закрепить в ПИКоАП конкретные сроки оценки поводов и форму фиксации наличия оснований для начала административного процесса, что в совокупности регламентирует деятельность органов, устранит спорные ситуации относительно установления даты обнаружения и будет способствовать защите интересов сторон.

Смирнова Д. В.

ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И АВТОМАТИЗАЦИИ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ И ЭТИЧЕСКИЕ АСПЕКТЫ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Смирнова Дарья Викторовна, студентка 2 курса Белорусского государственного университета, г. Минск, Беларусь,

Научный руководитель: заместитель декана по идеологической и воспитательной работе юридического факультета Сухопаров В. П.

В последние десятилетия развитие технологий искусственного интеллекта (ИИ) стало одним из самых значительных достижений науки и техники. Однако с ростом применения ИИ в различных сферах человеческой деятельности возникает необходимость в более глубоком понимании этических аспектов, связанных с его использованием. Понятие этики в сфере искусственного интеллекта охватывает широкий спектр вопросов, включая ответственность разработчиков, прозрачность алгоритмов, защиту данных и влияние на общество.

В эпоху цифровых технологий конфиденциальность личных данных становится одной из наиболее актуальных проблем. Сбор и обработка персональных данных без согласия пользователей представляют собой серьезное нарушение этических норм и прав человека. Многие компании и организации используют алгоритмы и системы для автоматического сбора информации о пользователях, зачастую не информируя их о целях и

способах обработки этих данных. Это может привести к утрате доверия со стороны потребителей и вызвать негативные последствия для репутации организаций. Кроме того, существует риск утечки информации, который может произойти из-за хакерских атак, недостатков в системах безопасности или неправомерных действий сотрудников. В Республике Беларусь за нарушение защиты персональных данных наступает ответственность согласно Закону Республики Беларусь «О защите персональных данных», ст. 19, ст. 23.7 Кодекса Республики Беларусь об административных правонарушениях, ст. 203-1, ст. 203-2 Уголовного кодекса Республики Беларусь.

Одна из наиболее острых проблем заключается в том, кто должен нести ответственность в случае аварий или нежелательных последствий, вызванных действиями ИИ. Например, если автономный автомобиль попадает в аварию, возникает вопрос: кто несет ответственность – разработчик программного обеспечения, производитель автомобиля, владелец транспортного средства или сам ИИ?

Другим важным аспектом является необходимость определения юридического статуса ИИ. В настоящее время ИИ не имеет правосубъектности, что затрудняет привлечение его к ответственности. Этот вопрос требует комплексного подхода и обсуждения на уровне законодательства, чтобы установить четкие правила и нормы, касающиеся действий ИИ. Возможные решения могут включать создание новых юридических категорий, которые позволят учитывать специфику работы ИИ и обеспечивать защиту прав людей, затронутых его действиями. На данный момент в Республике Беларусь некоторые аспекты использования ИИ регулируются следующими нормативными правовыми актами: Декрет Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики»; Указ Президента Республики Беларусь от 01.02.2010 № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет»; Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных»; Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации»; Концепция информационной безопасности Республики Беларусь, утвержденная постановлением Совета Безопасности Республики от 18.03.2019 № 1.

ИИ оказывает значительное влияние на социальные структуры и отношения. Прежде всего ИИ трансформирует рынок труда. Алгоритмы, используемые в социальных сетях и приложениях, влияют на то, как люди общаются и получают информацию.

Угрозы, связанные с использованием ИИ, в различных сферах значительны. Использование искусственного интеллекта (ИИ) в кибербезопасности, роботизации и военных технологиях открывает новые горизонты, но также влечет за собой значительные угрозы и этические дилеммы. В сфере кибербезопасности ИИ может быть использован как для защиты систем, так и для атак на них. Автоматизированные системы могут анализировать огромные объемы данных для выявления уязвимостей, но также могут быть использованы злоумышленниками для создания более

сложных и эффективных кибератак. В контексте роботизации, особенно в производственной сфере, автоматизация процессов может привести к значительным изменениям на рынке труда и повысить риски для безопасности работников. Роботы, управляемые ИИ, могут действовать автономно, что ставит под сомнение вопросы ответственности в случае их сбоев или аварий.

Для того чтобы минимизировать риски и гарантировать, что создаваемые системы соответствуют высоким стандартам безопасности и этики, необходимо внедрение этических принципов в процесс разработки. Тестирование новых технологий является ключевым шагом к созданию ответственного ИИ. Этические нормы должны быть интегрированы на всех этапах – от концептуализации и проектирования до реализации и оценки. Это может включать создание мультидисциплинарных команд, которые будут учитывать различные перспективы, а также разработку четких стандартов и руководств, направленных на соблюдение этических норм. Такие меры помогут не только повысить качество разрабатываемых систем, но и укрепить доверие пользователей к технологиям ИИ, что, в свою очередь, будет способствовать их более широкому и безопасному применению в различных сферах жизни.

Стельмах А. А.

ЦИФРОВОЙ СУВЕРЕНИТЕТ VS ЦИФРОВАЯ ДИКТАТУРА

Стельмах Анна Александровна, учащаяся 2 курса Юридического колледжа Белорусского государственного университета, г. Минск, Беларусь, mademoiselle_annanutasun@mail.ru

Научный руководитель: преподаватель Балицевич-Рында Л. Н.

При выходе на новый уровень развития технологий, преобразовании информации в цифровую форму государство должно оперативно реагировать на связанные с этим новые угрозы и принимать своевременные меры для обеспечения государственного суверенитета. Особенно актуальным становится проблема обеспечения информационного суверенитета как составной части государственного суверенитета.

Информационный суверенитет касается в первую очередь информации стратегического для государства значения, персональной информации граждан как охраняемых государством субъектов и внутригосударственного информационного пространства, которое имеет для независимости государства, по нашему мнению, не меньшее значение, чем его территория. В Концепции национальной безопасности Республики Беларусь информационная безопасность определена как состояние защищенности информационных пространства, инфраструктуры и ресурсов от внешних и внутренних угроз в информационной сфере. Для того чтобы иметь возможность прогнозировать, распознавать и купировать угрозы информационному суверенитету государства, необходима государственная поддержка развития