



приоритет2030<sup>+</sup>  
право для лидерства

# АНАЛИТИЧЕСКИЙ ДОКЛАД

*«Применение искусственного интеллекта  
в системе обеспечения национальной  
безопасности»*



СОЦИОПРАВО

**Аналитический доклад**  
**«Применение искусственного интеллекта**  
**в системе обеспечения национальной безопасности»**

**Введение**

В настоящее время все государства мира находятся в поиске решения проблем цифровой трансформации публичного управления, в основе которых определяющим фактором является внедрение искусственного интеллекта (далее – ИИ). Это обусловлено тем, что именно его (ИИ) использование определяет степень влияния любого государств на мировые политические процессы.

Термин ИИ впервые появился в 1956 году в Соединенных Штатах Америки в городе Дартмут, на собрании выдающихся учёных в области автоматизации и вычислений (математическую элиту того времени), интересующихся темами нейронных сетей. На встрече были заложены основы концепции ИИ и определен путь её дальнейшего развития. В 1950 году Аланом Тьюрингом была опубликована научная статья «Вычислительные машины и разум», в содержании которой раскрывалась концепция ИИ. В этой работе была заложена основа теста, способного определить поведение компьютерных систем. В дальнейшем этот тест стал именоваться тестом Тьюринга<sup>1</sup>.

По мере того, как применение ИИ становится повседневной реальностью, можно констатировать его влияние на оборонительные и наступательные возможности, а также на общую технологическую и экономическую конкурентоспособность страны<sup>2</sup>. Необходимо отметить, что Россия, признавая

---

<sup>1</sup> Pavic A. Artificial intelligence and national security strategy development: Challenges and perspectives // Национальный интерес. 2024. № 2. Т. 48. С. 55-56. URL: [https://www.researchgate.net/publication/382024057\\_ARTIFICIAL\\_INTELLIGENCE\\_AND\\_NATIONAL\\_SECURITY\\_STRATEGY\\_DEVELOPMENT\\_CHALLENGES\\_AND\\_PERSPECTIVES](https://www.researchgate.net/publication/382024057_ARTIFICIAL_INTELLIGENCE_AND_NATIONAL_SECURITY_STRATEGY_DEVELOPMENT_CHALLENGES_AND_PERSPECTIVES) (дата обращения: 20.09. 2024).

<sup>2</sup> Afsah E. Artificial Intelligence, Law, and National Security // The Cambridge Handbook of Responsible Artificial Intelligence Interdisciplinary Perspectives. Cambridge University Press 2022 Publisher. P.448.

воздействие технологических процессов на обеспечение национальной безопасности, с целью защиты от различных угроз, определила развитие ИИ в качестве важнейшего инструмента обеспечения национальной безопасности. Эта позиция нашла свое отражение в Национальной стратегии развития искусственного интеллекта на период до 2030 года<sup>3</sup> (далее – Стратегия развития искусственного интеллекта).

Осмысление влияния использования ИИ в сфере национальной безопасности не ограничивается обычным представлением о данной технологии как об инструменте какой-либо автоматизации. На наш взгляд, об ИИ можно говорить как о некоем явлении, обладающим не только возможностью самообучения, но и адаптации и выбора решений в любых условиях. В свою очередь, наличие таких технологических достижений требует необходимости их учета и внедрения в функционирование сложившийся годами системы обеспечения безопасности государства.

Известно, что обеспечение национальной безопасности охватывает множество процессов, среди которых несомненно заслуживают быть выделенными военно-стратегические, экономические, информационные, экологические. Совершенно очевидно, что внедрение ИИ позволит их усовершенствовать, например, в разы улучшить эффективность анализа больших данных и прогнозирование внешних и внутренних угроз (рисков).

Следует констатировать, что в настоящее время зафиксирован положительный эффект применения ИИ в решении проблемы обеспечения противодействия киберугрозам, поскольку алгоритмы машинного обучения обладают способностью определять возможные риски в режиме реального времени, причем многократно эффективнее любых систем защиты. Поскольку

---

<sup>3</sup> Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года» // Собрание законодательства. 14.10.2019. № 41. Ст. 5700.

кибератаки, целью которых является уничтожение государственной инфраструктуры, постоянно масштабируются, внедрение ИИ в механизм обеспечения национальной безопасности приобретает особую актуальность.

Совершенствование технологий ИИ, безусловно, является движущей силой, влияющей на становление высокотехнологичной экономики. В соответствии с положениями Национальной стратегии, применение ИИ в основных отраслях экономики (промышленность, сельское хозяйство и др.) позволит добиться повышения эффективности управленческих решений, принимаемых на всех уровнях публичного управления.

Следует все же признать, что использование ИИ в обеспечении национальной безопасности государства не связано лишь с технологическими аспектами. Владение технологиями ИИ, безусловно, повышает статус государства на международной арене. Россия активно ведет работу по корректировке и совершенствованию международного законодательства по использованию ИИ, поскольку осознает риски его применения в качестве инструмента, влияющего на безопасность общества и государства.

В современном мире существует множество факторов, влияющих на безопасность государства – это глобальное потепление, пандемии, военные конфликты и др. В таких условиях ИИ можно расценивать как инструмент, позволяющий государствам адаптироваться к любым процессам, влияющим на их безопасность, и поддерживать равновесии управленческих систем. В связи с этим нельзя не отметить необходимость интеграции ИИ в систему обеспечения национальной безопасности, что, на наш взгляд, позволит мгновенно выявлять риски и прогнозировать последствия для государства от принятия каких-либо возможных решений, с целью выбора наилучшего варианта действий в различных критических условиях.

Внедрение ИИ в систему обеспечения государственной безопасности позволит повысить эффективность функционирования механизмов защиты национальных интересов. Однако внедрение ИИ в управление в сфере безопасности требует проведение исследования передового международного

опыта с целью его применения в России. Полагаем, что в целях заимствования зарубежного опыта для имплементации технологий ИИ в систему обеспечения национальной безопасности Российской Федерации, особый интерес представляют такие страны, как Франция, США и о. Маврикий, являющиеся передовыми государствами по внедрению ИИ в сферу обеспечения национальной безопасности. Проведенное исследование содержания их стратегий и практических решений показало, что этим государствам удалось достичь положительного эффекта от использования ИИ в области национальной безопасности и, таким образом, минимизировать потенциальные риски в осуществлении государственного управления в административно-политической сфере. Так, Франция удачно внедрила ИИ в оборонный сектор, а США достигли лидирующих позиций в разработке ИИ-систем двойного назначения. Что касается о. Маврикия, то его опыт применения ИИ был бы полезен России с целью защиты морских границ.

## **I. Применение искусственного интеллекта в России и зарубежных странах**

Анализ Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 2 июля 2021 года № 400, демонстрирует важность научно-технологического развития для обеспечения национальной безопасности. В документе говорится, что «В условиях перехода мировой экономики на новую технологическую основу лидерство в развитии науки и технологий становится одним из ключевых факторов повышения конкурентоспособности и обеспечения национальной безопасности»<sup>4</sup>. Примечательно, что Стратегия определяет развитие искусственного интеллекта как одну из ос-

---

<sup>4</sup> П. 60 Стратегии национальной безопасности Российской Федерации (см.: Указ Президента РФ от 2 июля 2021 г. N 400 «О Стратегии национальной безопасности Российской Федерации») // Собрании законодательства Российской Федерации. 5.07.2021. № 27 (часть II). Ст. 5351.

новых задач в рамках научно-технологического развития, наряду с суперкомпьютерными системами, нанотехнологиями, робототехникой и другими высокими технологиями (медицинскими, биологическими, генной инженерии, информационно-коммуникационными, квантовыми, обработкой больших данных, энергетическими, лазерными, аддитивными, созданием новых материалов, когнитивными, природоподобными)<sup>5</sup>. Необходимо отметить, что роль ИИ в обеспечении национальной безопасности Российской Федерации носит системообразующий характер, так как он устанавливает направления технологического и стратегического развития страны в долгосрочной перспективе. Изучение сущности применения ИИ в области национальной безопасности основывается на междисциплинарном подходе, который, с одной стороны, провозглашает важность технологических аспектов ИИ, а с другой, – его влияние на социально-экономические и геополитические процессы.

Большое внимание уделяется также технологической независимости с целью обеспечения информационной безопасности посредством развития отечественных ИТ-решений и средств защиты информации. Таким образом, можно сделать вывод, что применение технологий ИИ является важнейшим элементом системы обеспечения национальной безопасности Российской Федерации в современных геополитических условиях.

В вопросах обеспечения национальной безопасности все государства мира развивают и внедряют ИИ, что подтверждается п. 23 Стратегии развития искусственного интеллекта на период до 2030 года, в котором в качестве од-

---

<sup>5</sup> пп.14 п.76 Стратегии национальной безопасности Российской Федерации (см.: Указ Президента РФ от 2 июля 2021 г. N 400 «О Стратегии национальной безопасности Российской Федерации») // Собрании законодательства Российской Федерации. 5.07.2021. № 27 (часть II). Ст. 5351.

ного из основных векторов его применения определено усиление национальной безопасности и поддержание правопорядка<sup>6</sup>. Для достижения поставленных целей в области обеспечения национальной безопасности в п. 24 Стратегии определены основные задачи развития искусственного интеллекта в Российской Федерации, среди которых: а) повышение доступности инфраструктуры, необходимой для развития технологий ИИ; б) поддержка организаций – разработчиков технологий ИИ; в) поддержка научных исследований и разработок в целях обеспечения опережающего развития ИИ; г) повышение уровня компетенций в области ИИ и уровня информированности граждан о технологиях ИИ; д) стимулирование внедрения технологий ИИ в отраслях экономики и социальной сферы; е) обязательное внедрение доверенных технологий ИИ в тех областях его использования, в которых может быть нанесен ущерб безопасности Российской Федерации; ж) создание комплексной системы нормативно-правового регулирования общественных отношений, связанных с развитием и использованием технологий ИИ, обеспечение безопасности применения таких технологий; з) укрепление международного сотрудничества в области использования технологий ИИ<sup>7</sup>.

Закрепленные в Стратегии развития искусственного интеллекта положения направлены на создание инфраструктуры, необходимой для развития и интеграции ИИ во все сферы публичной власти и общественную жизнь. Выполнение вышеперечисленных задач обеспечит технологический суверенитет России, достижение которого необходимо на данном этапе развития российской государственности, характеризуемым ростом использования разведками иностранных государств информационно-коммуникационных технологий в

---

<sup>6</sup> п. 23 Национальной стратегии развития искусственного интеллекта на период до 2030 года» (Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации») // Собрание законодательства. 14.10.2019. № 41. Ст. 5700.) // Собрание законодательства. 14.10.2019. № 41. Ст. 5700.

<sup>7</sup> п. 24 Национальной стратегии развития искусственного интеллекта на период до 2030 года» (Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации») // Собрание законодательства. 14.10.2019. № 41. Ст. 5700.) // Собрание законодательства. 14.10.2019. № 41. Ст. 5700.

условиях санкционного давления и проведения СВО, когда задача обеспечения национальной безопасности государства является первостепенной. В настоящее время Россия столкнулась с новыми с новым спектром угроз, связанных с применением высокотехнологичных инноваций. Анализируя применение ИИ, следует отметить, что, в первую очередь, он нацелен на использование в административно-политической сфере публичного управления. Важнейшее направление применения ИИ – это обеспечение информационной безопасности государства. Так, в соответствии с разделом 51 (8) Стратегии развития искусственного интеллекта особое внимание уделяется внедрению доверенных технологий ИИ. Данное направление особенно актуально в свете увеличения киберугроз, угрожающих критической информационной инфраструктуре. Например, в правоохранительной деятельности применение ИИ позволяет повысить эффективность принятия решений, поскольку его использование кардинально меняет организацию деятельности по анализу больших баз данных, совершенствуя деятельность по прогнозированию угроз национальной безопасности.

Несмотря на то, что в Стратегии развития искусственного интеллекта ничего не говорится об использовании ИИ в области обороны, представляется возможным заключить, что в этом направлении российским государством уже используются такие технологии, как компьютерное зрение, интеллектуальная поддержка принятия решений в модернизации Вооруженных сил РФ. Примечательно, что армия чуть быстрее осваивает новые технологии, чем различные правоохранительные органы, например, полиция. Например, в Британии государственная власть решила вооружить своих солдат сенсорами, искусственным интеллектом, дронами и боевыми лазерами. О самом крупном вливании средств в оборонную промышленность объявил премьер-министр страны Борис Джонсон – за 4 года он вынужден был потратить 16,5 млрд. фунтов, причем примерно треть этих денег - именно на новые технологии. «Солдат на вражеской территории будет предупрежден о дальней засаде сенсорами, спутни-

ками или дронами, мгновенно передающими сигнал тревоги с помощью искусственного интеллекта для обеспечения оптимальной реакции, и сможет выбрать целый ряд действий — от запроса воздушного удара до атаки роем дронов или нейтрализации противника кибероружием»<sup>8</sup>.

В настоящее время применение ИИ в области обороны способствует повышению эффективности комплексных систем вооружения. Наибольший интерес представляет использование беспилотных летательных аппаратов различного назначения - дронов. Если сегодня они управляются операторами дистанционно или посредством «примитивной» автоматизации, то в будущем ИИ, без сомнений, поможет значительно усовершенствовать их (дронов) управление, и тем самым оснастит дроны дополнительными свертехнологическими функциями, повышая при этом эффективность ведения боевых действий. Например, с помощью нейросетевых и узкоспециализированных технологий на основе данных коммерческой спутниковой съемки роботы-дроны будут способны уничтожать даже авианосцы и др. виды устаревшего вооружения<sup>9</sup>.

Ещё одним важным направлением использования технологий ИИ является развитие и совершенствование на его основе отечественных разработок в области обеспечения технологического суверенитета России. В п. 17(9) Стратегии развития искусственного интеллекта говорится о том, что между государствами усилилась конкуренция в области ИИ. Это выражается в создании препятствий для импорта передовых технологий микроэлектроники, привлечения квалифицированных специалистов в области ИИ из других государств, а также во введении ограничений на свободное распространение технологий. Вместе с тем усиливаются риски возникновения зависимости от недобросо-

---

<sup>8</sup> Торговцева А. Вор должен сидеть в цифре // Деловой Петербург. 27.11.2020. № 174-175. С. 23.

<sup>9</sup> Afsah E. Artificial Intelligence, Law, and National Security // The Cambridge Handbook of Responsible Artificial Intelligence Interdisciplinary Perspectives. Cambridge University Press 2022 Publisher. P.467-468.

вестных поставщиков решений в области ИИ. Поэтому достижение лидирующих позиций в этой области следует считать важной задачей государства – ведь в условиях глобальной конкуренции необходимо достичь наименьшего уровня технологической зависимости с целью укрепления национальной безопасности.

Стратегия развития искусственного интеллекта не оставляет без внимания также этические и правовые аспекты развития ИИ в сфере обеспечения безопасности государства. В частности, в п. 19 Стратегии гарантируется защита прав и свобод граждан, а также недопустимость использования ИИ в целях умышленного причинения вреда гражданам и организациям<sup>10</sup>. Кроме того, в п. 51(10) подчеркивается важность правового регулирования использования ИИ с целью предотвращения потенциального вреда гражданам и организациям: «... нормативно-правовое регулирование в области искусственного интеллекта не должно умалять право выбора и интеллектуальные способности человека, являющиеся самостоятельной ценностью и системообразующим фактором современной цивилизации»<sup>11</sup>.

Таким образом, внедрение технологий ИИ в систему обеспечения национальной безопасности России представляет собой многоаспектный процесс – от повышения эффективности публичного управления в административно-политической сфере до обеспечения технологического суверенитета и соблюдения этических стандартов. В свою очередь, это приводит к выводу о понимании государством не только важности использования и дальнейшего развития критически важных технологий, но и возможных последствий таких процессов.

---

<sup>10</sup> П. 19 Национальной стратегии развития искусственного интеллекта на период до 2030 года» (Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации») // Собрание законодательства. 14.10.2019. № 41. Ст. 5700.) // Собрание законодательства. 14.10.2019. № 41. Ст. 5700

<sup>11</sup> Пп. В п. 51 (10) Национальной стратегии развития искусственного интеллекта на период до 2030 года» (Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации») // Собрание законодательства. 14.10.2019. № 41. Ст. 5700.) // Собрание законодательства. 14.10.2019. № 41. Ст. 5700.

Помимо Стратегии развития искусственного интеллекта, в России разработан ряд других документов, регламентирующих использование ИИ с целью обеспечения безопасности государства. Среди них - Дорожная карта развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект»<sup>12</sup>, Концепция развития технологий машиночитаемого права<sup>13</sup>, Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»<sup>14</sup>, Дорожная карта развития «сквозной» цифровой технологии «Компоненты робототехники и сенсорика»<sup>15</sup>, Дорожная карта развития «сквозной» цифровой технологии «Технологии беспроводной связи»<sup>16</sup>, Дорожная карта развития «сквозной» цифровой технологии «Технологии виртуальной и дополненной реальности»<sup>17</sup>, До-

---

<sup>12</sup> Дорожная карта развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект». Москва, 2019. — Текст: электронный // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. — URL: <https://digital.gov.ru/ru/documents/6658/> (дата обращения: 20.09.2024).

<sup>13</sup> Концепция развития технологий машиночитаемого права (утв. Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 15.09.2021 № 31). — URL: <https://www.garant.ru/products/ipo/prime/doc/402785971/> (дата обращения: 20.09.2024).

<sup>14</sup> Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения СТО БР ИББС-1.0-2014». // Вестник Банка России. 2014. № 48-49.

<sup>15</sup> Дорожная карта развития «сквозной» цифровой технологии «Компоненты робототехники и сенсорика». Москва, 2019. // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. — URL: <https://digital.gov.ru/uploaded/files/07102019robototehnika-i-sensorika.pdf> (дата обращения: 20.09.2024).

<sup>16</sup> Дорожная карта развития «сквозной» цифровой технологии «Технологии беспроводной связи». Москва, 2019 // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. — URL: <https://digital.gov.ru/uploaded/files/07102019tbs.pdf> (дата обращения: 20.09.2024).

<sup>17</sup> Дорожная карта развития «сквозной» цифровой технологии «Технологии виртуальной и дополненной реальности». Москва, 2019 // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. — URL: <https://digital.gov.ru/ru/documents/6654/> (дата обращения: 20.09.2024).

рожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра»<sup>18</sup>, Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии»<sup>19</sup>, Дорожная карта развития «сквозной» цифровой технологии «Новые производственные технологии»<sup>20</sup> и др.

Рассмотрим содержание некоторых из них более подробно.

Прежде всего следует обратить внимание на подготовленную Министерством цифрового развития, связи и массовых коммуникаций РФ Дорожную карту развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект». Она представляет собой стратегию, целью реализации которой является разработка экосистемы для внедрения ИИ в критически важные области экономики и национальной безопасности. В данном документе основной акцент сделан на совершенствовании технологий обработки и анализа больших данных (Big Data), позволяющих определять потенциальные угрозы. Так, интеграция ИИ в системы мониторинга и прогнозирования обеспечивает возможность осуществления моделирования сценариев развития критических ситуаций, что позволяет мгновенно принимать верное решение в любой области обеспечения национальной безопасности.

По нашему мнению, следует согласиться с позицией зарубежных учёных о том, что развитие ИИ было во многом обусловлено необходимостью совершенствования механизмов обеспечения национальной безопасности. Потребности государств в этой области были вызваны необходимостью наблюдения,

---

<sup>18</sup> Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра». Москва, 2019 // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. — URL: <https://digital.gov.ru/ru/documents/6670/> (дата обращения: 20.09.2024).

<sup>19</sup> Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии». Москва, 2019 // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. — URL: <https://digital.gov.ru/uploaded/files/07102019kvantyi.pdf> (дата обращения: 20.09.2024).

<sup>20</sup> Дорожная карта развития «сквозной» цифровой технологии «Новые производственные технологии». Москва, 2019. – Текст: электронный // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. – URL: <https://digital.gov.ru/ru/documents/6662/> (дата обращения: 20.09.2024).

особенно взлома кодов, и отчасти разработкой оружия, в частности, моделированием ядерных испытаний. Учитывая, что использование некоторых форм машинного интеллекта является частью национальной безопасности на протяжении уже многих десятилетий, взрывной рост возможностей машин постепенно изменяет национальную и международную безопасность, затрагивая важные вопросы регулирования<sup>21</sup>.

В связи с изложенным нельзя оставить без внимания утвержденную Правительственной комиссией по цифровому развитию Концепцию развития технологий машиночитаемого права, предлагающую новый подход к использованию ИИ в правоприменительной деятельности. Данная Концепция раскрывает преимущества использования алгоритмов ИИ для автоматизированного анализа нормативных правовых актов, что обеспечивает повышение эффективности осуществления мониторинга соблюдения законодательства, а также исключение субъективного фактора при выявлении правонарушений. В будущем такие технологии планируется внедрить в деятельность различных государственных органов в сфере безопасности с целью обеспечения работы системы автоматического мониторинга, которая должна будет выявлять противоречащее правовым нормам поведение различных субъектов, что имеет важное значение для устранения рисков угрозам национальной безопасности.

Так, использование ИИ крайне необходимо для выявления и расследования преступлений, поскольку с обработкой и сравнением документов он справится лучше, чем человек. И здесь мы полностью согласны с мнением директора лаборатории компьютерной криминалистики при Университете ИТМО П. Кузьмичем, высказавшемся о накоплении сведений о преступлениях в единой системе, которая позволит выявлять схожие правонарушения в разных регионах. По его словам, «Преступник не будет специально работать только в одном регионе. Он действует, условно говоря, вокруг себя, иногда

---

<sup>21</sup> Afsah E. Artificial Intelligence, Law, and National Security // The Cambridge Handbook of Responsible Artificial Intelligence Interdisciplinary Perspectives. Cambridge University Press 2022 Publisher. P.447.

меня регионы. А учёты не пересекаются, скажем, в Ленинградской области и Новгородской. Могут быть совершены идентичные преступления, но свести их в серию крайне сложно. А вот нейросеть вполне может сличить дела, выявить закономерности и предложить следователю эти дела объединить»<sup>22</sup>.

Также ИИ может оказать существенную помощь в оперативном сборе и анализе данных с места происшествия, преобразовать огромные массивы информации в вид, удобный для восприятия человеком. Это существенная помощь в проведении дальнейших оперативно–розыскных и следственных мероприятий: в фиксации доказательств виновности или невиновности, а также в прогнозировании поведения и местонахождения интересующих субъектов<sup>23</sup>.

Наряду с этим, развитие технологий ИИ способствует увеличению потенциала блокчейна, обеспечивающего работу механизма для верификации и аудита решений, принимаемых системами ИИ. В настоящее время практически любое упоминание словосочетания «распределенные реестры» (блокчейн) так или иначе ассоциируется с криптовалютами. Подобная мысль укоренилась в головах людей из-за наиболее резонансных и обсуждаемых случаев мошенничества в названной сфере. Тем не менее, если мы абстрагируемся от предрассудков и разберем устройство технологии блокчейн, то ситуация не будет такой однозначной. Ведь технология распределенных реестров (блокчейн) может быть успешно применяется в криминалистике с целью расследования преступлений различного характера и противодействия им.

Начнем с того, что блокчейн представляет собой выстроенную по установленным правилам непрерывную цепочку блоков, каждый из которых содержит информацию о предшествующем блоке. Как правило, копии цепочек блоков хранятся на множестве устройств, что обуславливает децентрализованность всей системы. Ключевым в данном определении является то, что в блокчейне содержатся данные обо всех операциях, которые проходят через него.

---

<sup>22</sup>Торговцева А. Вор должен сидеть в цифре // Деловой Петербург. 27.11.2020. № 174-175. С. 22.

<sup>23</sup> Там же, с.23

Являясь распределенной базой данных, блокчейн хранит общую для всех информацию, которая сверяется на постоянной основе. Так как данные в блокчейне содержатся децентрализованным образом, никто не сможет повредить ключевой узел системы и организовать утечку или подмену информации. Такой формат хранения данных может использоваться не только для отслеживания транзакций, но и для создания универсальных закрытых регистров в абсолютно различных сферах правоохранительной деятельности, например, в криминалистике, с целью расследования преступлений на основе сведений, хранящихся в блокчейне. Иначе говоря, правоохранительные органы получили возможность использовать защищенную и распределенную базу (блокчейн), например, для фиксации в ней биометрических данных иностранных граждан и лиц без гражданства, данных о проступках и противоправных деяниях совершенных за рубежом, о наличии судимости, о нахождении лица в розыске, что позволит правильно и безошибочно выявлять преступников.

В настоящее время информация о судимости и лицах, находящихся в розыске, хранится в базе правоохранительных органов централизованным образом, что делает возможным получение к ней доступа третьих лиц вследствие коррупционных действий должностных либо хакерских атак. Так, например, в настоящее время вполне реально внести в базу данных «Розыск» изменения, что позволит исключить находящихся в розыске лиц из поле зрения правоохранительных органов, скрыться от следствия посредством беспрепятственного перемещения как по территории российского государства, так и иностранного. Таким образом, хранение информации в блокчейне исключает любое человеческое вмешательство с целью уничтожения информации о лицах, совершивших преступления и скрывающихся от следствия.

Это лишь только малая часть возможностей блокчейна и ИИ. Для криминалистики его роль бесценна. Представляется, что в будущем ИИ облегчит следователю его работу в части обработки материалов, в частности, поможет распознать текст, изучить интернет-контент, осуществить мониторинг информации в социальных сетях и др.

Примечательно, что благодаря технологиям ИИ материалы уголовных дел, протоколы следственных действий, информация, получаемая из различных источников в будущем смогут, с одной стороны, безопасно храниться в блокчейне, а с другой – молниеносно обрабатываться. Кроме того, в ходе расследования преступлений ИИ позволит выявить взаимодействие и связи подозреваемого с иными лицами, причастными к совершению преступления. Разработанный МВД России проект по внедрению ИИ в следственные мероприятия по существу является революционным, поскольку он в корне изменит реализацию правового статуса следователя, избавив его от рутинной работы, на которую сейчас он тратит большую часть своего рабочего времени. Здесь важно отметить и то, что при совершении следственных действий работа следователя значительно будет упрощена в части сбора доказательств и необходимой информации посредством ее мгновенного поиска и обработки.

Кроме того, создание в России реестра генетической информации и принятие проекта МВД России по внедрению ИИ в следственные мероприятия позволит определять личность преступника по ДНК. Как известно, раскрытие личности преступника по ДНК – это задача, поставленная реалиями современности и продолжаемым развитием технического прогресса. Кстати сказать, подобные проекты уже давно реализуются в Великобритании и США. И в этом плане Россия должна включиться в развитие технологий ИИ для правоохранительной сферы с обеспечения действия режима законности на всей территории государства<sup>24</sup>.

Особое значение имеет использование ИИ с целью обеспечения информационной безопасности государства, что в эпоху цифровизации приобретает особую актуальность, в том числе по вопросу защиты критической инфраструктуры. Наибольший интерес в этом направлении представляет обеспечение безопасности финансовых операций и функционирования банковской системы в условиях санкционного давления в целом. Стандарт Банка России

---

<sup>24</sup> Торговцева А. Вор должен сидеть в цифре // Деловой Петербург. 27.11.2020. № 174-175. С. 22.

«Обеспечение информационной безопасности организаций банковской системы Российской Федерации» раскрывает особенности и преимущества внедрения технологий ИИ в системы защиты данных от киберугроз и различных информационных атак. В частности, работа алгоритмов машинного обучения и нейронных сетей гарантирует высокий уровень киберзащиты посредством способности к оперативному выявлению аномалий в сетевом трафике и молниеносному реагированию на потенциальные угрозы, тем самым, обеспечивая бесперебойное функционирование финансовой системы, и, соответственно, высокий уровень финансовой безопасности государства. Блокчейн может стать именно той технологией, которая значительно снизит масштабы криминальных процессов в теневой экономике, облегчив контроль за движением финансов. При этом можно предположить, что в будущем не криптовалюты, работающие на прозрачном блокчейне, а фиатные деньги станут основной валютой преступников и террористов.

Говоря о трекинге транзакций, следует упомянуть взлом криптовалютной биржи Scryptoria, который произошел в конце 2018 г. Хакеры перевели с торговой площадки крупную сумму денежных средств в криптовалюте (23 млн дол.) на свои кошельки, тем самым подорвав нормальную работу биржи. Полиция Новой Зеландии, используя современные цифровые технологии, в сотрудничестве с высококвалифицированными IT-специалистами, добилась значительных успехов в выявлении организаторов данной атаки и возврате средств, учитывая, что украденная криптовалюта активно отслеживается через блокчейн. Обналичивание криптовалюты или ее обмен на другие криптоактивы через сторонние криптовалютные биржи становится проблемой для преступников (торговые и обменные площадки могут замораживать подозрительные аккаунты и изымать с них средства, возвращая их обратно владельцам). Являясь распределенной базой данных, блокчейн хранит общую для всех информацию, которая сверяется на постоянной основе. Так как данные в блокчейне содержатся децентрализованным образом, преступники не могут повредить ключевой узел системы и организовать утечку или подмену информации.

Такой формат хранения данных может использоваться не только для отслеживания транзакций, но и для создания универсальных закрытых регистров в абсолютно различных сферах деятельности<sup>25</sup>.

В целях повышения эффективности публичного управления в сфере безопасности важное значение приобретает зарубежный опыт применения ИИ. В настоящее время одним из лидеров внедрения ИИ в функционирование системы национальной безопасности является Республика Маврикий.

Так, «Стратегия искусственного интеллекта Республики Маврикий» (далее – Стратегия о. Маврикий) регулирует применение ИИ в управлении транспортной инфраструктурой, а также в деле обеспечения кибербезопасности государства, защиты данных, функционирования правоохранительных органов и т.д. В области противодействия кибератакам большой научный и практический интерес представляет разработка систем раннего предупреждения, основанных на алгоритмах машинного обучения, способных идентифицировать потенциальные угрозы на основе анализа больших данных. Революционным положением здесь необходимо считать стратегический подход к противодействию постоянным угрозам. Наиболее важной представляется **идея минимизации человеческого фактора** в деятельности государства, связанной с обеспечением кибербезопасности. Для решения этого вопроса законодательством о. Маврикий предусмотрено создание автономных систем, способных на самостоятельной основе принимать решения по предотвращению и нейтрализации угроз, что делает возможным молниеносное выявление проблемы и выбор единственного верного решения<sup>26</sup>. Немаловажное значение в Стратегии о. Маврикий придается использованию ИИ в работе правоохранительных органов, в том числе следователей. Считается, что его возможности могут карди-

---

<sup>25</sup> Суходолов А.П., Антонян Е.А., Рукинов М.В., Шамрин М.Ю., Спасенникова М.Г. Всероссийский криминологический журнал. 2019. Т. 13. № 4. С. 561.

<sup>26</sup> Mauritius Artificial Intelligence Strategy. P.16. Режим доступа: <https://mitci.govmu.org/Documents/Strategies/Mauritius%20AI%20Strategy.pdf>. (дата обращения: 20.09.2024).

нально повысить эффективность реализации их статуса в деле борьбы с преступностью<sup>27</sup>. Например, должностные лица, опираясь на алгоритмы машинного обучения и анализ больших данных, анализируют состояние преступности в государстве, информацию из множества разрозненных источников, включая базы данных правоохранительных органов, финансовые транзакции, записи камер видеонаблюдения и данные мобильных устройств. Это существенно ускоряет процесс идентификации подозреваемых и сбор доказательственной базы. Более того, ИИ помогает выявлять связи между, казалось бы, никак не связанными между собой преступлениями, обнаруживая общие фактические обстоятельства их совершения<sup>28</sup>.

Примером применения ИИ в правоохранительной деятельности о.Маврикий является использование технологии обработки естественного языка, позволяющей автоматизировать анализ текстовых и аудио данных, а именно: записей телефонных разговоров, сообщений в социальных сетях и электронной переписки в мессенджерах. ИИ способен выявлять угрозы по ключевым словам и фразам, анализировать эмоциональный критерий сообщений. Все эти возможности важны для предотвращения терактов и пропаганды запрещенной информации в социальных сетях (ЛГБТ, экстремизма).

Особую значимость на о. Маврикий приобрело использование ИИ для управления энергосистемами в кризисных ситуациях. В случае стихийных бедствий или целенаправленных кибератак на энергетические объекты, интеллектуальные системы способны в режиме реального времени анализировать огромные массивы данных, выявляя аномалии и потенциальные угрозы. Это позволяет оперативно локализовать проблемные участки сети, автоматически

---

<sup>27</sup> Mauritius Artificial Intelligence Strategy. P.11. Режим доступа: <https://mitci.govmu.org/Documents/Strategies/Mauritius%20AI%20Strategy.pdf>. (дата обращения: 20.09.2024).

<sup>28</sup> Mauritius Artificial Intelligence Strategy. P.58. Режим доступа: <https://mitci.govmu.org/Documents/Strategies/Mauritius%20AI%20Strategy.pdf> (дата обращения: 20.09.2024).

перенаправлять потоки энергии и обеспечивать бесперебойное электроснабжение критически важных объектов инфраструктуры, таких как больницы, центры управления и правительственные учреждения.

Стратегические инициативы Франции в сфере ИИ также важны и могут быть полезными для России, поскольку она позиционирует себя как государство – двигатель технологического прогресса в рамках ЕС и демонстрирует инновационный подход к использованию ИИ в вопросах обеспечения национальной безопасности.

Стратегия развития ИИ во Франции представляет собой комплексную программу, нацеленную на укрепление обороноспособности государства и обеспечение защиты прав и свобод ее граждан. В условиях масштабных киберугроз во Франции основным элементом этой стратегии является разработка систем киберзащиты, основанных на алгоритмах машинного обучения и нейронных сетях, позволяющих осуществлять комплексный анализ сетевого трафика в режиме реального времени.

Особое внимание во Франции уделяется защите объектов критической инфраструктуры. Французские специалисты разрабатывают интеллектуальные системы мониторинга, способные прогнозировать и предотвращать сбои в сложных системах.

Французская оборонная доктрина также предусматривает масштабное использование ИИ в системе военного управления и логистической деятельности. Так, одной из главных задач в этой области является развитие систем вооружений с использованием ИИ с целью повышении их тактической гибкости и адаптивности к обстановке.

Кроме того, французские исследователи разрабатывают новейшие системы видеоаналитики и поведенческого анализа, основанные на алгоритмах компьютерного зрения и обработки языка, для использования, например, на транспортных узлах и в местах массового скопления людей. В качестве примера можно привести внедрение в парижском метрополитене интеллектуаль-

ной системы видеонаблюдения, способной в режиме реального времени выявлять нестандартное поведение и потенциальные угрозы безопасности пассажиров.

Французская стратегия предусматривает создание интегрированных систем управления критической инфраструктурой на базе ИИ. Так, создаются модели для энергетических и транспортных сетей, способные прогнозировать и предотвращать аварии и сбои. Ключевым элементом этой стратегии стало внедрение суперкомпьютера Jean Zay, обеспечивающего возможность обработки и анализа данных в режиме реального времени.

Опыт Франции по внедрению ИИ в систему национальной безопасности, действительно интересен, поскольку демонстрирует возможность эффективного использования новейших технологий для укрепления обороны и обеспечения безопасности государства.

Вместе тем самым прогрессивным опытом применения ИИ в вопросах обеспечения национальной безопасности является опыт США. Национальная стратегия США по ИИ, обновленная в 2023 году, нацелена на создание надежных систем с целью эффективного противодействия современным угрозам в сфере безопасности. В данном контексте одной из важнейших задач считается разработка инновационных систем защиты критической инфраструктуры от кибератак. При этом особый акцент делается на создание алгоритмов, которые обладают возможностью нейтрализовать известные киберугрозы, а также противостоять новейшим типам атак.

Известно, что кибератаки являются наиболее быстро распространяющимся преступлением в США, постоянно увеличиваясь в размерах, сложности и стоимости наносимого ущерба. Так, взлом Yahoo (крупнейший за всю историю) затронул 3 млрд учетных записей пользователей, а атака на Equifax в 2017 г. — 145,5 млн клиентов, что превзошло крупнейшие взломы, о которых когда-либо сообщалось. Эти крупные кибератаки наряду с кибератаками

WannaCry и NotPetya<sup>29</sup>, которые произошли в 2017 г., не только масштабнее и сложнее, чем предыдущие, но и свидетельствуют о развитии криминальных кибертехнологий<sup>30</sup>.

В военной сфере США ИИ применяется с целью осуществления комплексного анализа больших данных и управления беспилотниками. Внедрение автономных ИИ-комплексов позволяет в разы повысить оперативность обработки информации и принятия решений в режиме реального времени, что имеет важное значение как для защиты государственных границ, так и для проведения военных операций в современных условиях<sup>31</sup>.

США постоянно взаимодействуют с международными партнерами по вопросам разработки и имплементации новых стандартов в сфере ИИ с целью создания глобальной системы безопасности, в основе которой лежит соблюдение этических норм и ответственное использование технологий ИИ.

В конечном счете, стратегия США в области применения ИИ в сфере обеспечения национальной безопасности показывает многоаспектный подход, сочетающий инновации с международным сотрудничеством, что позволяет государству эффективно противостоять современным угрозам, одновременно сохраняя лидирующую позицию в сфере развития и практического применения передовых технологий ИИ.

По нашему мнению, уже принятые правовые акты федеральных органов исполнительной власти в области национальной безопасности, касающиеся искусственного интеллекта, не в полной мере учитывают его потенциал.

---

<sup>29</sup> кибератаки WannaCry и NotPetya представляли собой взлом серверов, приведший к нарушению функциональности целого ряда крупных корпораций более чем в 150 странах и, как результат, к перерыву в их работе и многим другим потерям, превысившим, по оценкам некоторых компаний, 300 млн дол. США.

<sup>30</sup> Суходолов А.П., Антонян Е.А., Рукинов М.В., Шамрин М.Ю., Спасенникова М.Г. Всероссийский криминологический журнал. 2019. Т. 13. № 4. С. 558.

<sup>31</sup> NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH AND DEVELOPMENT STRATEGIC PLAN 2023 UPDATE.

A Report by the SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE of the NATIONAL SCIENCE AND TECHNOLOGY COUNCIL May 2023. P.16-17. URL: <https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf> (дата обращения: 20.09.2024).

Так, ведомственная программа цифровой трансформации МВД России на 2022 - 2024 годы<sup>32</sup> упоминает искусственный интеллект лишь несколько раз. Одна из задач программы – ликвидация имеющихся отставаний по вопросам применения технологий искусственного интеллекта, должна быть решена посредством технических заданий на опытно-конструкторские работы по внедрению технологий искусственного интеллекта в 2021<sup>33</sup> и 2022 гг.

При этом количество доступных дата-сетов (наборов данных) для реализации задач искусственного интеллекта, указанное в программе по годам, запланировано в количестве 0 (нуля) сетов для каждого года (см. Раздел 1 «Показатели результативности цифровой трансформации» названной программы). Предусмотренный программой План внедрения искусственного интеллекта в деятельности МВД России на 2021 год и плановый период 2022 и 2023 годов не согласован с общими сроками самой программы, которая рассчитана и на 2024 год (см.: Раздел 3 «Методика расчета показателей Программы»). За внедрение искусственного интеллекта в деятельность МВД России ответственен Департамент информационных технологий, связи и защиты информации МВД России<sup>34</sup>.

В то же время схожая ведомственная программа, действующая в Росгвардии, имеет иные показатели. Согласно данной программе, в 2023 году должно быть не менее одного дата-сета (набора данных) для реализации задач искусственного интеллекта, а в 2024 году – не менее двух<sup>35</sup>.

Минобороны России не ставит задачей внедрение искусственного интеллекта в своей деятельности, ограничиваясь лишь упоминанием искусствен-

---

<sup>32</sup> См.: Распоряжение МВД России от 11.01.2022 N 1/37.

<sup>33</sup> С учетом того, что программа была принята в 2022 г.

<sup>34</sup> П. 12.62 Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации (утв. приказом МВД России от 15.06.2021 N 444).

<sup>35</sup> Ведомственная программа цифровой трансформации Федеральной службы войск национальной гвардии на 2022 год и на плановый период 2023 - 2024 годов".

ного интеллекта в нормативных актах, посвященных деятельности технополиса «Эра»<sup>36</sup>, и Порядка разработки и утверждения программ развития федеральных государственных образовательных организаций высшего образования, находящихся в ведении Министерства обороны Российской Федерации<sup>37</sup>.

Представляется, что МВД России и Минобороны России следует предусмотреть реальные количественные показатели внедрения искусственного интеллекта.

## **II. Цифровое административное усмотрение в системе обеспечения национальной безопасности**

Системное нормативно-правовое регулирование ИИ, равно как и регламентация административного усмотрения органов исполнительной власти и их должностных лиц, а также административного усмотрения роботов (цифрового административного усмотрения), в отечественном законодательстве к настоящему моменту времени отсутствует. Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона “О персональных данных”» системообразующим в данной сфере считаться не может, поскольку является лишь экспериментальное регулирование, которое проводится при этом не в масштабах

---

<sup>36</sup> П. 1.12 Приложения N 4 к Порядку получения статуса участника Военного инновационного технополиса "Эра" Министерства обороны Российской Федерации (утв. заместителем Председателя Правительства Российской Федерации, председателем Совета Военного инновационного технополиса "Эра" Минобороны России 31 мая 2022 г. N 5709п-П22).

<sup>37</sup> Абз. 5 пп. 2 п. 9 Порядка разработки и утверждения программ развития федеральных государственных образовательных организаций высшего образования, находящихся в ведении Министерства обороны Российской Федерации (утв. приказом Минобороны России от 22.09.2022 N 565) // Официальный интернет-портал правовой информации <http://pravo.gov.ru>, 27.10.2022.

всей страны, а лишь на территории столицы. Однако в нормах этого закона дается легальное определение искусственного интеллекта как «комплекса технологических решений, позволяющего **имитировать** когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека» (см. п. 2 ч. 1 ст. 2 указанного закона). Что же касается цифрового административного усмотрения, то даже и легальная его дефиниция пока не выработана.

Вообще административное усмотрение трактуется в юридической науке по-разному: как степень доверия к должностному лицу<sup>38</sup>; как право администрации самостоятельно оценивать условия, в которых применяется закон, чтобы избрать наиболее целесообразное решение из всех тех, которые предоставляются законом<sup>39</sup>; как оценка фактических обстоятельств, основания (критерии) которой не закреплены в правовых нормах достаточно полно или конкретно, производимая органом исполнительной власти (должностным лицом) при выборе оптимального варианта решения конкретного управленческого вопроса в пределах, допускаемых нормативными актами<sup>40</sup>; как некоторая степень оперативной самостоятельности органа государственного управления в принятии решения о том, вступать или не вступать в действие в том или ином случае, в выборе момента вступления в действие и наиболее целесообразного, по мнению данного органа, решения вопроса из нескольких допускаемых законом вариантов<sup>41</sup>. Известно и множество других определений.

---

<sup>38</sup> См.: Зайцев Д.И. Генеалогия административного усмотрения // Сибирское юридическое обозрение. 2023. Т. 20. № 3. С. 272-284.

<sup>39</sup> См.: Социалистическая законность в советском государственном управлении / А.Е. Лунев, С.С. Студеникин, Ц.А. Ямпольская; под общ. ред. С.С. Студеникина. М., 1948. 136 с.

<sup>40</sup> См.: Соловей Ю.П. Усмотрение в административной деятельности советской милиции : автореф. дис. ... канд. юрид. наук. М., 1982. С. 20.

<sup>41</sup> См.: Лазарев Б.М. Компетенция органов управления. М., 1972. С. 92; Тихомиров Ю.А. Управленческое решение. М., 1972. С. 143.

Важность проблематики административного усмотрения подтверждается живым интересом, проявляемым к ней со стороны научного сообщества.

Так, Ю.А. Тихомиров, исследуя вопросы прогнозирования и рисков в праве, говорит о важности корреляции между статусом бизнес-структур и текущими решениями, между принципами политики государства и возможными последствиями реализации новых правовых актов, а главное – между **сферой усмотрения** и имеющими непосредственное отношение к национальной безопасности **коррупционными рисками**<sup>42</sup>. Он же писал и о «**патологии усмотрения**» как о крайне негативном, чрезвато самыми отрицательными последствиями для государства и общества в целом и для отдельных граждан в частности.

В науке не сложилось единого подхода к судьбе административного усмотрения в условиях цифрового общества и, как следствие, в условиях наступающей эпохи ИИ.

Одна группа ученых пришла к выводу, что роль административного усмотрения существенно уменьшилась вследствие появления новой задачи должностных лиц – оценивать деятельность ИИ. Цифровизация, по их мнению, серьезно сократила круг вопросов, входящих в компетенцию служащих, приняв на себя «простейшие управленческие функции»<sup>43</sup>.

Так, по мнению А.В. Мартынова, при принятии управленческого решения на основе ИИ практически сокращается или даже **обнуляется** возможность административного усмотрения<sup>44</sup>. Это означает возможное игнорирование тяжелых жизненных ситуаций, социально-политических условий. Достижимость целей и задач государственного управления, лишенного справедливости и гуманизма, представляется сомнительной.

---

<sup>42</sup> См.: Тихомиров Ю.А. Прогнозы и риски в правовой сфере // Журнал российского права. 2014. №3 (207).

<sup>43</sup> См.: Зайцев Д.И. Административное усмотрение в цифровую эпоху // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 11. С. 203.

<sup>44</sup> См.: Мартынов А.В. Актуальные вопросы применения искусственного интеллекта при осуществлении контрольно-надзорной деятельности органов исполнительной власти // Вестник Нижегородского университета им. Н.И. Лобачевского. 2020. N 2. С. 184.

Однако существует и другая позиция, согласно которой цифровизация не лишила должностных лиц, «надзирающих» за решениями ИИ, должной степени усмотрения<sup>45</sup>.

Мы считаем, что именно вторая позиция в большей степени соответствует фактическому положению дел. Думается, что с развитием цифровых технологий дискреция в качественном измерении осталась прежней, а в количественном – или увеличилась (в ситуациях, когда технологии искусственного интеллекта ускоряют ведение юридически значимых действий), или же не изменилась<sup>46</sup>.

Справедливости идеи о сохранении административного усмотрения придают и мысль о том, что «исполнительно-распорядительная деятельность, как и всякая иная публично-властная деятельность, **невозможна** без определенного пространства свободного усмотрения должностных лиц (административное усмотрение)»<sup>47</sup>.

Если же степень усмотрения государственного служащего ограничивается, то его личность рефлекторно приспособляется к совершению рутинных и стереотипных действий, что, с одной стороны, ускоряет течение административных процедур и производств, а с другой – притупляет внимательность служащего, его способность индивидуализировать административные дела, вникать в суть ситуации, видеть фактическую, а не формальную, сторону дела.

Цян Юэ и К.В. Кичик отмечают, что в Стратегии развития искусственного интеллекта на период нет какого-либо упоминания о применении ИИ для национальной безопасности и обороны. По мнению авторов, это является

---

<sup>45</sup> См.: Boer N. de, Raaphorst N. Automation and discretion: explaining the effect of automation on how street-level bureaucrats enforce // Public Management Review. 2021. May. P. 12.

<sup>46</sup> О терминах «качественные и количественные объемы дискреционных полномочий» см.: Щепалов С.В., Зайцев Д.И. Административное и судебное усмотрение в российской науке: проблемы соотношения // Вестник Томского государственного университета. Право. 2022. № 46.

<sup>47</sup> Краснов М.А., Талапина Э.В., Южаков В.Н. Коррупция и законодательство: анализ закона на коррупциогенность // Журнал российского права. 2005. № 2.

большим упущением. Военные, командно-административные, компьютерные, коммуникационные, разведывательные и наблюдательные системы российского оборонного ведомства достигли значительного прогресса. Применение технологий ИИ в этих областях может способствовать их дальнейшему развитию и влиянию на иные сферы общественных отношений, в частности – на сферу обеспечения национальной безопасности<sup>48</sup>.

Как справедливо отмечено А.А. Карцхия, ИИ является квинтэссенцией технологий двойного назначения, поскольку способен воспринимать, оценивать и действовать быстрее и точнее, чем человек, представляя таким образом конкурентное преимущество в любой области – гражданской или военной.

Технологии ИИ оказываются средством власти как для бизнес-структур, так и для государств<sup>49</sup>. Они расширяют зону уязвимости друг друга, а расширение возможностей ИИ становится инструментом первой необходимости в новую эпоху конфликтов<sup>50</sup>. Геополитические противники разрабатывают технологии применения искусственного интеллекта в военных и иных вредоносных целях.

Относительно доступные широким массам технологии искусственного интеллекта также таят опасность для национальной безопасности. Угрозы варьируются от технологий deepfake, используемых как для безобидных шуток, так и для создания заведомо ложного общественно значимого контента, до беспилотных летательных аппаратов.

Несомненна истинность слов А.А. Карцхия: «Цифровая зависимость во всех сферах жизни превращает личные и коммерческие уязвимости в потен-

---

<sup>48</sup> Юэ Цян, Кичик К.В. Исследование российской стратегии развития искусственного интеллекта через призму концепции верховенства права // Право и цифровая экономика. 2023. № 2. С. 14–24.

<sup>49</sup> THE NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE (USA), Final Report, [https://cybercemetery.unt.edu/nscai/20211005231042mp\\_/https://www.nscai.gov/wp-content/uploads/2021/03/Final\\_Report\\_Executive\\_Summary.pdf](https://cybercemetery.unt.edu/nscai/20211005231042mp_/https://www.nscai.gov/wp-content/uploads/2021/03/Final_Report_Executive_Summary.pdf).

<sup>50</sup> См.: Карцхия А.А. Правовая охрана достижений искусственного интеллекта // ИС. Авторское право и смежные права. 2024. № 4. С. 4–16.

циальные недостатки национальной безопасности, а нарастающий шторм иностранного влияния и вмешательства делает необходимыми организационные и политические реформы для повышения нашей устойчивости».

Однако искусственный интеллект, допускающий усмотрение в принятии решений, может быть полезен в национальной безопасности.

Так, С.С. Горохова пишет о передовых разработках отечественной оборонной промышленности. В январе 2020 года Уральский завод гражданской авиации завершил испытания экспериментального образца перспективного беспилотного летательного аппарата «Альтиус-У», оснащенного спутниковым каналом обмена данными и управления, создание которого ведется по проекту «Альтаир». Разработка беспилотника «Альтиус» осуществляется с 2011 года. Кроме того, в ноябре 2016 года Воздушно-космические войска России приступили к опытной эксплуатации перспективных ударных беспилотников «Орион». Экспортная версия данного БПЛА была представлена на авиасалоне МАКС-2017. Максимальная взлетная масса аппарата составляет 1,2 тонны, максимальная продолжительность его полета – 30 часов, а высота полета – около 8 тысяч метров. Беспилотный аппарат может нести боевую нагрузку массой до 450 килограммов<sup>51</sup>.

Беспилотные летательные аппараты могли бы, действуя под контролем оператора, самостоятельно, **по своему усмотрению**, определять и захватывать цели, а решение о применении боезапаса принимал бы уже оператор. Подобный опыт (правда, без участия оператора), по словам С.С. Гороховой, уже реализован в летальных автономных оружейных системах (LAWs) – особом классе оружейных систем, способных самостоятельно идентифицировать цель и использовать бортовую оружейную систему для поражения и уничтожения ее без участия человека. LAWs требуют наличия системы компьютерного зре-

---

<sup>51</sup> См.: Горохова С.С. Искусственный интеллект в контексте обеспечения национальной безопасности // Национальная безопасность / nota bene. 2020. № 3. С. 15–31.

ния и продвинутых алгоритмов машинного обучения для классификации объекта как враждебного, принятия решения о захвате и направлении оружия к цели<sup>52</sup>.

Национальную безопасность нельзя сводить к деятельности только лишь вооруженных сил, полиции, национальной гвардии и органов государственной безопасности. В Стратегии национальной безопасности РФ в качестве одной из задач указано повышение доверия граждан к судебной системе Российской Федерации, совершенствование системы общественного контроля, механизмов участия граждан и организаций в обеспечении государственной и общественной безопасности.

Доверие граждан к судебной системе проявляется в рамках судопроизводства. Правосудие как приоритетный способ защиты прав и свобод человека и гражданина, сталкивается с множеством проблем. Но «традиционной» проблемой является высокая доли нагрузки на судей.

Как отмечает Э.В. Талапина, одним из направлений исследовательской работы и практического применения технологий ИИ является попытка объединения алгоритмов ИИ с процессом правового мотивирования судебных актов<sup>53</sup>. Полагаем, что эта работа актуальна и для аналогичного упрощения внесудебной деятельности публичной администрации как, несомненно, более масштабной части механизма правоприменения в Российском государстве.

Судебные акты, принимаемые с участием искусственного интеллекта, по мнению Э.В. Талапиной, должны обосновываться на комплексе так называемых «опорных компонентов» – достаточности доказательств по делу, критическом анализе процедур оценки доказательств и его применения в выработке позиции по делу, логическом сопоставлении оцененных доказательств обстоятельствам дела, оценке самих обстоятельств, установленных в ходе су-

---

<sup>52</sup> См.: Горохова С.С. Указ. соч.

<sup>53</sup> См.: Талапина Э.В. Искусственный интеллект в правосудии: небольшой обзор больших последствий // Российская юстиция. 2024. № 5.

допроизводства. Однако автор справедливо констатирует, что ИИ невосприимчив к пониманию природы права и контексту принимаемых законов, хотя и способен работать с «опорными компонентами».

Сопоставимые компоненты имеются и у административного процесса, но в несколько упрощенном виде. Применительно к административной ответственности – важного элемента системы обеспечения национальной безопасности – цифровые технологии длительное время применяются для фиксации административных правонарушений в области дорожного движения и благоустройства территорий, т.е. для установления факта и доказательств события административного правонарушения и его совершения собственником конкретного автомобиля (регистрационный номер, скорость движения, дорожная разметка и т.д.).

Оценку качества зафиксированных данных проводят должностные лица соответствующих органов административной юрисдикции (органы внутренних дел РФ, органы исполнительной власти субъектов РФ). Именно они сохраняют за собой полномочия по реализации мер административного принуждения в виде принятия постановлений о наложении административного штрафа. Но стоит признать, что участие человека в изложенном процессе уже сведено к минимуму<sup>54</sup>.

Судья или должностное лицо при принятии правоприменительного акта, разрешающего дело по существу, осознает сложившиеся условия, в рамках которого возникает дело. Судьи, осуществляя правосудие, например, по уголовным делам, принимают во внимание личность подсудимого, его мотивы и обстоятельства, способствовавшие совершению преступления. Усмотрение судьи здесь незаменимо – сомнительно, что ИИ сумеет проявить должное снисхождение или, напротив, большую строгость к лицу, будучи неспособным в полной мере уяснить **все обстоятельства** совершения преступления, кото-

---

<sup>54</sup> См.: Зайцев Д.И. Административное усмотрение в цифровую эпоху // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 11. С. 199–208.

рые не могут быть учтены в законе или алгоритме. Иное привело бы к ненужной казуистичности.

Административные же правонарушения рассматриваются по достаточно простым правилам (кроме правонарушений, рассматриваемых по правилам главы 25 АПК РФ). Та же упрощенность (причем совершенно неприемлемая) присутствует в процессе судебного обжалования вступивших в законную силу постановлений и решений по жалобам в кассационных судах общей юрисдикции и Верховном Суде РФ – жалобы рассматриваются судьей единолично без вызова заинтересованных лиц и судебного заседания. Это делает подсудность жалоб кассационным судам общей юрисдикции, учрежденным для изживания рудиментов надзорного производства в современной кассации, малоэффективным инструментом<sup>55</sup>. Но пока законодатель не признает ошибочность института судебного обжалования по главе 30 КоАП РФ и не передаст рассмотрение соответствующих жалоб в ведение административного судопроизводства по аналогии с кассацией по АПК РФ, потенциальное использование искусственного интеллекта при рассмотрении жалоб по КоАП РФ могло бы лишь незначительно ухудшить и без того ненадлежащую форму судебного контроля.

Как отметили И.Н. Спицин и И.Н. Тарасов, даже в бесспорных производствах необходимы не только формализованные действия, но и «смыслообразование» при работе с *оценочными категориями*. Авторы заметили, что даже в предельно простом производстве по вынесению судебного приказа, судьи в пределах своего усмотрения осуществляют юридическую квалификацию правоотношения как бесспорного, оценивая представленные заявителем письменные доказательства по собственному внутреннему убеждению – этому

---

<sup>55</sup> См.: Князькин С.И. Экстраординарный характер деятельности надзорной судебной инстанции в гражданском и арбитражном процессе России. М., 2015. 224 с.; Вольфсон В.Л. Непринужденная неустойчивость. О судьбах публичного интереса в пересмотре вступивших в силу судебных актов // Вестник Санкт-Петербургского университета. Серия «Право». 2014. Вып. 2. С. 6; Верещагин А.Н. О происхождении российской судебной системы и ее перспективах // Закон. 2019. № 4. С. 54–66; Жуйков В.М., Долова М.О. Актуальные проблемы унификации процессуального законодательства // Журнал российского права. 2019. № 8. С. 121–135.

способствует принцип свободной оценки доказательств<sup>56</sup>. При этом искусственный интеллект, по мнению И.Н. Спицына и И.Н. Тарасова, «не способен оперировать смыслами», поскольку оперирует исключительно синтаксисом, а не семантикой<sup>57</sup>.

То же касается и административного усмотрения. Например, принятие правоприменительных актов по вопросам гражданства Российской Федерации, выезда и въезда на территорию Российской Федерации, не может не сопровождаться анализом как данных личности лица, в отношении которого принимается решение, так и сопутствующей обстановки. Например, в условиях распространения опасных инфекционных заболеваний, угрозы террористических актов и иных неблагоприятных факторов, принятие правоприменительного акта на основе строго заданного системе набора информации влечет риски не только для нормального функционирования соответствующих органов публичной власти, от имени которых действует искусственный интеллект, но и для всей системы национальной безопасности.

Важное значение здесь приобретает не усмотрение как таковое, а фактор сомнения, неуверенности в правомерности поведения, вынуждающий должностное лицо применять весь набор законных средств для установления всех обстоятельств, игнорирование которых могло бы, пусть даже и косвенно, привести к нежелательным социальным последствиям. Именно с этих позиций административное усмотрение (равно как и судебное усмотрение) приобретает характер **необходимого** элемента, обосновывающего незаменимость человека в процессе принятия юридически значимых решений, который хотя и пользуется достижениями науки и алгоритмами искусственного интеллекта, **помогающих** в процессе принятия решения, но сохраняет свободу воли и продолжает нести ответственность за принимаемые решения.

---

<sup>56</sup> См.: Спицын И.Н., Тарасов И.Н. Разрешение споров с использованием технологии искусственного интеллекта на интернет-площадках (Amazon.com, Ebay и др.) // Арбитражный и гражданский процесс. 2021. № 8.

<sup>57</sup> См.: Searle J.R. Is the Brain's Mind a Computer Program? // Scientific American. Vol. 262. 1990. № 1. P. 20–25; Paul M. Churchland and Patricia Smith Churchland. Could a Machine Think? // Scientific American. Vol. 262. 1990. № 1. P. 26–31.

С другой же стороны, алгоритмы ИИ способны избежать маскируемых под «усмотрение» ошибок в правоприменительных актах, причиной которых могут быть недостаточно высокий уровень правовой культуры, либо коррупционные риски.

Что касается усмотрения не человека, а ИИ, то нужно отметить, что цифровое административное усмотрение рассматривается как замена «традиционного» усмотрения государственных служащих и лиц, осуществляющих публично-властные полномочия<sup>58</sup>. При этом цифровое административное усмотрение балансирует на грани между фактом и фикцией<sup>59</sup>.

Усмотрение человека и усмотрение ИИ имеют ряд принципиальных различий. Эмпирически подтверждено, что ИИ имеет преимущество перед человеческим в плане решения задач, характеризующихся высокой степенью неопределенности, но низкой сложностью. В то же время человеческий разум способен реагировать на вызовы, отличающиеся *неопределенностью*, что для искусственного интеллекта *пока* не достижимо<sup>60</sup>.

Вероятно, цифровое административное усмотрение будет уместно в тех областях функционирования исполнительной власти, где гражданин, попавший в затруднительную ситуацию, сможет самостоятельно выявить способы ее преодоления и предложить их искусственному интеллекту. Когда же, напротив, для поиска выхода из такой ситуации понадобятся специальные знания и профессиональные навыки, агентом публичной администрации должен быть именно человек, чьей ответственности добиться проще.

Другая проблема внедрения искусственного интеллекта в публично-управленческие процессы заключается в том, что он не соотносим с традиционными административно-правовыми категориями (компетенция, полномо-

---

<sup>58</sup> См.: Boer N. de, Raaphorst N. Automation and discretion: explaining the effect of automation on how street-level bureaucrats enforce // Public Management Review. 2021. May. P. 6.

<sup>59</sup> См.: Зайцев Д.И. Административное усмотрение в цифровую эпоху // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 11. С. 199–208.

<sup>60</sup> См.: Bullock J.B. Artificial Intelligence, Discretion, and Bureaucracy // The American Review of Public Administration. 2019. № 49. P. 6.

чия, ответственность, правонарушение, наказание), а также общечеловеческими ценностями (мораль, нравственность, совесть, справедливость, солидарность и др.). В этом смысле взаимодействие с машиной а priori непредсказуемо, ибо она может посчитать оптимальной такую рекомендацию, которая для человека окажется элементарно неприемлемой.

Если же допустить, что искусственный интеллект обретет достаточную свободу усмотрения в исполнительно-распорядительной деятельности, граждане станут общаться с соответствующими системами напрямую, без какого-либо посредничества со стороны государственных служащих. Последние же будут лишь проверять решения роботов, причем исключительно в тех случаях, когда на них поступят жалобы от граждан<sup>61</sup>.

Но по ряду «дискреционных» направлений контакт между гражданами и машинами будет, как минимум, неполноценным. Речь идет прежде всего о юрисдикционной деятельности, деятельности по предоставлению пенсий, социальных пособий и льгот, требующих от управленца понимания нуждаемости в получении соответствующих мер государственной поддержки, и других областях административного процесса, требующих не только знания закона, но и эмпатии. Ведь и государственное управление в целом, и его отдельные составляющие (например, государственные услуги) нередко рассматривают в качестве совместного творчества служащих и граждан, а основой такого со-творчества как раз и является административное усмотрение<sup>62</sup>.

Способность человека – должностного лица избегать ошибок в правоприменительной деятельности зависит от его правовой культуры. Аналогичная способность ИИ поставлена в зависимость от качества технической составляющей искусственного интеллекта, за которую также отвечают люди,

---

<sup>61</sup> См.: Paulin A. Digitalisation vs. Informatisation. Different Approaches to Governance Transformation // CEE Dem and Gov Days 2018. № 331. P. 257.

<sup>62</sup> См.: Muravska T., Stacenko S., Zeibote Z. Digitalisation in the Regional Context: The Case of E-Government Services in Latvia // Studia Europejskie — Studies in European Affairs. 2018. № 4. P. 259.

наделившие искусственный интеллект верным алгоритмам самообучения, включающим получение неверных выводов. Тут тоже есть поле для усмотрения, но уже не административного – формирование алгоритмов в процессе разработки программного обеспечения основывается на усмотрении технических специалистов, в том числе, при ошибочно понятом или ошибочно реализованном задании<sup>63</sup>.

Р.В. Амелин и С.Е. Чаннов приводят интересный случай – в 2009 году Саратовский облсуд своим решением прекратил функционирование программного средства оценки кадастровой стоимости, применяемого Федеральным государственным учреждением «Земельная кадастровая палата» по Саратовской области, поскольку для определенного вида объектов кадастрового учета в нем использовалась формула, не предусмотренная законом, а взятая по усмотрению разработчиками системы – это привело к приостановлению кадастровой оценки в регионе на несколько месяцев<sup>64</sup>. При этом в науке отмечается наличие усмотрения администраций технологических платформ распространения информации<sup>65</sup>.

### **III. Рекомендации для федеральных органов исполнительной власти по использованию искусственного интеллекта в обеспечении национальной безопасности**

Проведенное исследование позволило сделать вывод о том, что России необходимо следовать опыту США, Франции и о. Маврикий при использовании ИИ в решении вопросов обеспечения национальной безопасности. Этим государствам (США, Франции и о. Маврикий) удалось достичь положительного эффекта от использования ИИ в области национальной безопасности и,

---

<sup>63</sup> См.: Амелин Р.В., Чаннов С.Е. Эволюция права под воздействием цифровых технологий // СПС «Гарант».

<sup>64</sup> См.: Решение Саратовского областного суда от 2 февраля 2009 г. по делу № 3-1/2009.

<sup>65</sup> См.: Амелин Р.В., Чаннов С.Е. Указ. соч.

таким образом, минимизировать потенциальные риски в осуществлении государственного управления в административно-политической сфере. При этом необходимо иметь в виду, что активное использование ИИ требует значительных финансовых вложений.

Искусственный интеллект, как и всякая автоматическая система, должен внедряться в систему обеспечения национальной безопасности, но только в качестве помощника человека.

Многие риски, связанные с искусственным интеллектом, по своей природе имеют интернациональный характер, и поэтому необходимо международное сотрудничество, чтобы обеспечить ориентированный на человека, заслуживающий доверия и ответственный искусственный интеллект, который будет безопасен и послужит всеобщему благу. Сотрудничество могло бы включать в себя там, где это уместно, классификацию рисков на основе национальных условий и применимых правовых рамок, а также разработку общих принципов и кодексов поведения в области искусственного интеллекта.

В настоящее время весьма сомнительно, что цифровое административное усмотрение сможет найти место в системе обеспечения национальной безопасности. Искусственный интеллект – не субъект права. Единственной принудительной мерой в отношении искусственного интеллекта, применяемой в случае ошибок и иных нежелательных его проявлений, может быть его ограничение, а в качестве исключительной меры – отключение. Спектр же ответственности человека несоизмеримо шире.

Но опасность цифрового административного усмотрения в системе национальной безопасности заключается в самом риске ошибки. Всякая ошибка в публичном управлении, а тем более в системе обеспечения национальной безопасности влечет неблагоприятные социальные последствия как для самой системы обеспечения национальной безопасности, так и для населения. Ошибки систем обнаружения баллистических ракет могут привести к неоправданному применению ядерного оружия либо несрабатыванию мер защиты. Ошибки в уголовном судопроизводстве могут привести не только к

убыткам от незаконных следственных действий, но и, например, к оправданию лица, представляющего угрозу для государственной безопасности.

В целях совершенствования системы обеспечения национальной безопасности России представляется целесообразным внедрить технологии ИИ в работу федеральных органов исполнительной власти, реализующих свой правовой статус в административно-политической сфере. Среди таких органов могут быть названы Федеральная служба безопасности (далее – ФСБ России), Федеральная служба по финансовому мониторингу (далее – Росфинмониторинг), Федеральная служба по техническому и экспортному контролю (далее – ФСТЭК).

ФСБ России предлагается изучить возможность создания специализированного подразделения по использованию систем ИИ в контрразведывательных мероприятиях и противодействия терроризму. Это, безусловно, повысило бы эффективность работы системы мониторинга и аналитики информационных потоков в цифровом пространстве, основанной на методе компьютерной лингвистики. Подобное нововведение позволит анализировать любые текстовые материалы в Интернете в целом и в конкретных социальных сетях. Для этого потребуется наладить взаимодействие с лучшими IT-компаниями и научно-исследовательскими центрами по вопросу создания эффективного алгоритма обработки естественного языка и анализа сетевой активности.

Важно наладить функционирование системы предиктивной аналитики, на основе обработки больших данных. Данный шаг обеспечит выявление и дальнейший эффективный прогноз угроз безопасности государства. В этих целях, очевидно, потребуется обучение должностных лиц ФСБ по программе «Intelligence Community Data Strategy»<sup>66</sup> (Стратегия данных разведывательного сообщества). Подобной программе обучают сотрудников ЦРУ в США. В основе работы системы предиктивной аналитики лежит внедрение технологий

---

<sup>66</sup> <https://www.dni.gov/index.php/>.

ИИ в анализ информации, осуществляемый ФСБ РФ, что в разы позволяет повысить эффективность оперативно-розыскной деятельности.

Росфинмониторингу было бы целесообразно начать совместную работу с Центром технологий распределенных реестров СПбГУ по использованию ИИ для идентификации финансовых правонарушений, в том числе криптовалютных транзакций, способствующих легализации доходов, полученных преступным путем. В этих целях Росфинмониторингу следует взаимодействовать исключительно с указанным выше ведущим в России центром компетенций программы «Национальная технологическая инициатива» по развитию технологии и экосистемы блокчейн в России (Центр технологий распределенных реестров СПбГУ). Этот центр сможет наладить использование технологии распределенного реестра для выявления всех подозрительных операций. На следующем этапе не обойтись без разработки алгоритма машинного обучения уже для исследования этих финансовых операций и определения аномальных. Данные мероприятия позволят обеспечить выявление и прекращение действия криминальных схем вывода финансов за рубеж и финансирование терроризма. На завершающем этапе, после выявления незаконных транзакций в действие должна вступить система автоматизированного обмена информацией с банками и правоохранительными органами, работающая на базе технологий ИИ. То есть обмен информации будет осуществляться мгновенно и в автоматическом режиме.

ФСТЭК рекомендуется обратить внимание на необходимость внедрения ИИ по защите критической информационной инфраструктуры, что особенно важно в условиях проведения СВО, поскольку серьезную опасность представляет деятельность разведок США и Великобритании. Так, в мировой практике во всех подобных органах выработана рекомендация по формированию специального отдела информационной безопасности, в основе работы которого лежит использование технологии ИИ. Для сравнения отметим, что такая технология уже в успешно используется США и способствует автоматизирован-

ному обнаружению и предотвращению кибератак. Данная технология ориентирована на использование нейронных сетей. Представляется, что внедрение ИИ будет способствовать эффективной работе по предупреждению заражения вирусами программного обеспечения, влияющего на работу критически важных объектов, например, атомных станций и др.

В этом плане предлагается начать работу по подготовке проекта Федерального Закона «Об использовании технологий искусственного интеллекта в сфере национальной безопасности». Принятие такого закона позволило бы оформить легальное применение технологий ИИ и закрепить на законодательном уровне формы контрольно-надзорных мероприятий в сфере национальной безопасности.

Разработку данного проекта Закона необходимо осуществлять указанным федеральным органам исполнительной власти совместно, при этом координация этой работы должна осуществляться Советом Безопасности РФ. Именно на него Президенту РФ необходимо возложить контроль за подготовкой данного законопроекта.

Представляется, что реализация искусственного интеллекта в деятельности МВД России и Минобороны России происходит не вполне своевременно. Это проявляется, в частности, в отсутствии реальных числовых показателей внедрения дата-сетов (наборов данных) для реализации задач искусственного интеллекта.

Полагаем, что изменения следует внести в ведомственную программу цифровой трансформации МВД России на 2022 - 2024 годы<sup>67</sup>, а именно:

- продлить действие программы не более чем до 2030 г.;
- уточнить задачу программы «ликвидация имеющихся отставаний по вопросам применения технологий искусственного интеллекта» в части указа-

---

<sup>67</sup> См.: Распоряжение МВД России от 11 января 2022 г. № 1/37 «Об утверждении Ведомственной программы цифровой трансформации МВД России на 2022 – 2024 годы».

ния 2024 и последующих годов, во время которых МВД России должно осуществлять мероприятия по внедрению искусственного интеллекта, в том числе – технических заданий на ОКР;

– определить реальные показатели в виде натуральных чисел, обозначающих количество дата-сетов (наборов данных) для реализации задач искусственного интеллекта (от одного и более).

Минобороны России необходимо принять аналогичную ведомственную программу цифровой трансформации, учитывающую названные выше рекомендации.

При этом представляется, что при подготовке правовых норм для искусственного интеллекта (т.н. «машиночитаемого права») в указанных нормах не должно быть ни пробелов, ни коллизий, ориентирующих машину на бесконтрольное применение своих дискреционных полномочий. Причина этого заключается в том, что риски наступления негативных последствий, которые влечет за собой использование цифрового административного усмотрения, являются крайне высокими. В идеале в такой важной системе, как система обеспечения национальной безопасности, их не должно быть вообще.

В заключение необходимо отметить, что ИИ позволит избежать киберпреступности, повысить эффективность борьбы с финансированием терроризма, остановить вывод финансов за рубеж, фиксировать миллионы терабайтов противоправной информации и в автоматическом режиме мгновенно передавать её правоохранительным органам.