Цифровые алгоритмы государственного и муниципального контроля и надзора как риск для субъектов предпринимательской деятельности: правовые аспекты

Усольцева Наталья Андреевна,
канд.юрид.наук, доцент кафедры частного и предпринимательского права, Сургутский государственный университет, netali77@list.ru

Усольцев Юрий Михайлович,
доцент кафедры публичного и уголовного права, Сургутский государственный университет, yusoltsev@mail.ru

Цифровизация государственного и муниципального контроля и надзора, это не просто разговор про удобство для должностных лиц, проводящих соответствующие процедуры, это разговор, в том числе и о рисках для тех субъектов, которые попадают под контрольно-надзорные мероприятия. И такими субъектами сейчас являются субъекты предпринимательской деятельности. В основу всех процессов цифровизации и соответственно в основу принятия решения в рамках контрольно-надзорных мероприятий положены цифровые алгоритмы. И уже сейчас мы подошли к переломному моменту, когда цифровые алгоритмы станут самостоятельными субъектами контрольно-надзорных мероприятий в отношении субъектов предпринимательской деятельности. В подобной ситуации естественным становится вопрос о тех рисках, которые возникают у субъектов предпринимательской деятельности в подобной ситуации и о правовом статусе самого цифрового алгоритма. В основной части статьи исследуются вопросы понятия цифрового алгоритма и его статуса, определения его значения в разрезе правовой категории. Оценивается включенность цифровых алгоритмов в процедуры и процессы государственного и муниципального контроля и надзора. Выявляется главный вопрос – с какими рисками сталкиваются субъекты предпринимательской деятельности при проведении мероприятий государственного и муниципального контроля и надзора на основе цифрового алгоритма. В результате исследования делается вывод о необходимости определения статуса цифрового алгоритма при проведении контрольно-надзорных мероприятий на нормативно-правовом уровне и защите прав субъектов предпринимательской деятельности.

Ключевые слова: цифровые алгоритмы, государственный и муниципальный контроль и надзор, предпринимательская деятельность, риски субъектов предпринимательской деятельности, цифровизация государственного и муниципального контроля и надзора.

Исследование выполнено при финансовой поддержке Фонда научно-технологического развития Югры в рамках научного Проекта № 2023-05-01.

Введение

Наша современная действительность, которая складывается из повсеместной цифровизации всех процессов государственного и муниципального управления, процессов юридического сопровождения, не могла обойти своим вниманием механизмы государственного и муниципального контроля и надзора, и этого не произошло. Государственный и муниципальный контроль и надзор, особенно в отношении субъектов предпринимательской деятельности, максимально заведены на цифровые сервисы и решения, и в основу всего положен определенный цифровой алгоритм принятия решения.

И с одной стороны это очень удобно и современно, и даже прозрачно, но с другой стороны, возникает вопрос - почему в основу именно правовых, юридических значимых решений, влекущих за собой серьезные последствия, положен цифровой алгоритм? Допустимо ли это? И что мы знаем о цифровом алгоритме как категории и есть ли такая правовая категория? Не является ли цифровой алгоритм риском для субъектов, чья деятельность подлежит муниципальному контролю, а именно для предпринимателей?

Обсудим это. Начнем по порядку.

Материалы и методы

Методологической основой для исследования послужили общенаучные, а также частнонаучные методы. В качестве общенаучных использовались методы: анализ, сравнение, обобщение, описание, дедукция. Среди частнонаучных методов применялись формально-логический, сравнительно-правовой методы, а также метод юридической герменевтики, а также кибернетический метод.

Информационной основой для проведения исследования стали нормативные правовые акты и источники литературы по теме исследования. В частности были проанализированы работы таких исследователей как: Антропцева И.О., Казанцев Д.А., Киселев А.С., Липчанская М.А., Чаннов С.Е., Чурикова А.Ю., Понкин И.В. и других.

Основной раздел

В целом, алгоритм достаточно часто встречающееся понятие и предполагающее определенную последовательность действий, выполнение которой приводит к достижению конкретного результата [20, с. 46-48]. Алгоритм задает определенную последовательность действий и в этом ключе можно сказать, что нас повсеместно окружают алгоритмы.

Юридическая среда не является исключением, наоборот, можно сказать, что юридическая деятельность создана на основе алгоритмов. Любая последовательность юридических действий, приводящих к юридически значимому результату, является алгоритмом. Особенно ярко это представлено в ситуациях оказания государственной или муниципальной услуги, когда конкретный процесс построен на соответствующем административном регламенте.

Рассматривая ситуацию в этом контексте отметим, что процедуры государственного и муниципального контроля и надзора, являются юридическим алгоритмом, и результат проверочных мероприятий должен полностью соответствовать юридическому алгоритму проверки, закрепленному в основополагающих нормативных правовых актах.

Но это юридические алгоритмы, а как быть с цифровыми алгоритмами, и какая между ними разница?

Вернемся в начало разговора, что мы знаем об алгоритмах в целом и об их классификации в частности.

Итак, алгоритм - это конкретная последовательность действий, выполнение которой приводит к определенному результату. В цифровом мире алгоритмы являются основой для всей системы программирования и работы цифровых технологий. В информатике и математике алгоритм рассматривают как базовое понятие, представляющее собой набор последовательных инструкций и действий для достижения конкретного результата, для решения задачи.

Цифровые алгоритмы положены в основу деятельности всей вычислительной техники, автоматизированных процессов, программ любой сложности и сервисов. И здесь кроется основная проблема. Ведь если алгоритм ошибочен, то вынесенное на его основе решение то же будет ошибочным. А если это решение является основой для юридически значимых последствий, то кто будет отвечать за эти последствия?

Рассматривая цифровые алгоритмы как явление, встроенное в цифровые процессы, и являющееся базой для юридических действий мероприятий государственного и муниципального контроля и надзора, отметим, что такое явление нуждается в идентификации и определении его свойств.

Согласимся с уже существующим подходом, отмечающим, что все алгоритмы, в том числе и цифровые алгоритмы, характеризуются наличием следующих свойств:

- дискретность (внутренняя структура алгоритма последовательно структурирована);
- результативность (ориентированность на конкретный результат);
- детерминированность (однозначность каждого действия внутри алгоритма);
- массовость (применимость к любому множеству однотипных задач);
- конечность (последовательность алгоритма всегда завершается за определенное число действий) [3, с. 59-62].

Указанные свойства действительно обозначают цифровые алгоритмы как фундаментальное, базовое понятие, но точно не как правовую категорию.

В какой-то степени цифровой алгоритм можно рассмотреть и как философскую категорию, оценивая его способность к упорядочению реальности, и рассматривая весь мир через понятие алгоритмов в целом и через цифровые алгоритмы в частности [21; 22; 23], когда весь мир - это система цифровых вычислений.

Для понимания природы цифрового алгоритма как правовой категории стоит обозначить его как последовательность формализованных предписаний, являющуюся регулятором поведения участников правоотношений. В такой ситуации цифровой алгоритм становится не просто правовой категорией, но уже и объектом новых видов правоотношений. А если учесть, что цифровые алгоритмы являются основой для искусственного интеллекта, то на фоне существующих подходов о статусе искусственного интеллекта как субъекта правоотношений - цифровые алгоритмы могут существенно изменить логику правовых категорий, в том числе став субъектом права (хотя более правильным видится статус квази-субъекта) в категории «математическая модель» (своеобразная юридическая фикция).

Но вернемся к вопросу классификации цифровых алгоритмов, отметим, что она значительна и базируется на разных основаниях. Так, например, можно выделить классификацию по структуре, применению, способу представления, назначению и сложности. То есть в принципе любой цифровой алгоритм может быть абсолютно разнообразным с позиции классификации, например, линейный, основной, обработка данных, программный код и т.д. Представленная классификация дает представление о разнообразии цифровых алгоритмов как о базовом явлении, и даже больше, как о технической категории. Для идентификации цифрового алгоритма в качестве правовой категории, самому цифровому алгоритму должно быть дано правовое понятие, то есть должно быть встроено в правовую действительность не как технический, а именно как правовой термин. Стоит предположить, что для идентификации цифрового алгоритма как правовой категории ему стоит обозначить такие признаки как:

- конкретность цифрового алгоритма (то есть речь должна о чем-то выраженном, а не условно существующем);
- способность к автономному существованию цифрового алгоритма;
- быть связанным с правами и обязанностями разных субъектов;
- наличие юридически значимых последствий от его существования и применения;
- наличие условий и элементов ответственности.

При подобных признаках цифровых алгоритмов как правовой категории обозначим, что он уже максимально близко подошел к данному статусу.

Для классификации цифрового алгоритма как правовой категории более уместно было бы разделение на алгоритмы, участвующие в государственном и муниципальном управлении или государственном и муниципальном контроле и надзоре; степень автономности цифрового алгоритма; классификация по последствиям его деятельности или применения; по назначению.

Оценивая названные характеристики и свойства цифровых алгоритмов, отметим, что в текущем состоянии цифровой алгоритм остался в статусе базового понятия, и остается вопрос - является ли он основой для автоматизированного принятия юридически значимых решений в ситуации с государственным и муниципальным контролем и надзором, и насколько это допустимо.

Оценим ситуацию, которая складывается на настоящий момент, и проанализируем, существует ли угроза для субъектов предпринимательской деятельности при осуществлении государственного и муниципального контроля и надзора именно от использования цифровых алгоритмов. Поговорим немного о государственном и муниципальном контроле и надзоре, и роли цифровых алгоритмов в нем.

Фактически государственный и муниципальный контроль и надзор можно рассмотреть как самостоятельный элемент управленческой деятельности государственных и муниципальных органов власти, особенно исходя из логики, что управление это целенаправленное воздействие субъекта управления на объект управления с разнообразными целями: эффективность функционирования, приведение в упорядоченное состояние, недопущение нарушения закона и т.д. [2, с. 7-10].

При проведении контрольно-надзорных мероприятий необходимо соблюдение основных общих принципов [12; 15], причем сейчас уже можно говорить, что цифровые алгоритмы встроились в контрольно-надзорные мероприятия даже на их уровне, и даже произошла соответствующая трансформация принципов. Поговорим о некоторых из них.

1. Принцип законности - основополагающий принцип всех видов контроля и надзора, основанный на строгом выполнении требований закона при назначении, проведении контрольно-надзорных мероприятий (действия самих

проверяющих в том числе) и принятии решений по их итогам [16].

2. Принципы достоверности и объективности проведения контрольно-надзорных мероприятий предполагает, что решения по итогам контрольно-надзорных мероприятий базируются на законно собранных, достоверных и объективных доказательствах и данных. При этом указанные решения не должны основываться на чьих-то мнениях и позициях внутренних или внешних, в том числе не зависеть от личного мнения проверяющего. Именно на базе этих принципов можно начать говорить о закреплении цифрового алгоритма как элемента контрольно-надзорных мероприятий. Ведь сбор данных и доказательств осуществляется на анализе и обработке информации в открытых и закрытых информационных системах. Считается, что указанные цифровые алгоритмы работают с учетом требования законодательства РФ и позволяют сделать проверку быстрее, качественнее, объективнее и достовернее, без лишних контактов и субъективного мнения [2, с. 7-12]. Не можем с этим не согласится. Только остаются сомнения, в частности - остался ли цифровой алгоритм лишь инструментом контрольно-надзорных мероприятий, не стал ли он их субъектом. И в подтверждение указанных сомнений обозначим повторно, что цифровые алгоритмы являются основой всех, даже самых сложных программ, в том числе и самообучающихся. А значит, со временем, участником таких контрольно-надзорных мероприятий станет уже не просто цифровой алгоритм, а искусственный интеллект [5; 11]. А может ли цифровой алгоритм допустить ошибку при проверке данных, может ли сам алгоритм иметь ошибку, допустить ошибку, произойти сбой программы или проявить симпатию/антипатию, если он самообучающийся, и ответ - однозначно да. Будут ли достоверны и объективны результаты контрольно-надзорных мероприятий, если оставить их только цифровому алгоритму и убрать основного субъекта - человека? И ответ - однозначно нет. Цифровой алгоритм должен оставаться исключительно инструментом контрольно-надзорных мероприятий без права на принятие решения. Основным субъектом проверки должно остаться проверяющее лицо, служащий, несущий за свою деятельность, в том числе, уголовную ответственность.

3. Еще один принцип, связанный с использованием цифровых алгоритмов (и они здесь также исключительно приветствуются, по мнению ведущего числа ученых и специалистов [1, с. 81-82; 9, с. 120-121]) - это принцип независимости. Он в некоторой степени сродни принципу объективности, и предполагает, что субъект проверки независим от всех, и от органов власти разного уровня и от самого объекта проверки. И именно здесь приветствуются цифровые алгоритмы, так как именно они обеспечивают эту независимость - в материалах проверки ничего нельзя исправить и подправить - все данные выгружены из алгоритмичных систем и ими же обнаружены. Но риски угрозы сохраняются путем воздействия через авторов программ, операторов, технических аудиторов и т.д. Цифровые алгоритмы могут быть изменены, переписаны, дискредитированы.

Несомненно, что это далеко не все принципы, но у нас не было задачи обозначить их все, мы просто посмотрели на ситуацию внедрения цифровых алгоритмов в контрольно-надзорные мероприятия с их позиции. Логично предположить, что внедрение цифровых алгоритмов в мероприятия государственного и муниципального контроля и надзора потребует разработки специальных общих руководящих начал, и такие уже формируются в теории права [18, с. 9-11].

Предполагается, что эти начала и иные правила будут определять уже цифровые ценности: цифровое доверие, достоверность и безопасность данных, бесперебойное функционирование информационных систем, исключение третьих лиц из системы функционирования цифровых алгоритмов (что практически невозможно, так как обеспечительная функция деятельности цифровых алгоритмов остается у внешних исполнителей, например, у авторов или правообладателей, у технической поддержки) и другие. Все эти руководящие начала выделяются при любом встраивании цифровых технологий в любые виды процессинговой деятельности, и в государственный и муниципальный контроль и надзор в том числе.

Несомненно, что появление базовых правил для использования цифровых алгоритмов, создаст некую обеспечительную функцию для их внедрения. Правовым же основанием должен стать конкретный нормативный правовой акт, определяющий использование цифровых алгоритмов в конкретном виде государственного или муниципального контроля и надзора, его функционале, роли и задачах, а также последствиях применения. И если цифровой алгоритм становится единственным участником проверки (то есть он получает роль субъекта контрольно-надзорного мероприятия) - то порядок обжалования и особенности доказывания по таким категориям дел.

Оценивая ситуацию с нормативным правовым регулированием цифровизации государственного и муниципального контроля и надзора, отметим, что преимущественно базовое регулирование осуществляется за счет: Федерального закона от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»; Федерального закона от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»; Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [17]; Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [14]; Постановления Правительства РФ от 21.04.2018 № 482 «О государственной информационной системе «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» [13] и других нормативных правовых актов.

Касательно уже введенных и используемых цифровых сервисов (и соответственно – цифровых алгоритмов) в системе государственного и муниципального контроля и надзора стоит отметить:

- Государственную информационную систему «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» (ГИС ТОР КНД), которой пользуется значительное число государственных органов разного уровня;

- Единый реестр контрольных (надзорных) мероприятий (ЕРКНМ);

- Автоматизированные системы АСК НДС-3, АИС «Налог-3» (АИС «Налог-4»); ЭКГ-рейтинг; ИИ-скоринг; Налоговый мониторинг;

- и другие цифровые сервисы и решения государственных органов власти разного уровня, а также сервисы, используемые для муниципальных проверок.

В контексте перспектив развития цифровых технологий и повсеместного внедрения искусственного интеллекта можно предположить, что механизмы государственного и муниципального контроля и надзора тоже станут платформой для такого внедрения. Существует уже значительное число исследователей, отмечающих значительные плюсы такого внедрения - беспристрастность, объективность, постоянность сбора данных для проведения контрольно-надзорных мероприятий. При этом существует и понимание того, что такие цифровые алгоритмы будут осуществлять такие контрольно-надзорные мероприятия без присутствия человека, действуя от имени

уполномоченного государственного или муниципального органа власти.

И здесь, в том числе возникает вопрос о рисках для субъектов предпринимательской деятельности, которые становятся объектом контрольно-надзорных мероприятий, проводимых с применением цифровых алгоритмов и о возможном ущербе для них [19, с.77-79].

Классически выделяют риски, связанные с самими данными и в целом с информационной безопасностью [10, с. 86-87] (внутренней и внешней). В принципе ситуация с этими рисками уже всем хорошо знакома и требует в большей степени не столько нормативного регулирования, сколько соблюдения требований и условий безопасности со стороны самих субъектов видов деятельности. Причем это касается и ситуации с государственным и муниципальным контролем и надзором, когда подобные требования по информационной безопасности уже распространяются на государственных и муниципальных служащих.

Более сложной становится ситуация с иными рисками, и здесь в первую очередь стоит назвать «человеческий фактор», связанный с применением цифровых технологий. Сюда можно отнести все категории пользовательских рисков (действия пользователей, в результате которых третьи лица получают доступ к ресурсам или информации соответствующего субъекта), а также умышленные действия определенных специалистов, связанных с обеспечением информационной безопасности, техническим сопровождением, программированием и т.д. Главным условием для обеих групп рисков становится «уход» информации из компании, доступ третьих лиц к ресурсам, отказы и ошибки программного обеспечения и т.д., что приводит к значительному ущербу. Разграничение данных групп субъектов и соответственно рисков считаем обязательным, так как уровень ответственности, трудовые права и обязанности у них значительно различаются, и говорить о гражданско-правовой и иной ответственности нужно в разных объемах.

Дополнительно стоит выделить риски, связанные с техническими ошибками цифровых алгоритмов (не предполагающие «человеческий фактор»). Например, цифровой алгоритм создан искусственным интеллектом, и иные похожие ситуации. В этой ситуации стоит продумать систему ответственности за действия соответствующего цифрового алгоритма - найти крайнего в цепочке ответственности. Полагаем, что гражданско-правовой договор, на основе которого будет предоставлено право пользования соответствующим цифровым алгоритмом, в обязательном порядке должен отвечать на вопрос об ответственности в подобных ситуациях. В системе контрольно-надзорных мероприятий оба названных риска имеют критически важное значение, так как ущерб для объекта проверки при утечке данных, доступе к внутренней информации субъекта предпринимательской деятельности, ошибочных решениях о привлечении объекта проверки к ответственности, и прочих обстоятельствах, будет очень значительным.

Еще один риск, который уже достаточно давно описывается не только писателями-фантастами, но учеными-правоведами - бесконтрольность искусственного интеллекта [7, с. 457-458; 8, с. 139-140]. Причем здесь речь может идти и о слабом нормативном правовом сопровождении процесса внедрения искусственного интеллекта в разные сферы деятельности (сейчас эту проблему пытается решить государство, так как разработан и принят Государственной Думой РФ проект Федерального закона «О поддержке развития технологий искусственного интеллекта в Российской Федерации» [6]), но и о простом контроле за искусственным интеллектом со стороны пользователей. Наличие искусственного интеллекта любого уровня (и сильного, и слабого), к сожалению, предполагает изначально слабый уровень контроля со стороны юридического или физического лица в ситуации с возможностями его использования. Конечно, мы понимаем, что основная масса юридических лиц вводит на локальном уровне определенного рода регулирование, связанное с возможностями использования искусственного интеллекта. Но в любом случае проблемы сохраняются: это и использование ненадежного искусственного интеллекта, и использование искусственного интеллекта без маркировки контента, и использование сотрудниками без уведомления работодателя, в том числе для выполнения трудовых задач и создания продуктов. Все это усиливает проблемы слабого контроля.

Ситуация с контролем за искусственным интеллектом усугубляется дополнительным риском - риском принятия решения цифровым алгоритмом без участия человека. В ситуации с государственным и муниципальным контролем и надзором такое решение будет принимать искусственный интеллект, действуя от имени соответствующего органа власти, и это решение даже не будет проверяться уполномоченным специалистом, и автоматически будет предполагать привлечение субъекта предпринимательской деятельности к ответственности. И ситуация усугубляется на фоне следующего риска, а именно риска фактической презумпции достоверности всех цифровых материалов и заключений, как следствии - вины субъекта предпринимательской деятельности при проведении контрольно-надзорных мероприятий с использованием цифровых технологий. Речь не идет об отмене презумпции невиновности, речь идет именно о презумпции достоверности всех выводов, решений, аналитики, собранных цифровыми сервисами.

Риски прогнозирования виновного поведения объекта контрольно-надзорных мероприятий и осуществление постоянного мониторинга (наблюдения) - это один из самых критических рисков, так как внедрение указанной системы уже реализуется в нашей стране [12]. В последние годы вопрос о системе постоянного умного мониторинга (наблюдения) субъектов предпринимательской деятельности поднимается и анализируется постоянно [4] и значительное число специалистов отмечают в его введении значительное число плюсов [2, с. 140-150]. Но сейчас происходит переход на систему цифрового мониторинга (наблюдения) когда в автоматическом режиме все данные о деятельности субъекта предпринимательской деятельности будут постоянно проверяться в фоновом режиме. Данные для такого мониторинга цифровые алгоритмы берут из всех доступных источников, в том числе открытых. Для внедрения системы такого цифрового мониторинга в отдельных сферах контрольно-надзорной деятельности разрабатываются специальные нормативные правовые акты [4].

Цель такого постоянного мониторинга (наблюдения) весьма благая - сделать более прозрачным и консолидированным конкретный вид деятельности, но вот какие могут быть последствия - стоит порассуждать.

Как возможное следствие внедрения такой системы постоянного мониторинга может происходить прогнозирование поведения субъекта предпринимательской деятельности, и постепенное выстраивание именно прогнозирования его виновного поведения. Это заключается в следующем: процесс контроля идет постоянно и непрерывно путем автоматизированной обработки данных, выявления всех критических и рисковых позиций в деятельности объекта проверки. И если это будет некая единая база данных со строгими правилами внесения информации и своевременности такого внесения, то ситуация одна. Если же это будет свободный поиск данных, проверка всей деятельности объекта контроля через любые

ресурсы, то всегда будет основание для привлечения его к ответственности. Как следствие такой ситуации цифровые алгоритмы могут проецировать сомнительность или незаконность деятельности субъекта предпринимательской деятельности, блокировать какие-то сделки, блокировать движение денежных средств и т.д., что приводит фактически к крушению цифровой репутации субъекта предпринимательской деятельности. Все это впоследствии придется оспаривать в административном или судебном порядке.

Что необходимо для минимизации ущерба для объектов контроля: четкие критерии для мониторинга (например, на основе риск-ориентированного подхода); согласие объекта контроля на введение в отношении него системы постоянного мониторинга (как минимум на начальном этапе функционирования данного контроля); некое единое цифровое пространство, где будет проходить указанный мониторинг (причем оно должно быть структурировано определенным образом и нормативно закреплено); наличие технологических и технических возможностей для всех участников контроля (и объектов, и субъектов) для участия в нем; методические и нормативные правовые основы для применения подобной системы мониторинга.

Еще одной значительной проблемой, создающей значительные риски для субъектов предпринимательской деятельности, является цифровизация муниципального контроля, то есть введение самостоятельных цифровых алгоритмов на уровне муниципального контроля, не связанных с введенными едиными для страны инструментами и сервисами. Вообще цифровизация муниципального управления на настоящий момент является сложным стихийно образуемым явлением. И касается это и технико-технологической оснащенности, и подготовленности специалистов, и нормативного регулирования, и финансовых возможностей муниципалитетов и регионов. И все это переходит на систему муниципального контроля в том числе. Для устранения подобной ситуации, стоит выбрать путь развития цифровизации муниципального управления и муниципального контроля: либо государство оставляет процесс в его текущем состоянии, либо выделяет соответствующую финансовую и техническую помощь, но одновременно вводит законодательные рамки, методическую помощь для организации соответствующего процесса цифровизации.

Результаты

Завершая процесс исследования темы, подведем итоги. Цифровизация государственного и муниципального контроля и надзора процесс, который будет продолжаться и усиливаться постоянно, и в основу всего уже и сейчас и в дальнейшем будет положен цифровой алгоритм. И в подобной ситуации и государству и обществу необходимо определиться с правовым значением и пониманием статуса цифрового алгоритма. На текущий момент времени единственной группой субъектов для кого в категорию рисков, в рамках государственного и муниципального контроля и надзора, входит цифровой алгоритм, являются субъекты предпринимательской деятельности, но ведь в дальнейшем эта ситуация перейдет на обычных граждан.

Соответственно, если государство считает допустимым и возможным разрешить цифровым алгоритмам принимать юридически значимые решения, которые создают существенные последствия для субъектов предпринимательской деятельности, государство должно и создать полноценный нормативно-правовой базис для подобной деятельности, исключив нарушения прав субъектов предпринимательской деятельности.

Литература

1. Агамагомедова С. А. Государственный контроль и надзор в условиях цифровизации экономики. // Вестник ННГУ. 2020. №3. С. 79-85.
2. Антропцева И. О. Правовое регулирование публичного финансового контроля. М.: Статут, 2024. 254 с.
3. Бирюков О. Н., Хасанов Н. А. О методике определения основных понятий теории алгоритмов. // Modern European Researches. 2021. №2-1. С. 58-65.
4. Ведомственный проект Министерства финансов РФ «Электронный СМАРТ-контроль (контроллинг) и учет государственных финансов для управленческих решений 2022-2027» (Направление (подпрограмма) «Повышение качества управления бюджетным процессом и эффективности управления общественными финансами») [Электронный ресурс]. Режим доступа:://https://minfin.gov.ru/ru/perfomance/projects/electronic_SMART_control (дата обращения: 18.06.2026).
5. Гаджиева М. Дело у техники: контрольные ведомства сокращают штат из-за внедрения ИИ и дронов: Как это влияет на бизнес и кто приходит на замену инспекторам. 17 марта 2026. [Электронный ресурс]. Режим доступа:://https://iz.ru/2060387/milana-gadzhieva/delo-u-tekhniki-kontrolnye-vedomstva-sokrashchayut-shtat-iz-za-vnedreniya-ii-i-dronov (дата обращения: 28.05.2026).
6. Законопроект № 1271570-8 «О поддержке развития технологий искусственного интеллекта в Российской Федерации». [Электронный ресурс]. Режим доступа:://https://sozd.duma.gov.ru/bill/1271570-8 (дата обращения: 15.07.2026).
7. Казанцев Д. А. Правовые механизмы распределения ответственности за вред, причиненный системами искусственного интеллекта. // Journal of Digital Technologies and Law. 2025. № 3(3). С. 446-471.
8. Киселев А. С. Перспективы и риски использования искусственного интеллекта в сфере правовой аналитики и правотворческой деятельности. // Lex russica. 2025. № 78(6). С. 127-143.
9. Лагаева В. П. Технологическая нейтральность принципов государственного контроля (надзора) // Аграрное и земельное право. 2024. №10 (238). С. 120-121.
10. Липчанская М. А., Чаннов С. Е., Чурикова А. Ю. Риски использования цифровых технологий в деятельности органов местного самоуправления. // Правоприменение. 2024. №3. С. 82-91.
11. Надзор выходит на интеллектуальный уровень / Аналитический центр при Правительстве РФ. 01 декабря 2025. [Электронный ресурс]. Режим доступа:://https://ac.gov.ru/news/page/nadzor-vyhodit-na-intellektualnyj-uroven-28266 (дата обращения: 28.05.2026).
12. О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации: Федеральный закон от 31.07.2020 № 248-ФЗ (ред. от 17.04.2026) // Официальный интернет-портал правовой информации www.pravo.gov.ru, 31.07.2020.
13. О государственной информационной системе «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности: Постановление Правительства РФ от 21.04.2018 № 482 (ред. от 10.05.2026) // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 25.04.2018.
14. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Российская газета. № 165. 2006.
15. О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля: Федеральный закон от 26.12.2008 № 294-ФЗ (ред. от 29.12.2025) // Собрание законодательства Российской Федерации. 2008. № 52. Ст. 6249.

16. Об общих принципах организации и деятельности контрольно-счетных органов субъектов Российской Федерации, федеральных территорий и муниципальных образований: Федеральный закон от 07.02.2011 № 6-ФЗ (ред. от 28.12.2025) // Российская газета. № 29. 2011.

17. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 26.06.2026) // Российская газета. № 165. 2006.

18. Омелехина Н. В. Цифровое прочтение принципов финансового права: к постановке проблемы исследования // Финансовое право. 2022. № 5. С. 9-11.

19. Понкин И. В. К вопросу о недостатках и рисках внедрения и применения цифровых инструментов в государственном управлении // Государственная служба. 2024. № 4 (150). С. 76-82.

20. Фисенко О. В., Юраш Ю. С., Сафаргалина Э. И. Что такое алгоритм? // The Scientific Heritage. 2020. №5 7-2. С.46-48.

21. Fredkin, E. An Introduction to Digital Philosophy. // International Journal of Theoretical Physics. 2003. Vol. 42. № 2. P. 189-241.

22. Wolfram, S. A New Kind of Science. Champaign, IL: Wolfram Media, 2002. 1192 p.

23. Zuse, K. Rechnender Raum = Calculating Space. Braunschweig : Vieweg & Sohn, 1969. 74 p.

Digital algorithms of state and municipal control and supervision as a risk for business entities: legal aspects

Usoltseva N.A., Usoltsev Yu.M.
Surgut State University

Digitalization of state and municipal control and supervision is not just a conversation about convenience for officials conducting appropriate procedures, it is a conversation, including about the risks for those entities that fall under control and supervisory measures. And such subjects are now subjects of entrepreneurial activity. Digital algorithms are the basis of all digitalization processes and, accordingly, the basis for decision-making within the framework of control and supervisory measures. And now we have reached a turning point when digital algorithms will become independent subjects of control and supervisory measures in relation to business entities. In such a situation, it is natural to ask about the risks that business entities face in such a situation and about the legal status of the digital algorithm itself. The main part of the article examines the issues of the concept of a digital algorithm and its status, determining its meaning in the context of a legal category. The inclusion of digital algorithms in the procedures and processes of state and municipal control and supervision is assessed. The main question is revealed – what risks do business entities face when conducting state and municipal control and supervision activities based on a digital algorithm. As a result of the study, it is concluded that it is necessary to determine the status of the digital algorithm when conducting control and supervisory measures at the regulatory and legal level and protecting the rights of business entities.

Keywords**:** digital algorithms, state and municipal control and supervision, entrepreneurial activity, risks of business entities, digitalization of state and municipal control and supervision.

References

1. Agamagomedova S. A. State control and supervision in the context of digitalization of the economy. // Bulletin of UNN. 2020. No. 3. pp. 79-85.
2. Antroptseva I. O. Legal regulation of public financial control. Moscow: Statut, 2024. 254 p.
3. Biryukov O. N., Khasanov N. A. On the methodology for defining the basic concepts of the theory of algorithms. // Modern European Researches. 2021. No. 2-1. pp. 58-65.
4. Departmental project of the Ministry of Finance of the Russian Federation "Electronic SMART control (controlling) and accounting of public finances for management decisions 2022-2027" (Direction (subprogram) "Improving the quality of budget process management and the efficiency of public finance management") [Electronic resource]. Available at: https://minfin.gov.ru/ru/perfomance/projects/electronic_SMART_control (Accessed: June 18, 2026).
5. Gadzhieva M. Technology is in the Game: Regulatory Agencies Are Cutting Staff Due to the Introduction of AI and Drones: How This Affects Business and Who Is Replacing Inspectors. March 17, 2026. [Electronic resource]. Available at: https://iz.ru/2060387/milana-gadzhieva/delo-u-tekhniki-kontrolnye-vedomstva-sokrashchayut-shtat-iz-za-vnedreniya-ii-i-dronov (Accessed: May 28, 2026).
6. Bill No. 1271570-8 "On Supporting the Development of Artificial Intelligence Technologies in the Russian Federation." [Electronic resource]. Access mode: https://sozd.duma.gov.ru/bill/1271570-8 (date accessed: 15.07.2026).
7. Kazantsev D. A. Legal mechanisms for distributing liability for damage caused by artificial intelligence systems. // Journal of Digital Technologies and Law. 2025. No. 3 (3). pp. 446-471.
8. Kiselev A. S. Prospects and risks of using artificial intelligence in the field of legal analytics and lawmaking. // Lex russica. 2025. No. 78 (6). pp. 127-143.
9. Lagaeva V. P. Technological neutrality of the principles of state control (supervision) // Agrarian and land law. 2024. No. 10 (238). pp. 120-121.
10. Lipchanskaya M. A., Channov S. E., Churikova A. Yu. Risks of Using Digital Technologies in the Activities of Local Governments. // Law Enforcement. 2024. No. 3. pp. 82-91.
11. Supervision is Reaching an Intelligent Level / Analytical Center under the Government of the Russian Federation. December 1, 2025. [Electronic resource]. Available at: https://ac.gov.ru/news/page/nadzor-vyhodit-na-intellektualnyj-uroven-28266 (accessed: May 28, 2026).
12. On state control (supervision) and municipal control in the Russian Federation: Federal Law of July 31, 2020 No. 248-FZ (as amended on April 17, 2026) // Official Internet Portal of Legal Information www.pravo.gov.ru, July 31, 2020.
13. On the state information system "Standard cloud solution for automation of control (supervisory) activities: RF Government Resolution of April 21, 2018 No. 482 (as amended on May 10, 2026) // Official Internet Portal of Legal Information http://www.pravo.gov.ru, April 25, 2018.
14. On personal data: Federal Law of 27.07.2006 No. 152-FZ (as amended on 24.06.2025) // Rossiyskaya Gazeta. No. 165. 2006.
15. On the protection of the rights of legal entities and individual entrepreneurs in the implementation of state control (supervision) and municipal control: Federal Law of 26.12.2008 No. 294-FZ (as amended on 29.12.2025) // Collected Legislation of the Russian Federation. 2008. No. 52. Art. 6249.
16. On the General Principles of the Organization and Activities of Audit Bodies of the Subjects of the Russian Federation, Federal Territories, and Municipalities: Federal Law of February 7, 2011 No. 6-FZ (as amended on December 28, 2025) // Rossiyskaya Gazeta. No. 29. 2011.
17. On Information, Information Technologies, and Information Protection: Federal Law of July 27, 2006 No. 149-FZ (as amended on June 26, 2026) // Rossiyskaya Gazeta. No. 165. 2006.
18. Omelyokhina N.V. Digital Reading of the Principles of Financial Law: Toward a Research Problem Statement // Financial Law. 2022. No. 5. pp. 9-11.
19. Ponkin, I. V. “On the Disadvantages and Risks of Implementing and Using Digital Tools in Public Administration.” Public Service. 2024. No. 4 (150). pp. 76–82.
20. Fisenko, O. V., Yurash, Yu. S., Safargalina, E. I. “What is an Algorithm?” The Scientific Heritage. 2020. No. 5, 7–2, pp. 46–48.
21. Fredkin, E. “An Introduction to Digital Philosophy.” International Journal of Theoretical Physics. 2003. Vol. 42, No. 2, pp. 189–241.
22. Wolfram, S. “A New Kind of Science.” Champaign, IL: Wolfram Media, 2002. 1192 p.
23. Zuse, K. Rechnender Raum = Calculating Space. Braunschweig: Vieweg & Sohn, 1969. 74 r.