ПРАВОВЫЕ ГАРАНТИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ЗАЯВИТЕЛЕЙ И ЗАЩИТЫ ОТ КИБЕРПРЕСЛЕДОВАНИЯ В УСЛОВИЯХ ЦИФРОВЫХ АЛГОРИТМОВ

Акмалжон Исабаев
Главный консультант Отдела анализа конституционного законодательства Конституционного суда Республики Узбекистан, PhD

Аннотация: В статье представлен системный анализ конституционно-правовых гарантий защиты персональных данных заявителей и их защиты от киберпреследования в условиях, когда государственные органы обрабатывают электронные обращения с использованием алгоритмических систем. Актуальность исследования обусловлена расширением практики автоматизированной сортировки обращений и их обработки с помощью искусственного интеллекта - практики, сопутствующие риски которой (алгоритмическая дискриминация, утечки данных, доксинг) до сих пор недостаточно урегулированы национальным законодательством. Цель исследования - раскрыть правовую природу указанных рисков и предложить комплексную модель защиты от них. Использованы сравнительно-правовой, нормативно-догматический и системно-функциональный методы. Анализ опирается на научные взгляды учёных стран СНГ (Э.В. Талапина) и Узбекистана (О.Т. Хусанов, А.Д. Гофуров, А.О. Халмуратов), а также на положения GDPR, Конвенции Совета Европы 108+ и Регламента ЕС об искусственном интеллекте. В качестве научной новизны в статью введено понятие «цифровой процессуальной безопасности заявителей» и предложена четырёхступенчатая правовая модель - превентивная, процессуальная, киберзащитная и восстановительная. Практическая значимость исследования выражена в конкретных предложениях по совершенствованию законодательства.

Ключевые слова: цифровое государство, алгоритмическое управление, право на обращение, персональные данные, кибербезопасность.

Введение

Процесс цифровизации государственного управления - в особенности в сфере приёма и рассмотрения обращений граждан - в

последние годы вышел на качественно новый уровень: неуклонный рост числа электронных обращений подталкивает государственные органы к использованию автоматизированных систем, включая алгоритмы искусственного интеллекта, для их сортировки и распределения. Однако у этого процесса есть и вторая, пока недостаточно изученная сторона: по мере того как алгоритм обрабатывает данные заявителя, вторжение в его частную жизнь порождает новые, ранее не существовавшие риски - автоматическое отнесение заявителя к категории «неблагонадёжных» на основе его данных (алгоритмическая дискриминация), неправомерное раскрытие персональных данных из баз данных, а также подверженность лица доксингу, кибертравле или иным формам цифрового давления именно вследствие подачи обращения.

Актуальность проблемы усугубляется тем, что действующее законодательство - об обращениях, о персональных данных и о кибербезопасности - действует каждое в рамках своего предмета регулирования, однако на стыке этих сфер, то есть непосредственно в процессе рассмотрения обращений, отсутствует специальное комплексное регулирование возникающих цифровых рисков. Как показывает американский учёный Р. Кало, технологии искусственного интеллекта ставят перед административным правом принципиально новую проблему: традиционные правовые категории - полномочие, ответственность, контроль - не всегда напрямую применимы к системам автоматизированного принятия решений, что требует доктринального переосмысления возникающих пробелов [21]. В связи с этим проблема исследования формулируется следующим образом: каким образом безопасность персональных данных заявителей и их защищённость от киберпреследования могут быть обоснованы как самостоятельная, составная гарантия права на обращение, и посредством какой комплексной модели она может быть обеспечена.

В Новом Узбекистане цифровизация государственного управления рассматривается не как средство ограничения прав человека, а как механизм их более эффективного обеспечения. Как подчёркивал Президент Шавкат Мирзиёев, принцип «ради достоинства человека» и идея служения государственных органов народу стали главным критерием деятельности государства [30]. Данный методологический критерий должен сохраняться и в условиях цифрового государства: реализация права на обращение, защита персональных данных и обеспечение подотчётности государственных органов - по сути, различные проявления защиты человеческого достоинства в цифровой среде. Исследование выстроено на следующей логической цепочке:

достоинство человека - право на обращение - безопасность персональных данных - цифровая безопасность - искусственный интеллект - алгоритмическая справедливость, при этом выбор достоинства человека в качестве отправной точки не случаен: именно оно образует общую конституционную основу как права на обращение, так и защиты персональных данных, и алгоритмической справедливости, объединяя все рассматриваемые ниже институты в рамках единого методологического критерия.

Глава I. Правовая природа права на обращение в цифровой среде

1.1. Конституционное содержание

Право на обращение, закреплённое в статье 40 Конституции Республики Узбекистан, имеет двоякое значение в системе прав человека - как процессуальное, так и материальное: оно охватывает не только возможность гражданина вступить в коммуникацию с государством, но и требование, чтобы его персональные данные в ходе этой коммуникации использовались законно и безопасно [1]. Как отмечает О.Т. Хусанов, современное понимание конституционных прав охватывает не только негативную обязанность государства воздерживаться от вмешательства, но и его позитивную обязанность активно обеспечивать права граждан [2]; применительно к безопасности персональных данных эта позитивная обязанность приобретает особое значение: принимая обращение, государственный орган обязан предпринимать активные меры по защите данных заявителя, в противном случае само право на обращение приобретает лишь формальный характер.

Особое методологическое значение здесь имеет принцип соразмерности: объём данных, собираемых государственным органом о заявителе, и способ их обработки должны быть соразмерны цели рассмотрения обращения и не должны выходить за её пределы. Данный принцип, в свою очередь, вытекает из конституционного признания достоинства человека высшей ценностью: если алгоритм рассматривает заявителя лишь как «набор данных», не принимая во внимание его индивидуальную ситуацию, это противоречит принципу уважения человеческого достоинства. Как отмечает А.Б. Гафуров (Аскар Боисович) в своих исследованиях цифровизации органов правосудия и конституционного контроля, цифровизация государственных институтов не является самоцелью, а служит средством формирования эффективного государственного управления, обеспечивающего права человека [31]; цифровая обработка обращений также должна быть подчинена именно этой цели - технология призвана расширять права, а не сужать их.

1.2. Правовые особенности электронных обращений

Электронное обращение принципиально отличается от традиционного письменного: оно сопровождается электронной идентификацией (например, через систему ONE ID), автоматической регистрацией и «цифровым следом» - IP-адресом, идентификатором устройства, временем отправки и иными метаданными. Как показывает А.Д. Гофуров, цифровизация сокращает дискреционные пределы усмотрения должностного лица внутри ведомства и стандартизирует процесс [3], однако именно вследствие такой стандартизации резко возрастает объём собираемых данных, что пропорционально усиливает необходимость их защиты.

1.3. Понятие алгоритмического государственного управления

В международной литературе понятие «Algorithmic Governance» обозначает практику принятия государственных решений посредством частично или полностью автоматизированных систем. Как показывает российская учёная Э.В. Талапина, такие системы порождают особый риск: они формируют вероятностную оценку в отношении человека, что может нарушать право на индивидуализированное, справедливое рассмотрение [4]. Применительно к обращениям это означает, что если алгоритм автоматически относит заявителя к категории «часто жалующихся» или «предвзятых» на основании истории его обращений, это способно повлиять на рассмотрение его последующих обращений и фактически привести к скрытой дискриминации. Согласно известной формуле Л. Лессига «код - это закон», в цифровой среде поведение гражданина в первую очередь и зачастую наиболее жёстко ограничивает не писаная норма, а сам программный код [18] - вывод, напрямую применимый к алгоритмам, обрабатывающим обращения: если код алгоритма остаётся вне правового контроля, он на практике превращается в более сильный регулирующий фактор, чем закон.

Глава II. Правовые основы защиты персональных данных заявителей

2.1. Правовой режим персональных данных

Закон «О персональных данных» (ЗРУ-547, 2 июля 2019 г.) устанавливает общий порядок обработки персональных данных [5], однако не содержит специальной нормы об автоматизированной обработке и сортировке обращений. В зарубежной практике данный пробел восполняется Общим регламентом ЕС по защите данных (GDPR): его статья 22 закрепляет право лица не подвергаться решению, основанному исключительно на автоматизированной обработке и порождающему для него юридические последствия [6].

Модернизированная Конвенция 108+ Совета Европы распространяет аналогичное право за пределы регионального уровня в широком международном масштабе [7], а Принципы конфиденциальности ОЭСР сохраняют значение как первый документ, сформулировавший принципы минимизации данных и целевого ограничения их обработки [8].

2.2. Категории данных, обрабатываемых в процессе рассмотрения обращений

В ходе рассмотрения электронного обращения, как правило, обрабатываются фамилия, имя и отчество заявителя, номер телефона, адрес электронной почты, IP-адрес, а в отдельных случаях - геолокация и биометрические данные (например, в системах распознавания лиц). Европейский суд по правам человека по делу S. and Marper против Соединённого Королевства установил, что бессрочное хранение биометрических данных может нарушать право на неприкосновенность частной жизни [13], а по делу Bărbulescu против Румынии указал, что даже при мониторинге электронной переписки работника должен соблюдаться принцип соразмерности [14] - оба вывода в полной мере применимы к биометрическим и мониторинговым данным в системах обращений. Кроме того, система обращений хранит всю «историю обращений» гражданина, что со временем формирует детальный профиль его социальной и правовой активности; именно этот профиль становится основой для алгоритмического анализа и потому должен оцениваться не только как административная, но и как персональная информация. Как показывают В. Майер-Шёнбергер и К. Кукьер, большие объёмы данных (Big Data) позволяют извлекать из по отдельности безобидных фактов новые, ранее не существовавшие знания и выводы - особенность, требующая повышенной осторожности в отношении агрегированных баз данных, таких как история обращений, поскольку совокупный анализ способен раскрыть больше персональной информации, чем отдельно взятые данные [19].

2.3. Принципы обработки данных

Принципы, закреплённые в GDPR и национальном законодательстве, - минимизация, целевое ограничение, соразмерность, прозрачность и подотчётность - должны применяться к системам обращений следующим образом: система должна собирать лишь минимально необходимые для рассмотрения обращения данные, использовать их исключительно в этой цели, соблюдать соразмерный срок хранения, информировать заявителя о порядке обработки его данных, а ведомство должно нести ответственность за данный процесс. Теоретическую основу этих принципов составляет концепция «информационной приватности» Дж.Э.

Коэн: по её мнению, приватность - это не просто сокрытие информации, а возможность контролировать, каким образом формируется собственный социальный «профиль» человека [22]. Н. Ричардс через понятие «интеллектуальной приватности» показывает, что человек, ощутивший наблюдение за своими мыслями и поступками, теряет способность действовать свободно [23] - вывод, особенно значимый для заявителей: если гражданин знает, что его обращения постоянно отслеживаются и профилируются алгоритмом, это может ограничить его готовность обращаться в будущем.

Глава III. Правовые риски, возникающие вследствие применения цифровых алгоритмов

3.1. Алгоритмическая дискриминация

Систематическая ошибка (bias), профилирование (profiling), ранжирование (ranking) и фильтрация (filtering) - четыре основных механизма алгоритмической дискриминации. Э.В. Талапина показывает, что обеспечение прозрачности алгоритмов является центральным направлением этики искусственного интеллекта в государственном управлении, поскольку проблема «чёрного ящика» (black box) - непрозрачность того, каким образом алгоритм приходит к выводу, - создаёт угрозу институту юридической ответственности [9]. Согласно предложенной К. Йенг типологии «алгоритмического регулирования» (Algorithmic Regulation), такие системы могут действовать реактивно или превентивно, но в обоих случаях их легитимность строится не на открытых, оспариваемых правилах, а на постоянно меняющемся потоке данных, что бросает вызов традиционным механизмам правового контроля [24]. Ф. Паскуале в концепции «общества чёрного ящика» показывает, что внутренняя логика автоматизированных систем может оставаться непрозрачной даже для контролирующих органов, что подрывает принцип демократической подотчётности [25]. В качестве правового решения этой проблемы С. Вахтер, Б. Миттельштадт и К. Расселл предлагают метод «контрфактических объяснений»: не раскрывая полностью внутреннюю логику алгоритма, можно предоставить объяснение вида «если бы было иначе, результат был бы другим», что на практике обеспечивает требование объяснимости, предусмотренное статьёй 22 GDPR [26]. В контексте обращений эта проблема особенно остра: если заявитель не может узнать, почему его заявление получило статус «низкого приоритета» или почему был продлён срок его рассмотрения, он не в состоянии эффективно защищать своё право.

3.2. Утечки персональных данных

Несанкционированное раскрытие данных (Data Breach), риски облачной инфраструктуры (Cloud Risks) и несанкционированный доступ третьих лиц (Third Party Access) - риски, связанные с централизованным хранением баз данных обращений. Как показывает Ш. Зубофф в концепции «капитализма слежки», накопление данных о личности - не просто технический процесс, а может стать средством установления косвенной власти над обладателем данных [27] - вывод, применимый и к государственным базам данных обращений: если такая база расширяется бесконтрольно, она рискует превратиться в неформальный инструмент контроля над гражданином. А.О. Халмуратов на примере Узбекистана показывает, что такие правонарушения, как фишинг и кибершантаж, недостаточно отражены в законодательстве, что ослабляет принцип неотвратимости наказания [10]. Утечка данных из базы обращений, особенно если она затрагивает чувствительную информацию, способна причинить гражданину не только материальный, но и серьёзный психологический и личностный вред.

3.3. Понятие киберпреследования

Научная классификация киберпреследования включает следующие формы: доксинг (несогласованное публичное раскрытие персональных данных лица), кибертравлю (cyber stalking), онлайн-запугивание (online intimidation), публикацию из мести (revenge publication) и кражу личности (identity theft). Д.К. Ситрон, глубоко анализируя данные явления, показывает, что киберпреследование представляет собой серьёзное правонарушение, оказывающее непосредственное влияние на реальную жизнь жертвы - её работу, членов семьи и физическую безопасность, - и что оценивать его лишь как «онлайн-конфликт» - ошибочный, упрощающий подход [28]. Правовое значение данной классификации состоит в том, что она выделяет объективную сторону каждой формы, что позволяет установить соответствующие различные правовые и технические меры реагирования (например, право на удаление данных - для доксинга, мониторинг и блокировку - для кибертравли).

3.4. Цифровые формы преследования заявителей

Наиболее опасной на практике является ситуация цифрового давления на лицо именно вследствие подачи им обращения: неправомерное распространение данных заявителя, его алгоритмическое обозначение как «проблемного лица» либо использование государственных реестров ему во вред. Подобные ситуации приводят к «сдерживающему эффекту» (chilling effect) в отношении права на обращение: опасаясь незащищённости своих данных, гражданин может отказаться даже от юридически обоснованной жалобы. Именно в этой

точке наиболее ярко проявляется неразрывная связь между правом на обращение и безопасностью персональных данных.

Глава IV. Международные стандарты и зарубежный опыт

4.1. Международные документы

Статья 12 Всеобщей декларации прав человека закрепляет право на неприкосновенность частной жизни в общей форме [20], и, согласно современным правовым подходам, данное право в полной мере применяется и в цифровой среде. Статья 17 Международного пакта о гражданских и политических правах также запрещает произвольное или незаконное вмешательство в личную и семейную жизнь человека, и в условиях цифровой эпохи эта норма распространяется на электронную почту, мессенджеры и иные данные, обрабатываемые в интернет-среде. Резолюции Генеральной Ассамблеи ООН о праве на неприкосновенность частной жизни в цифровую эпоху (в том числе резолюции 68/167 и 69/166) подтверждают, что права, которыми люди обладают офлайн, должны в равной степени защищаться и онлайн, с особым вниманием к рискам неправомерной массовой слежки. В докладах Верховного комиссара ООН по правам человека также анализируется влияние искусственного интеллекта, биометрических данных, систем распознавания лиц и средств шифрования на права человека и неприкосновенность частной жизни. Конвенция № 108 Совета Европы, одна из первых крупных международных договоров в сфере защиты данных, заложила основополагающие стандарты автоматизированной обработки персональных данных и трансграничной передачи данных.

4.2. Опыт Европейского союза

GDPR устанавливает общий стандарт защиты персональных данных, а Регламент ЕС об искусственном интеллекте (Регламент (ЕС) 2024/1689) закрепляет требования человеческого контроля и прозрачности для высокорисковых систем ИИ, применяемых в государственных услугах [11]. Директива NIS2 (ЕС) 2022/2555 устанавливает минимальные обязательства государственных органов в сфере кибербезопасности, включая сроки уведомления об инцидентах [12]. В совокупности эти три документа образуют единую правовую цепочку, объединяющую безопасность персональных данных, алгоритмическую прозрачность и киберзащиту в системах обращений.

4.3. Опыт зарубежных государств

В Германии административные цифровые услуги подчиняются принципу «privacy by design», закреплённому в статье 25 GDPR [6]. Департамент информационных систем Эстонии (RIA) внедрил сервис «Data Tracker», который фиксирует каждый запрос к государственной

базе данных и позволяет гражданину через государственный портал eesti.ee лично отслеживать, кто, когда и с какой целью обращался к его данным [32]. В Республике Корея Комиссия по защите персональной информации (PIPC), получившая после реформы 2020 года статус независимого центрального органа, обладает полномочиями по проверке и аудиту автоматизированных систем, используемых государственными ведомствами [33]. Опыт Сингапура требует уточнения: в рамках программы «Smart Nation» действует инструмент тестирования «AI Verify», однако это не обязательный государственный аудит, а добровольный инструмент, позволяющий организациям самостоятельно оценивать свои алгоритмы по признанным на международном уровне критериям [34]. Данный опыт показывает, что независимо от уровня технического развития независимый контроль и формализованный механизм играют важную роль в каждой системе - при этом обязательный (Германия, Корея) либо добровольный (Сингапур) характер такого механизма существенно влияет на его практическую эффективность.

Глава V. Правовые гарантии и существующие пробелы в законодательстве Узбекистана

5.1. Анализ действующего законодательства

Статья 31 Конституции гарантирует неприкосновенность частной жизни и защиту персональных данных, статья 40 - право на обращение. Закон «Об обращениях физических и юридических лиц» регулирует порядок рассмотрения обращений, Закон «О персональных данных» [5] - общий порядок их обработки, а Закон «О кибербезопасности» (ЗРУ-764, 15 апреля 2022 г.) устанавливает государственную систему киберзащиты информационных систем [16]. Однако указанные три закона действуют независимо друг от друга - специальное регулирование на их стыке, применительно именно к системе обращений, отсутствует, что препятствует формированию единой комплексной системы кибербезопасности и защиты персональных данных в процессе рассмотрения обращений физических и юридических лиц.

5.2. Правовые пробелы

По результатам анализа выявлено пять пробелов: во-первых, отсутствует специальный порядок использования искусственного интеллекта при обработке обращений в государственных органах; во-вторых, законодательно не гарантирована открытость (объяснимость) решений, принятых на основе алгоритмов; в-третьих, отсутствует специальный, упрощённый механизм обжалования автоматизированных решений; в-четвёртых, само понятие «киберпреследование» не имеет чёткого правового определения в национальном законодательстве и

отражается фрагментарно в различных законах (незаконное распространение, защита чести, вмешательство в частную жизнь); в-пятых, для заявителей не предусмотрены специальные меры цифровой защиты (например, анонимизированный канал подачи жалоб). В результате принцип неотвратимости ответственности за правонарушения в сфере информационной безопасности не обеспечивается в полной мере, что порождает необходимость пересмотра правового статуса уполномоченных государственных органов в данной сфере.

5.3. Проблемы правоприменительной практики

Помимо нормативных пробелов, на практике наблюдаются бесконтрольное расширение интеграции баз данных между различными ведомствами, недостаточная компетентность сотрудников в вопросах информационной безопасности (человеческий фактор), а также отсутствие у ведомств чёткой системы ответственности за «утечку» данных. Как отмечает А.О. Халмуратов, нехватка высококвалифицированных IT-специалистов в правоохранительных органах ещё более усугубляет данные проблемы [17]. Для устранения указанных проблем необходимо разработать единый правовой механизм, регулирующий межведомственный обмен данными, а также законодательно закрепить чёткую юридическую ответственность каждого государственного органа за нарушение неприкосновенности персональных данных.

Глава VI. Правовая модель защиты персональных данных заявителей

На основании проведённого анализа автор предлагает концепцию «цифровой процессуальной безопасности заявителей» (Digital Procedural Security of Petitioners) и обеспечивающую её четырёхступенчатую правовую модель. Данная модель последовательно объединяет этапы профилактики, процедуры, кибертехнической защиты и устранения последствий (реституции), при этом каждый последующий этап восполняет недостаточность предыдущего.

I. Превентивные гарантии (Preventive safeguards): шифрование данных, принцип минимального сбора данных, обеспечение конфиденциальности на этапе проектирования (Privacy by Design) и предварительная оценка рисков (Privacy Impact Assessment) - меры, направленные на устранение риска ещё до внедрения системы.

II. Процессуальные гарантии (Procedural safeguards): обязанность уведомлять заявителя о применении алгоритма (Explainability - объяснимость); право на пересмотр автоматизированного решения с участием человека (Human Oversight - человеческий контроль, в

соответствии с подходом статьи 22 GDPR [6]); обязанность обосновывать принятое решение (Accountability - подотчётность); право оспаривать решение и требовать его повторной оценки (Contestability - оспоримость, основанная на концепции контрфактических объяснений С. Вахтер и Б. Миттельштадта [26]); а также независимый электронный аудит (AI Risk Management - управление рисками). Данные пять элементов образуют единую, взаимодополняющую доктринальную систему: без объяснимости оспоримость на практике теряет смысл; без человеческого контроля подотчётность приобретает лишь формальный характер.

III. Киберзащита (Cyber Protection): анонимизация и псевдонимизация данных, двухфакторная аутентификация, журналирование всех обращений и изменений (logging), а также постоянный мониторинг - меры, реализующие на практике требования соразмерности и контроля, сформулированные в деле Big Brother Watch [15].

IV. Восстановительные гарантии (Remedial safeguards): право на возмещение вреда при утечке или неправомерном использовании данных, право на удаление данных (проявление «права на забвение» применительно к системе обращений), цифровая реабилитация (например, отмена ошибочно присвоенного алгоритмом статуса «опасного лица»), а также материальная и дисциплинарная ответственность допустившего это государственного органа.

Модель носит системный характер: если превентивный этап нарушен (например, собран избыточный объём данных), процессуальный этап должен это выявить; если и он не сработает, киберзащита должна выполнить функцию технического барьера; если же вред всё же причинён, должен включиться восстановительный механизм. Ни одна из гарантий не является самодостаточной - каждая из них выступает связующим звеном единой цепи.

Глава VII. Алгоритмический конституционализм и доктрина цифровых прав

Рассмотренные выше риски и гарантии представляют собой не разрозненные технико-правовые меры, а опираются на более широкую теоретическую основу - доктрину «цифрового конституционализма» (Digital Constitutionalism). Данная доктрина означает, что государственная власть остаётся связанной конституционными пределами и в цифровой среде: алгоритм не может стать новой, но при этом внеправовой формой государственной власти. Согласно предложенной Л. Флориди и Дж. Коулзом концепции «искусственного интеллекта для общества», системы ИИ должны подчиняться принципам благодеяния, ненанесения вреда,

уважения автономии, справедливости и объяснимости - пять принципов, в полной мере применимых и к алгоритмам, обрабатывающим обращения, в качестве конституционно-этических пределов [29].

Конституционный предел государственных алгоритмов проявляется в двух аспектах. Во-первых, обозначенная в разделе 3.1 проблема алгоритмической легитимности - то есть неподатливость алгоритма традиционным механизмам правового контроля - означает в конституционно-правовом смысле, что, коль скоро алгоритм осуществляет исполнительную функцию государственной власти, он в полной мере должен подчиняться принципам законности и соразмерности. Во-вторых, права гражданина, противостоящие алгоритмическому решению, - право на получение объяснения, право на возражение, право требовать пересмотра решения человеком - формируются как новое поколение «цифровых» прав, которые, в отличие от традиционных поколений прав человека (личных-политических, социально-экономических, коллективных), регулируют именно отношения между человеком и автоматизированной системой и на этом основании заслуживают признания в качестве самостоятельной категории.

Алгоритмическая прозрачность и алгоритмическая подотчётность - два основных инструмента, посредством которых данная доктрина воплощается на практике. Как отмечалось в разделе 3.1, само по себе раскрытие внутренней логики алгоритма недостаточно - без независимого контролирующего института прозрачность остаётся лишь декларативной. Отсюда вытекает важный конституционно-правовой вывод: если административный и парламентский контроль отслеживают повседневное функционирование алгоритма, то именно судебный - в том числе конституционный - контроль остаётся окончательной и наиболее сильной гарантией проверки его нормативных оснований, затрагивающих права человека. Обязательность человеческого контроля - требование, согласно которому любое автоматизированное решение, порождающее существенные правовые последствия, должно быть в конечном счёте подтверждено человеком, - образует практическое ядро цифрового конституционализма. Применительно к системам обращений это означает: сколь бы далеко ни зашла цифровизация ведомства, окончательное решение, определяющее судьбу заявителя, всегда должно оставаться в сфере ответственности человека - алгоритм способен быть лишь вспомогательным средством, но никогда не может стать окончательным арбитром.

Заключение

Проведённое исследование показывает, что эффективная реализация права на обращение в цифровой среде неразрывно связана с обеспечением безопасности персональных данных заявителя и его защитой от киберпреследования; оба этих элемента следует рассматривать как неотъемлемые, составные гарантии самого права на обращение. Хотя на национальном уровне действуют три отраслевых закона (об обращениях, о персональных данных, о кибербезопасности), именно на их пересечении - то есть применительно к алгоритмическим рискам, возникающим непосредственно в процессе рассмотрения обращений, - сохраняется пробел специального регулирования.

Предложенная четырёхступенчатая модель по своей сути представляет собой практическое воплощение идеи «цифровой процессуальной справедливости» (Digital Procedural Justice): она обеспечивает право заявителя на справедливое отношение на любом этапе - от сбора данных до исполнения окончательного решения. Блок процессуальных гарантий выступает конкретным выражением принципа «алгоритмического надлежащего процесса» (Algorithmic Due Process) - подобно традиционному справедливому судебному разбирательству, автоматизированное решение также должно гарантировать право быть услышанным, право на получение объяснения и право на оспаривание. В целом предложенную модель можно рассматривать как национальное, применённое к сфере государственного управления воплощение концепции «доверенного искусственного интеллекта» (Trustworthy AI), основанной на пяти принципах Л. Флориди, что, в свою очередь, составляет часть охарактеризованной выше доктрины цифрового конституционализма. Наконец, блок кибертехнических гарантий, представленный в главе VI, обозначает направление, которое можно было бы назвать «конституционной кибербезопасностью» (Constitutional Cybersecurity), - в рамках которого кибербезопасность признаётся не просто технической функцией, а средством защиты прав человека конституционного уровня. Данные положения могут быть далее выражены через две смежные категории: «конституционное цифровое доверие» (Constitutional Digital Trust), обозначающее необходимость того, чтобы цифровые отношения между государством и гражданином основывались на доверии, обеспеченном конституционными гарантиями, и «алгоритмическая процессуальная справедливость» (Algorithmic Procedural Justice) - более широкая, системная гарантия, отличная от гарантированного Algorithmic Due Process права быть услышанным по конкретному делу: она требует, чтобы алгоритм действовал последовательно и на равных условиях в отношении всех заявителей,

будучи свободным от рисков систематической ошибки и профилирования, указанных в разделе 3.1.

В качестве практических рекомендаций предлагается: (1) включить в Закон «Об обращениях физических и юридических лиц» специальную норму об автоматизированной обработке обращений, включая право заявителя на пересмотр решения с участием человека; (2) установить обязательное требование объяснимости для решений, принимаемых на основе алгоритмов; (3) ввести единое правовое определение понятия «киберпреследование» и создать оперативный административный механизм противодействия ему (например, при Омбудсмане); (4) установить чёткую систему материальной ответственности государственных органов за утечку данных из баз обращений. Ограничением работы является то, что модель пока не проверена на практике. Её пилотное тестирование и оценка эффективности — это задачи для будущих исследовани.

В качестве итогового методологического вывода следует подчеркнуть, что конституционная ценность цифрового государства определяется не степенью использования им искусственного интеллекта, а тем, в какой мере данные технологии защищают достоинство человека, неприкосновенность частной жизни и право на обращение. Именно этот критерий замыкает изложенную во введении логическую цепочку - достоинство человека, право на обращение, персональные данные, цифровая безопасность, искусственный интеллект, алгоритмическая справедливость - и именно он в конечном счёте определяет, можно ли считать цифровое государственное управление подлинно успешным.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Конституция Республики Узбекистан (новая редакция от 30 апреля 2023 г.), ст. 40.
2. Хусанов О.Т. Конституционное право: учебник. - Ташкент: Адолат, 2022. - С. 95-98.
3. Гофуров А.Д. Цифровая экономика и электронное правительство. - Ташкент: ТГЮУ, 2021. - 312 с.
4. Талапина Э.В. Обработка данных при помощи искусственного интеллекта и риски дискриминации // Правовая мысль: история и современность. - 2021 (эл. изд.: НИУ ВШЭ).
5. Закон Республики Узбекистан «О персональных данных», ЗРУ-547, 02.07.2019 // lex.uz/docs/4396419.
6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Art. 22, Art. 25.

7. Council of Europe. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), CETS No. 223, 2018.
8. OECD. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 1980 (rev. 2013).
9. Талапина Э.В. Прозрачность алгоритмов искусственного интеллекта // Право. Журнал Высшей школы экономики. - 2025. - Т. 18, № 3. - С. 4-27. DOI: 10.17323/2072-8166.2025.3.4.27.
10. Khalmuratov A.O. Legal aspects of enhancing measures to prevent and counter cybercrime in the Republic of Uzbekistan // Eurasian Journal of Law, Finance and Applied Sciences. - 2026. - Vol. 6, Issue 4. - P. 137-147.
11. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
12. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive).
13. European Court of Human Rights [GC]. S. and Marper v. United Kingdom, Judgment of 4 December 2008, Applications nos. 30562/04 and 30566/04.
14. European Court of Human Rights [GC]. Bărbulescu v. Romania, Judgment of 5 September 2017, Application no. 61496/08.
15. European Court of Human Rights [GC]. Big Brother Watch and Others v. United Kingdom, Judgment of 25 May 2021, Applications nos. 58170/13, 62322/14 and 24960/15.
16. Закон Республики Узбекистан «О кибербезопасности», ЗРУ-764, 15.04.2022 // lex.uz/docs/5960604.
17. Халмуратов А.О. Правовые аспекты совершенствования мер по предупреждению и противодействию киберпреступности в Республике Узбекистан // Eurasian Journal of Law, Finance and Applied Sciences. - 2026. - Т. 6, № 4. - С. 137-147.
18. Lessig L. Code: Version 2.0. - New York: Basic Books, 2006. - 410 p.
19. Mayer-Schönberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. - New York: Eamon Dolan/Houghton Mifflin Harcourt, 2013. - 242 p.
20. Всеобщая декларация прав человека, ООН, 10 декабря 1948 г., ст. 12.
21. Calo R. Artificial Intelligence Policy: A Primer and Roadmap // UC Davis Law Review. - 2017. - Vol. 51, No. 2. - P. 399-435.
22. Cohen J.E. Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. - New Haven: Yale University Press, 2012. - 336 p.

23. Richards N.M. Intellectual Privacy: Rethinking Civil Liberties in the Digital Age. - Oxford: Oxford University Press, 2015. - 256 p.
24. Yeung K. Algorithmic Regulation: A Critical Interrogation // Regulation & Governance. - 2018. - Vol. 12, No. 4. - P. 505-523. DOI: 10.1111/rego.12158.
25. Pasquale F. The Black Box Society: The Secret Algorithms That Control Money and Information. - Cambridge, MA: Harvard University Press, 2015. - 320 p.
26. Wachter S., Mittelstadt B., Russell C. Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR // Harvard Journal of Law & Technology. - 2018. - Vol. 31, No. 2. - P. 841-887.
27. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. - New York: PublicAffairs, 2019. - 704 p.
28. Citron D.K. Hate Crimes in Cyberspace. - Cambridge, MA: Harvard University Press, 2014. - 352 p.
29. Floridi L., Cowls J. A Unified Framework of Five Principles for AI in Society // Harvard Data Science Review. - 2019. - Vol. 1, No. 1.
30. Мирзиёев Ш.М. Выступление на видеоселекторном совещании, посвящённом вопросам внедрения в жизнь Конституции в новой редакции и продолжения последовательных реформ // газета «Халк сузи». - 2023. - 9 мая. - № 92.
31. Гафуров А.Б. (Аскар Боисович). Цифровизация деятельности Конституционного суда Республики Узбекистан - важное условие обеспечения открытости и прозрачности // журнал «Демократизация и права человека». - 2023. - № 4 (100). - С. 88-97.
32. Republic of Estonia Information System Authority (RIA). Data Tracker // ria.ee/en/state-information-system/people-centred-data-exchange/data-tracker.