УДК 342

СПЕЦИАЛЬНЫЕ СПОСОБЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНТЕРНЕТЕ ПО ЗАКОНОДАТЕЛЬСТВУ РЕСПУБЛИКИ УЗБЕКИСТАН

М.Б. Атажанова

докторант Высшей школы судей
при Высшем судейском совете Республики Узбекистан

Аннотация. *В статье проводится комплексное исследование специальных правовых механизмов защиты персональных данных в цифровой среде, предусмотренных действующим законодательством Республики Узбекистан. Анализируются современные правовые и технологические вызовы в сфере обеспечения информационной безопасности персональных данных в интернет-пространстве, систематизируются специфические способы правовой защиты, закрепленные в национальном законодательстве. Особое внимание уделяется доктринальному анализу практических аспектов применения специальных мер защиты персональных данных и оценке их эффективности в условиях активной цифровизации общественных отношений и формирования информационного общества в Республике Узбекистан.*

Ключевые слова: *персональные данные, защита информации, интернет-право, цифровые права, информационная безопасность, Республика Узбекистан.*

Abstract. *The article provides a comprehensive study of the special legal mechanisms for protecting personal data in the digital environment, as provided for by the current legislation of the Republic of Uzbekistan. It analyzes the current legal and technological challenges in ensuring the information security of personal data in the Internet space, and systematizes the specific methods of legal protection enshrined in national legislation. Special attention is paid to the doctrinal analysis of the practical aspects of the application of special measures for protecting personal data and assessing their effectiveness in the context of the active digitalization of social relations and the formation of an information society in the Republic of Uzbekistan.*

Keywords: *personal data, information protection, internet law, digital rights, information security, Republic of Uzbekistan.*

Стремительное развитие информационно-коммуникационных технологий и повсеместное внедрение цифровых платформ в различные сферы общественной жизни создают принципиально новые правовые вызовы в области защиты персональных данных граждан. В условиях активной реализации государственной политики цифровизации, масштабного внедрения электронного документооборота, развития системы электронного правительства и цифровых государственных услуг в Республике Узбекистан вопросы обеспечения надежной и всесторонней правовой защиты персональной

информации граждан в интернет-среде приобретают стратегическую важность и требуют углубленного научно-правового анализа с позиций современной доктрины информационного права.

Специальные способы защиты персональных данных в интернете в контексте национального правопорядка представляют собой системно организованный комплекс взаимосвязанных правовых, технических и организационно-управленческих мер, направленных на предотвращение неправомерного доступа, несанкционированного использования, незаконного распространения и искажения личной информации граждан в цифровой среде. Данная система правовых гарантий основывается на конституционных принципах неприкосновенности частной жизни и требует комплексного подхода к правовому регулированию, учитывающего специфику функционирования информационных технологий и особенности правоотношений в цифровом пространстве.

1. Правовые основы защиты персональных данных в Республике Узбекистан

Нормативно-правовую базу защиты персональных данных в Республике Узбекистан составляет иерархически структурированная система правовых актов различной юридической силы, обеспечивающая комплексное регулирование отношений в сфере обработки и защиты персональной информации. Конституция Республики Узбекистан как основной закон государства закрепляет фундаментальное право каждого гражданина на неприкосновенность частной жизни в статье 31, устанавливая конституционно-правовые основы защиты персональных данных и создавая правовой фундамент для развития специализированного законодательства в данной сфере. Данная конституционная норма имеет прямое действие и служит основой для всей системы правового регулирования защиты персональных данных в национальном правопорядке.

Ключевым специализированным нормативным актом в исследуемой сфере является Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года № ЗРУ-547, который определяет основополагающие принципы обработки персональных данных, устанавливает правовой статус субъектов персональных данных и операторов, закрепляет систему требований к обеспечению защиты персональных данных и механизмы правовой ответственности за нарушение установленных требований. Данный закон создает комплексную правовую основу для регулирования отношений в сфере обработки персональных данных и их защиты в цифровой среде, устанавливая баланс между необходимостью использования персональных данных для развития цифровой экономики и обеспечением защиты прав и свобод граждан.

Существенное значение в системе правового регулирования имеет Закон Республики Узбекистан «Об информатизации», который регулирует отношения в сфере создания, обработки, передачи и использования информационных ресурсов, включая персональные данные, в информационных системах различного назначения. Этот правовой акт устанавливает общие принципы информационной безопасности, определяет требования к защите информации в информационных системах и создает правовую основу для применения технических средств защиты информации. Дополнительное правовое регулирование осуществляется через систему подзаконных нормативных актов, включая постановления Кабинета Министров Республики Узбекистан, которые конкретизируют порядок применения норм о защите персональных данных в различных сферах экономической и социальной деятельности.

2. Специальные способы защиты персональных данных в интернет-среде

2.1 Технические меры защиты

Действующее законодательство Республики Узбекистан устанавливает императивные требования к обязательному применению специализированных технических средств защиты информации при осуществлении любых операций по обработке персональных данных в информационных системах, подключенных к сети Интернет или функционирующих в цифровой среде. Система технических мер защиты основывается на применении современных криптографических методов, средств контроля доступа и технологий обеспечения целостности данных, что соответствует международным стандартам информационной безопасности и учитывает специфику национальной системы технического регулирования в сфере защиты информации.

Криптографическая защита персональных данных представляет собой фундаментальный элемент системы технических мер безопасности, предусматривающий обязательное применение сертифицированных средств криптографической защиты информации при передаче персональных данных по открытым каналам связи, включая сеть Интернет, а также при их долгосрочном хранении в информационных системах различного назначения. Правовое регулирование использования криптографических средств осуществляется в соответствии с требованиями национального законодательства о технических средствах защиты информации и предусматривает применение только тех криптографических алгоритмов и программно-технических решений, которые прошли процедуру сертификации в установленном порядке и включены в реестр разрешенных к использованию средств защиты информации.

Системы аутентификации и авторизации пользователей представляют собой комплекс программно-технических средств, обеспечивающих надежную идентификацию лиц, получающих доступ к персональным данным, и контроль полномочий таких лиц в отношении осуществления различных операций с персональными данными. Современные требования информационной безопасности предполагают внедрение многофакторной аутентификации, основанной на использовании нескольких независимых факторов подтверждения подлинности пользователя, включая биометрические данные, криптографические ключи и временные коды подтверждения. Правовое регулирование систем аутентификации учитывает необходимость обеспечения баланса между надежностью защиты и удобством использования информационных систем для законных пользователей.

Средства контроля целостности персональных данных включают в себя технические решения, основанные на использовании электронной цифровой подписи, хеш-функций и других криптографических механизмов, обеспечивающих возможность обнаружения любых несанкционированных изменений в массивах персональных данных. Данные технические средства играют критически важную роль в обеспечении достоверности персональных данных и предотвращении их искажения в результате технических сбоев или преднамеренных противоправных действий. Правовые требования к средствам контроля целостности устанавливаются с учетом категории персональных данных и уровня потенциального ущерба от их искажения или утраты.

2.2 Организационные меры защиты

Система организационных мер защиты персональных данных в интернет-среде представляет собой комплекс управленческих решений, процедур и регламентов, направленных на создание эффективной системы управления информационной безопасностью в организациях, осуществляющих обработку персональных данных. Правовое регулирование организационных мер защиты основывается на принципе персональной ответственности руководителей организаций за обеспечение защиты персональных данных и предусматривает создание специализированных структурных подразделений или назначение ответственных должностных лиц, обладающих необходимыми компетенциями в области информационной безопасности и правового регулирования обработки персональных данных.

Обязательное назначение ответственных должностных лиц за организацию обработки и защиты персональных данных представляет собой ключевой элемент организационной системы защиты, предусматривающий

делегирование конкретным сотрудникам организации полномочий и ответственности за соблюдение требований законодательства о персональных данных. Ответственные лица должны обладать необходимой квалификацией в области информационного права и информационной безопасности, регулярно повышать свою квалификацию и обеспечивать координацию деятельности различных структурных подразделений организации по вопросам защиты персональных данных. Правовой статус ответственных лиц определяется внутренними документами организации с учетом требований действующего законодательства и включает как права по организации системы защиты персональных данных, так и обязанности по обеспечению соблюдения установленных требований.

Разработка и внедрение локальных нормативных актов, регламентирующих порядок обработки и защиты персональных данных, представляет собой обязательное требование действующего законодательства, направленное на создание детализированной правовой основы для деятельности организации в сфере обработки персональных данных. Локальные акты должны учитывать специфику деятельности конкретной организации, особенности используемых информационных технологий и характер обрабатываемых персональных данных, а также содержать детальные процедуры обеспечения защиты персональных данных в интернет-среде. Система локальных актов включает положения о защите персональных данных, должностные инструкции ответственных лиц, регламенты технического обслуживания средств защиты информации и процедуры реагирования на инциденты информационной безопасности.

Организация регулярного обучения и повышения квалификации персонала, имеющего доступ к персональным данным, представляет собой важнейший элемент системы организационных мер защиты, направленный на формирование у сотрудников необходимых знаний и навыков в области защиты персональных данных в цифровой среде. Программы обучения должны включать изучение требований действующего законодательства, особенностей правового регулирования обработки различных категорий персональных данных, современных угроз информационной безопасности в интернет-среде и методов их предотвращения. Эффективность системы обучения обеспечивается через регулярную оценку знаний сотрудников, актуализацию учебных программ с учетом изменений в законодательстве и развития информационных технологий, а также через создание системы мотивации персонала к соблюдению требований информационной безопасности.

2.3 Правовые гарантии защиты

Система правовых гарантий защиты персональных данных в интернет-среде основывается на признании персональных данных объектом особой правовой защиты и закреплении специальных прав субъектов персональных данных, направленных на обеспечение контроля над использованием их персональной информации в цифровом пространстве. Правовые гарантии включают как материально-правовые нормы, определяющие содержание прав субъектов персональных данных и обязанностей операторов, так и процессуальные механизмы реализации и защиты этих прав. Система правовых гарантий строится на основе международно признанных принципов защиты персональных данных, адаптированных к особенностям национального правопорядка и специфике функционирования интернет-среды в Республике Узбекистан.

Институт согласия субъекта персональных данных представляет собой фундаментальную правовую гарантию, предусматривающую обязательность получения предварительного, осознанного и недвусмысленного согласия граждан на обработку их персональных данных в интернет-среде с обязательным указанием конкретных целей обработки, способов использования персональных данных, перечня лиц, которым могут быть переданы персональные данные, и срока их обработки. Согласие должно быть выражено в форме, позволяющей подтвердить факт его получения, и может быть отозвано субъектом персональных данных в любое время без объяснения причин отзыва. Правовое регулирование института согласия учитывает особенности различных способов выражения согласия в цифровой среде и устанавливает повышенные требования к получению согласия на обработку специальных категорий персональных данных.

Право субъектов персональных данных на забвение представляет собой современную правовую гарантию, закрепляющую возможность граждан требовать удаления своих персональных данных из интернет-ресурсов и информационных систем при наступлении определенных правовых условий, включая достижение целей обработки, истечение срока хранения персональных данных или отзыв согласия на их обработку. Реализация права на забвение в интернет-среде связана с особыми техническими и правовыми сложностями, обусловленными распределенным характером хранения информации в цифровом пространстве и необходимостью балансирования права на забвение с другими конституционными правами, включая свободу информации и выражения мнений. Правовое регулирование данного инсти-

тута предусматривает установление разумных ограничений права на забвение в случаях, когда сохранение персональных данных необходимо для обеспечения свободы выражения мнений, научных исследований или выполнения правовых обязанностей.

Обязанность операторов персональных данных по уведомлению о нарушениях защиты персональных данных представляет собой важную правовую гарантию, направленную на обеспечение оперативного реагирования на инциденты информационной безопасности и минимизацию потенциального ущерба от несанкционированного доступа к персональным данным. Система уведомлений включает обязательность информирования уполномоченного государственного органа по защите персональных данных о всех случаях нарушения защиты персональных данных в установленные сроки, а также уведомление субъектов персональных данных в случаях, когда нарушение может повлечь высокий риск для их прав и свобод. Правовые требования к процедуре уведомления включают установление минимального содержания уведомления, сроков направления уведомлений и мер по устранению последствий нарушений защиты персональных данных.

3. Особенности защиты персональных данных в различных сферах интернет-деятельности

3.1 Электронная коммерция

Правовое регулирование защиты персональных данных в сфере электронной коммерции характеризуется повышенными требованиями к обеспечению безопасности финансовой информации потребителей и создания доверительной среды для развития цифровой торговли. Операторы интернет-магазинов и других платформ электронной коммерции обрабатывают широкий спектр персональных данных потребителей, включая контактную информацию, данные о платежных картах, адреса доставки товаров, информацию о покупательских предпочтениях и историю совершенных покупок. Специфика правового регулирования в данной сфере обусловлена необходимостью обеспечения баланса между потребностями развития электронной коммерции, требующей активного использования персональных данных для персонализации услуг и повышения качества обслуживания потребителей, и обеспечением надежной защиты персональной информации граждан от несанкционированного использования и мошеннических действий.

Обязанности операторов интернет-магазинов в сфере защиты персональных данных включают обеспечение безопасной передачи платежной информации с использованием сертифицированных криптографических

средств защиты, ограничение доступа к персональным данным клиентов только теми сотрудниками, которые нуждаются в такой информации для выполнения своих трудовых обязанностей, и создание эффективной системы контроля за использованием персональных данных в маркетинговых целях. Особое внимание в правовом регулировании уделяется защите данных о платежных картах, которая должна осуществляться в соответствии с международными стандартами безопасности платежных систем и предусматривать применение технологий токенизации и других современных методов защиты финансовой информации. Операторы электронной коммерции также обязаны обеспечивать прозрачность использования персональных данных клиентов, включая предоставление подробной информации о целях обработки данных, сроках их хранения и правах клиентов в отношении своих персональных данных.

3.2 Социальные сети и мессенджеры

Правовое регулирование защиты персональных данных пользователей социальных сетей и систем мгновенного обмена сообщениями представляет собой одну из наиболее сложных и динамично развивающихся областей информационного права, что обусловлено масштабом обработки персональных данных на таких платформах, интенсивностью их использования гражданами и многообразием форм коммуникации в цифровой среде. Операторы социальных сетей и мессенджеров обрабатывают не только базовую личную информацию пользователей, но также содержание их переписки, данные о социальных связях, информацию о местоположении, поведенческие данные и другие сведения, которые в совокупности создают детальный цифровой профиль личности. Специфика правового регулирования в данной сфере связана с необходимостью обеспечения баланса между свободой коммуникации, развитием социальных взаимодействий в цифровой среде и защитой частной жизни пользователей от вмешательства как со стороны операторов платформ, так и со стороны третьих лиц.

Обязанности операторов социальных сетей и мессенджеров включают обеспечение конфиденциальности электронной переписки пользователей с применением технологий сквозного шифрования, защиту личной информации профилей от несанкционированного доступа и использования, создание эффективных механизмов контроля за распространением персональных данных пользователей третьими лицами без их согласия, а также обеспечение возможности для пользователей осуществлять эффективный контроль над настройками приватности своих аккаунтов. Особое внимание

в правовом регулировании уделяется защите персональных данных несовершеннолетних пользователей, которая предусматривает установление дополнительных ограничений на обработку их персональных данных, усиленные требования к получению согласия законных представителей и создание специальных механизмов модерации контента. Операторы также обязаны обеспечивать прозрачность алгоритмов обработки персональных данных, используемых для персонализации контента и рекламы, и предоставлять пользователям возможность контролировать использование их данных для таких целей.

3.3 Государственные электронные услуги

Правовое регулирование защиты персональных данных при предоставлении государственных и муниципальных услуг в электронном виде характеризуется применением наиболее строгих требований к обеспечению информационной безопасности, что обусловлено особым статусом государственных органов как субъектов, обладающих властными полномочиями, и повышенной степенью доверия граждан к государственным информационным системам. Система электронного правительства в Республике Узбекистан предусматривает обработку широкого спектра персональных данных граждан, включая биометрические данные, сведения о доходах и имуществе, медицинскую информацию, данные о трудовой деятельности и другую конфиденциальную информацию, что требует создания особо надежной системы защиты такой информации. Специфика правового регулирования в данной сфере связана с необходимостью обеспечения высокого уровня доступности государственных услуг для граждан при одновременном соблюдении строжайших требований к защите их персональных данных.

Система защиты персональных данных в сфере электронных государственных услуг основывается на применении национальной системы электронной идентификации граждан, использовании квалифицированной электронной подписи для обеспечения подлинности электронных документов, создании централизованной системы управления доступом к государственным информационным ресурсам и внедрении комплексной системы аудита всех операций с персональными данными граждан. Правовые требования к защите персональных данных в государственных информационных системах включают обязательное применение сертифицированных средств криптографической защиты информации, создание резервных копий персональных данных с обеспечением их защиты на уровне не ниже основных массивов данных, регулярное проведение мероприятий по оценке защищен-

ности информационных систем и обеспечение непрерывности функционирования систем защиты персональных данных. Особое внимание уделяется обеспечению межведомственного взаимодействия при обработке персональных данных граждан, которое должно осуществляться с соблюдением принципа минимизации обрабатываемых данных и исключения их дублирования в различных государственных информационных системах.

4. Ответственность за нарушение требований защиты персональных данных

Система юридической ответственности за нарушение требований законодательства о защите персональных данных в интернет-среде представляет собой комплексный правовой институт, включающий различные виды ответственности в зависимости от характера совершенного правонарушения, степени общественной опасности деяния и размера причиненного ущерба. Правовое регулирование ответственности в данной сфере основывается на принципах неотвратимости наказания, соразмерности санкций тяжести совершенного правонарушения и эффективности правоохранительных механизмов в обеспечении защиты прав граждан на неприкосновенность частной жизни. Система ответственности включает административную, уголовную и гражданско-правовую ответственность, каждая из которых имеет свои особенности применения и направлена на решение специфических задач правовой защиты персональных данных в цифровой среде.

Административная ответственность за нарушение требований законодательства о персональных данных применяется в случаях совершения административных правонарушений, связанных с нарушением установленного порядка сбора, обработки, хранения, использования и распространения персональных данных граждан в интернет-среде. Кодекс Республики Узбекистан об административной ответственности предусматривает специальные составы административных правонарушений в сфере защиты персональных данных, включающие нарушение требований к получению согласия субъектов персональных данных, несоблюдение установленных сроков и порядка уведомления о начале обработки персональных данных, нарушение требований к обеспечению защиты персональных данных при их обработке в информационных системах. Размер административных штрафов дифференцируется в зависимости от субъекта правонарушения и может применяться как к должностным лицам организаций, так и к юридическим лицам в целом, что обеспечивает комплексное воздействие на нарушителей требований законодательства о персональных данных.

Уголовная ответственность за преступления в сфере защиты персональных данных наступает в случаях совершения общественно опасных деяний, причинивших существенный вред правам и интересам граждан, общества или государства. Уголовный кодекс Республики Узбекистан содержит специальные составы преступлений, связанных с неправомерным доступом к персональным данным, их незаконным использованием, распространением или уничтожением, если эти деяния совершены с использованием служебного положения, причинили крупный ущерб или были сопряжены с извлечением незаконной выгоды. Особое внимание в уголовно-правовом регулировании уделяется преступлениям, совершаемым в отношении персональных данных несовершеннолетних, а также деяниям, связанным с использованием персональных данных для совершения других преступлений, включая мошенничество, шантаж или нарушение неприкосновенности частной жизни. Санкции за преступления в сфере защиты персональных данных включают как меры уголовного наказания, так и дополнительные меры в виде конфискации орудий совершения преступления и возмещения причиненного ущерба.

Гражданско-правовая ответственность за нарушение требований защиты персональных данных основывается на общих принципах деликтной ответственности и предусматривает возмещение как материального, так и морального вреда, причиненного неправомерными действиями в отношении персональных данных граждан. Особенностью гражданско-правовой ответственности в данной сфере является презумпция вины причинителя вреда, что означает обязанность лица, осуществляющего обработку персональных данных, доказывать отсутствие своей вины в нарушении требований их защиты. Размер возмещения морального вреда определяется судом с учетом характера причиненного вреда, степени вины нарушителя, а также индивидуальных особенностей потерпевшего и обстоятельств причинения вреда. Гражданско-правовая ответственность может применяться независимо от привлечения нарушителя к административной или уголовной ответственности и направлена на восстановление нарушенных прав граждан и компенсацию причиненного им ущерба.

5. Проблемы правового регулирования и пути их решения

5.1 Существующие проблемы правового регулирования

Современное состояние правового регулирования защиты персональных данных в интернет-среде в Республике Узбекистан, несмотря на значительные достижения в создании комплексной нормативно-правовой базы, характеризуется наличием ряда системных проблем, требующих комплексного научно-обоснованного решения. Одной из ключевых проблем является

недостаточная осведомленность граждан о своих правах в области защиты персональных данных и механизмах их реализации в цифровой среде, что приводит к формированию низкого уровня правовой культуры в сфере информационной безопасности и создает предпосылки для нарушения прав граждан на неприкосновенность частной жизни. Данная проблема усугубляется отсутствием системной образовательной работы по повышению цифровой грамотности населения и недостаточным уровнем правового просвещения граждан в области защиты персональных данных, что требует разработки и реализации специальных государственных программ правового образования в данной сфере.

Существенной проблемой является отставание правового регулирования от темпов развития информационных технологий и появления новых способов обработки персональных данных в интернет-среде, включая технологии искусственного интеллекта, машинного обучения, больших данных и интернета вещей. Динамичный характер развития цифровых технологий создает ситуацию, когда новые способы обработки персональных данных начинают применяться на практике до создания соответствующего правового регулирования, что создает правовые пробелы и неопределенность в вопросах применения существующих норм к новым технологическим решениям. Данная проблема требует разработки гибких механизмов правового регулирования, способных адаптироваться к технологическим изменениям, и создания системы мониторинга развития информационных технологий для своевременного внесения изменений в законодательство о защите персональных данных.

Проблема обеспечения эффективного международного сотрудничества в сфере защиты персональных данных связана с трансграничным характером интернет-пространства и необходимостью гармонизации национального законодательства с международными стандартами защиты персональных данных. Различия в правовых подходах к регулированию защиты персональных данных в различных юрисдикциях создают сложности для операторов, осуществляющих трансграничную обработку персональных данных, и могут приводить к снижению уровня защиты прав граждан при передаче их персональных данных за пределы территории Республики Узбекистан. Решение данной проблемы требует активного участия в международных инициативах по гармонизации правового регулирования защиты персональных данных и заключения двусторонних и многосторонних соглашений о взаимном признании систем защиты персональных данных с зарубежными государствами.

5.2 Направления совершенствования правового регулирования

Совершенствование системы правового регулирования защиты персональных данных в интернет-среде должно осуществляться по нескольким взаимосвязанным направлениям, включающим как развитие нормативно-правовой базы, так и совершенствование механизмов правоприменения и правового просвещения граждан. Приоритетным направлением является усиление образовательной работы среди граждан по вопросам цифровой грамотности и защиты персональных данных, что предполагает разработку и реализацию комплексных программ правового образования, включающих изучение основ информационного права, практических навыков безопасного использования интернет-ресурсов и способов защиты персональных данных в цифровой среде. Данные программы должны быть адаптированы для различных возрастных и социальных групп населения и предусматривать использование современных образовательных технологий, включая онлайн-курсы, интерактивные обучающие платформы и мобильные приложения для повышения правовой грамотности граждан.

Развитие международного сотрудничества в области защиты персональных данных и кибербезопасности представляет собой стратегически важное направление совершенствования правового регулирования, предусматривающее активное участие Республики Узбекистан в международных организациях и инициативах, направленных на гармонизацию подходов к защите персональных данных в глобальном масштабе. Это направление включает заключение международных соглашений о взаимном признании систем защиты персональных данных, участие в разработке международных стандартов информационной безопасности, обмен опытом с зарубежными странами в области правового регулирования и правоприменительной практики в сфере защиты персональных данных. Особое внимание должно уделяться сотрудничеству с международными организациями по борьбе с киберпреступностью и созданию эффективных механизмов международного сотрудничества в расследовании преступлений, связанных с нарушением защиты персональных данных в трансграничном интернет-пространстве.

Регулярное обновление технических требований к защите персональных данных с учетом развития информационных технологий и появления новых угроз информационной безопасности представляет собой необходимое условие поддержания эффективности системы защиты персональных данных в динамично изменяющейся технологической среде. Данное направление предполагает создание постоянно действующей системы мониторинга

развития информационных технологий, оценки новых угроз информационной безопасности и разработки соответствующих изменений в технические требования к защите персональных данных. Система обновления технических требований должна предусматривать регулярные консультации с представителями IT-индустрии, научными организациями и международными экспертами в области информационной безопасности для обеспечения соответствия национальных требований лучшим мировым практикам и современному уровню развития технологий защиты информации.

Совершенствование системы государственного контроля и надзора за соблюдением требований защиты персональных данных должно предусматривать укрепление потенциала уполномоченных государственных органов, включая повышение квалификации их сотрудников, оснащение современными техническими средствами контроля и расширение полномочий по проведению проверок соблюдения требований законодательства о персональных данных. Эффективность системы контроля должна обеспечиваться через создание риск-ориентированного подхода к планированию контрольных мероприятий, внедрение автоматизированных систем мониторинга соблюдения требований защиты персональных данных и развитие сотрудничества с общественными организациями и профессиональными сообществами в области защиты прав граждан в цифровой среде.

Проведенное исследование специальных способов защиты персональных данных в интернет-среде по законодательству Республики Узбекистан позволяет сделать вывод о том, что национальная система правового регулирования в данной сфере представляет собой комплексную и достаточно развитую правовую конструкцию, основанную на современных принципах защиты персональных данных и учитывающую специфику функционирования цифровых технологий. Система специальных способов защиты персональных данных включает взаимосвязанный комплекс правовых, технических и организационных мер, направленных на обеспечение конфиденциальности, целостности и доступности персональной информации граждан в цифровой среде, что соответствует международным стандартам защиты персональных данных и создает надежную основу для развития цифровой экономики при соблюдении прав граждан на неприкосновенность частной жизни. Правовое регулирование защиты персональных данных в Республике Узбекистан характеризуется системным подходом, предусматривающим дифференциацию требований в зависимости от сферы деятельности операторов и категории обрабатываемых персональных данных.

Эффективность национальной системы защиты персональных данных в интернет-среде в значительной степени зависит от качества взаимодействия всех участников правоотношений в данной сфере, включая государственные органы, осуществляющие контроль и надзор за соблюдением требований законодательства, операторов персональных данных, обеспечивающих практическую реализацию мер защиты персональных данных, и самих граждан как субъектов персональных данных, обладающих правами и обязанностями в сфере защиты своей персональной информации. Достижение оптимального баланса между потребностями инновационного развития цифровых технологий, экономической эффективностью использования персональных данных для развития цифровой экономики и обеспечением надежной защиты прав граждан на неприкосновенность частной жизни представляет собой сложную правовую задачу, требующую постоянного совершенствования правового регулирования с учетом динамично изменяющихся технологических и социальных условий функционирования информационного общества.

Перспективы дальнейшего развития законодательства о защите персональных данных в интернет-среде должны учитывать глобальные тенденции цифровизации общественных отношений, включая развитие технологий искусственного интеллекта, интернета вещей, больших данных и других инновационных решений, которые создают новые возможности для использования персональных данных, но одновременно порождают и новые риски для защиты прав граждан. Совершенствование правового регулирования должно осуществляться на основе научно обоснованного подхода, предусматривающего регулярную оценку эффективности действующих правовых норм, анализ международного опыта правового регулирования и активное взаимодействие с заинтересованными сторонами, включая представителей бизнес-сообщества, научных организаций и гражданского общества. Стратегической целью развития национальной системы защиты персональных данных должно стать создание благоприятной правовой среды для инновационного развития цифровых технологий при обеспечении высокого уровня защиты прав и свобод граждан в информационном обществе.

Список использованных источников

1. Конституция Республики Узбекистан от 8 декабря 1992 года (с изменениями и дополнениями по состоянию на 2021 год). – Ташкент: Адолат, 2021. – 84 с.
2. О персональных данных : Закон Республики Узбекистан от 2 июля 2019 г. № ЗРУ-547 // Собрание законодательства Республики Узбекистан. – 2019. – № 27. – Ст. 547.

3. Об информатизации : Закон Республики Узбекистан от 11 декабря 2003 г. № 560-II (в редакции от 29 августа 2019 года) // Ведомости Олий Мажлиса Республики Узбекистан. – 2004. – № 1-2. – Ст. 15.
4. Кодекс Республики Узбекистан об административной ответственности от 22 сентября 1994 года № 2015-XII (в редакции по состоянию на 2024 год) // Ведомости Верховного Совета Республики Узбекистан. – 1995. – № 1. – Ст. 1.
5. Об утверждении Положения о порядке обработки персональных данных : постановление Кабинета Министров Республики Узбекистан от 5 июня 2020 г. № 342 // Собрание постановлений Правительства Республики Узбекистан. – 2020. – № 6. – Ст. 342.
6. О стратегии развития Нового Узбекистана на 2022-2026 годы : Указ Президента Республики Узбекистан от 28 января 2022 г. № УП-60 // Собрание законодательства Республики Узбекистан. – 2022. – № 4. – Ст. 84.
7. О мерах по дальнейшему развитию сферы информационных технологий : Постановление Кабинета Министров Республики Узбекистан от 3 июля 2018 г. № 528 // Собрание постановлений Правительства Республики Узбекистан. – 2018. – № 28. – Ст. 528.
8. Национальная стратегия по развитию системы кибербезопасности Республики Узбекистан на 2022-2025 годы : утв. Указом Президента РУз от 29 июня 2021 г. № УП-6229.