ПРОБЛЕМЫ ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ ЗА УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ЗАРУБЕЖНЫХ ОБЛАЧНЫХ СЕРВИСОВ

Студент ТГЮУ факультета Публичное Право

Турсунов Достон Рустамович

Аннотация. В статье рассматриваются теоретические основы защиты персональных данных при использовании зарубежных облачных сервисов. Основное внимание уделяется природе облачной обработки, распределению контроля между оператором и провайдером, понятию утечки, основаниям юридической ответственности и трудностям установления причинной связи в трансграничной цифровой среде. Обосновывается, что передача данных внешнему поставщику услуг не устраняет ответственности организации, определяющей цели обработки, но требует учитывать самостоятельную роль провайдера и других участников технологической цепочки. Делается вывод о необходимости сочетать правовые, организационные и технические подходы к защите данных.

Ключевые слова: персональные данные, утечка данных, облачные вычисления, трансграничная обработка, оператор, обработчик, информационная безопасность, юридическая ответственность.

ВВЕДЕНИЕ

Цифровизация общественных отношений привела к широкому распространению облачных технологий, при которых организации используют вычислительные ресурсы, программное обеспечение и хранилища данных, предоставляемые внешними поставщиками. Такая модель снижает затраты на техническую инфраструктуру и позволяет гибко масштабировать информационные системы. Вместе с тем она усложняет обеспечение конфиденциальности и безопасности сведений о физических лицах.

При использовании зарубежного облачного сервиса персональные данные могут собираться в одной стране, обрабатываться организацией из другой, а физически храниться на серверах в третьей. В результате привычная связь между местом обработки, субъектом данных и лицом, ответственным за безопасность, становится менее очевидной. При возникновении утечки необходимо определить не только факт нарушения, но и характер обязанностей каждого участника, степень его контроля над риском и возможность предотвратить негативные последствия.

Поэтому исследование данной темы требует не только перечисления правовых норм, но и раскрытия теоретических категорий: облачной обработки, распределённой ответственности, причинной связи, вины и эффективного возмещения вреда. Именно эти категории составляют основу для понимания современных проблем защиты персональных данных.

1. ОБЛАЧНЫЕ ТЕХНОЛОГИИ КАК СРЕДА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Облачные вычисления представляют собой модель предоставления вычислительных ресурсов по сети по мере необходимости. Пользователь получает доступ к инфраструктуре или программным средствам без необходимости самостоятельно приобретать и обслуживать весь комплекс оборудования. В теории информационных систем обычно выделяют три основные модели облачных услуг.

Инфраструктура как услуга (IaaS) предоставляет виртуальные серверы, сети и хранилища. Клиент самостоятельно устанавливает операционные системы, настраивает приложения и во многом отвечает за управление доступом. Платформа как услуга (PaaS) обеспечивает среду для разработки и запуска программ, передавая провайдеру часть задач по управлению системой. Программное обеспечение как услуга (SaaS) предполагает использование готового приложения, в котором значительная часть технических процессов контролируется поставщиком.

Эти модели различаются не только технологически, но и с точки зрения распределения рисков. Чем больше компонентов контролирует провайдер, тем выше его фактическое влияние на безопасность обработки. Однако уровень технического контроля сам по себе не означает автоматического перехода к нему всех юридических обязанностей. Организация, которая определяет цели и способы использования персональных данных, сохраняет ответственность за обоснованность их сбора, объём обработки и выбор поставщика, соответствующего характеру обрабатываемой информации.

Ключевым понятием в облачной среде является модель разделённой ответственности. Она описывает распределение задач по защите между клиентом и провайдером: поставщик обычно отвечает за физическую инфраструктуру, базовые сетевые средства и доступность облачной платформы, тогда как клиент — за настройки доступа, учётные записи, выбор объёма собираемых сведений и правила использования сервиса. Конкретное распределение зависит от вида услуги и условий договора. Такая модель полезна для организации безопасности, но не заменяет правовую оценку действий каждого участника.

2. ПОНЯТИЕ УТЕЧКИ И ОСНОВНЫЕ ПРИНЦИПЫ ЗАЩИТЫ ДАННЫХ

Утечку персональных данных целесообразно рассматривать как нарушение безопасности, которое приводит к несанкционированному доступу к данным, их раскрытию, изменению, утрате или уничтожению. В широком понимании утечка не сводится к внешнему хакерскому нападению. Она может быть следствием ошибочной настройки облачного хранилища, чрезмерно широких прав доступа, потери средств аутентификации, неправильной отправки информации или ненадлежащего контроля со стороны работников и подрядчиков.

Для теоретического анализа важно различать конфиденциальность, целостность и доступность информации. Конфиденциальность означает защиту

данных от доступа неуполномоченных лиц; целостность — сохранение их точности и неизменности без надлежащего основания; доступность — возможность использовать данные и системы тогда, когда это необходимо. Инцидент может затрагивать один или несколько элементов одновременно. Например, раскрытие сведений третьим лицам нарушает конфиденциальность, а уничтожение резервной копии может затронуть доступность и целостность.

Принцип минимизации данных предполагает, что организация собирает и хранит только те сведения, которые необходимы для определённой цели. Ограничение срока хранения сокращает период, в течение которого данные могут подвергаться риску. Контроль доступа, шифрование, резервное копирование, многофакторная аутентификация и регулярная проверка конфигураций уменьшают вероятность инцидента и его последствия. При этом ни одна отдельная мера не обеспечивает абсолютной безопасности: эффективная защита формируется сочетанием технических средств, внутренних процедур, обучения персонала и контроля поставщиков.

Важное значение имеет принцип подотчётности — способность организации показать, что она осознанно управляет рисками обработки. Для облачной модели это означает необходимость оценивать поставщика до заключения договора, понимать, где и кем обрабатываются данные, определять порядок сообщения об инцидентах и сохранять возможность проверять исполнение согласованных мер.

3. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ

Юридическая ответственность за утечку персональных данных выполняет несколько взаимосвязанных функций. Компенсационная функция направлена на возмещение причинённого человеку имущественного и неимущественного вреда. Превентивная функция стимулирует организации заранее инвестировать в безопасность и выстраивать надлежащие процедуры. Карательная функция

выражается в применении предусмотренных законом санкций за нарушение установленных обязанностей. Восстановительная функция связана с прекращением нарушения, устранением его последствий и снижением риска повторного инцидента.

В зависимости от характера нарушения могут рассматриваться гражданско-правовая, административная, уголовная и дисциплинарная формы ответственности. Их назначение различается. Гражданско-правовой механизм ориентирован прежде всего на защиту пострадавшего и возмещение вреда; административная ответственность применяется для обеспечения соблюдения обязательных требований; уголовная ответственность относится к наиболее общественно опасным деяниям при наличии предусмотренных законом признаков; дисциплинарные меры касаются нарушения работником своих трудовых обязанностей.

Для привлечения к ответственности обычно необходимо установить юридически значимые обстоятельства: наличие обязанности, факт её нарушения, вред или иные предусмотренные законом последствия, причинную связь и условия вины. При утечке эти элементы могут быть сложными для доказывания, поскольку технические сведения часто находятся под контролем оператора или облачного провайдера. Сам факт инцидента не всегда доказывает, какое именно лицо допустило нарушение: утечка может произойти вследствие ошибки клиента, недостатка инфраструктуры, действий субподрядчика либо сочетания нескольких причин.

В облачной среде особенно важна причинная связь. Она предполагает установление того, насколько поведение конкретного участника повлияло на возникновение утечки или увеличение причинённого вреда. Если организация оставила хранилище открытым для общего доступа, ответственность может быть связана с ненадлежащей конфигурацией. Если же причиной стала уязвимость управляемой провайдером инфраструктуры, требуется оценить, какие меры поставщик обязан был принять и мог ли он предотвратить инцидент. В сложных

случаях результат определяется совокупностью технической экспертизы, договорных условий и правового статуса участников.

Отдельную проблему составляет доказательственное неравенство. Пострадавший человек, как правило, не имеет доступа к журналам событий, внутренним отчётам и сведениям о действиях администраторов. Организация и провайдер обладают значительно большими техническими возможностями для выяснения причин инцидента. Поэтому теоретически обоснованная система защиты должна обеспечивать своевременное уведомление, сохранение цифровых доказательств и доступ к необходимой информации в пределах закона. Иначе формальное право на защиту может оказаться труднореализуемым.

4. РАСПРЕДЕЛЕНИЕ РОЛЕЙ МЕЖДУ ОПЕРАТОРОМ И ОБЛАЧНЫМ ПРОВАЙДЕРОМ

В отношениях по обработке данных обычно различают организацию, определяющую цели и основные способы обработки, и лицо, которое выполняет операции с данными по её поручению. В европейской терминологии эти роли обозначаются как контролёр и обработчик. Такое разграничение имеет теоретическое значение, поскольку позволяет соотнести юридические обязанности с реальным влиянием на процесс обработки.

Оператор определяет, зачем собираются персональные данные, какие категории сведений необходимы и для каких целей они будут использоваться. Он также выбирает облачного поставщика и устанавливает внутренние правила доступа. Обработчик, в свою очередь, выполняет порученные операции и должен соблюдать согласованные требования безопасности, не выходя за пределы предоставленных полномочий. При этом провайдер может выступать в иной роли в отношении отдельных операций, например когда самостоятельно определяет цели использования технических журналов или учётных данных.

Сложность заключается в том, что облачные услуги часто включают несколько уровней подрядчиков: основной провайдер, региональные компании, службы поддержки, резервного копирования и мониторинга. Чем длиннее такая цепочка, тем труднее определить, кто имел доступ к конкретным данным и какое действие привело к инциденту. Поэтому договорное распределение обязанностей должно сопровождаться прозрачностью цепочки поставщиков, ограничением доступа, правилами привлечения субподрядчиков и обязанностью сотрудничать при расследовании инцидентов.

При этом договор не должен рассматриваться как средство полного освобождения одной стороны от ответственности перед субъектом данных. Условия договора могут распределять обязанности и предусматривать последующее возмещение между компаниями, однако они не всегда способны ограничить права человека, не участвовавшего в заключении такого договора. В теоретическом плане следует различать внутреннее распределение рисков между контрагентами и внешнюю обязанность соблюдать права субъекта данных.

5. ТРАНСГРАНИЧНЫЙ ХАРАКТЕР ОБРАБОТКИ И СРАВНИТЕЛЬНЫЕ ПОДХОДЫ

Использование зарубежных облачных сервисов ставит вопрос о соотношении территориального принципа права и транснационального характера цифровой инфраструктуры. Физическое местонахождение сервера не всегда совпадает с местом нахождения провайдера, пользователя или лица, определяющего цели обработки. Кроме того, на деятельность поставщика могут распространяться требования нескольких государств, в том числе правила доступа государственных органов к информации.

В международной практике существуют разные подходы к решению этой проблемы. Европейская модель уделяет значительное внимание разграничению ролей контролёра и обработчика, договорным гарантиям, оценке трансграничной

передачи и обязанности уведомлять о серьёзных инцидентах. Российский подход традиционно придаёт существенное значение локализации отдельных операций с данными граждан и предусматривает специальные меры ответственности за утечки. В США регулирование складывается из отраслевых федеральных правил и законодательства штатов, а также включает нормы, позволяющие компетентным органам получать определённые данные у провайдеров, подпадающих под юрисдикцию страны.

Сопоставление этих моделей показывает, что ни локализация, ни договорные гарантии, ни технические меры сами по себе не устраняют все риски. Размещение сервера внутри страны не исключает ошибок доступа или действий инсайдеров. В свою очередь, трансграничная передача не обязательно означает снижение уровня защиты, если существует эффективная система контроля, прозрачные обязанности участников и доступные средства правовой защиты. Важнейшим критерием становится не только место хранения данных, но и возможность реально обеспечить соблюдение прав субъекта.

Для Республики Узбекистан развитие трансграничной обработки усиливает значение правовой определённости в отношениях между национальными операторами и зарубежными поставщиками. При этом детальное перечисление законодательных требований не заменяет теоретического решения ключевых вопросов: кто контролирует риск, как устанавливается причина утечки, какие доказательства должны сохраняться и каким образом пострадавший может реализовать право на защиту.

6. ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ЗАЩИТЫ ДАННЫХ В ОБЛАКЕ

Первая проблема связана с несовпадением технического контроля и юридической роли. Провайдер может управлять инфраструктурой, но не определять цели обработки; оператор может не владеть серверами, но выбирать сервис и

задавать правила использования данных. Следовательно, распределение ответственности должно учитывать не только формальные названия сторон, но и реальные функции, полномочия и возможности предотвращения вреда.

Вторая проблема — ограниченная прозрачность облачной среды. Пользователь обычно не знает точного расположения всех копий данных, состава субподрядчиков и внутренних процедур реагирования. Недостаток информации затрудняет оценку риска до заключения договора и расследование инцидента после его возникновения. Прозрачность здесь выступает не просто условием информированности, а необходимой предпосылкой контроля и доказуемости.

Третья проблема заключается в сложности оценки вреда. Раскрытие персональных данных может привести к финансовым потерям, мошенничеству, нарушению частной жизни, репутационному ущербу или длительному беспокойству человека относительно дальнейшего использования сведений. Не все последствия имеют прямое денежное выражение, а связь между утечкой и конкретным ущербом иногда проявляется спустя значительное время. Это требует гибких подходов к оценке причинности и компенсации.

Четвёртая проблема — различие между формальным соблюдением требований и фактической безопасностью. Организация может иметь необходимые документы и договоры, но при этом использовать слабые настройки доступа или не проверять действия подрядчиков. Эффективность правового регулирования поэтому зависит от того, стимулирует ли оно реальное управление рисками, регулярную проверку мер защиты и своевременное устранение недостатков.

Наконец, трансграничность усложняет практическое исполнение требований. Даже если обязанность провайдера сформулирована ясно, её реализация может зависеть от юрисдикции, наличия представительства, доступности доказательств и возможности исполнить судебное или административное решение. По этой причине

правовая защита должна проектироваться с учётом не только содержания нормы, но и механизмов её практического применения.

ЗАКЛЮЧЕНИЕ

Облачные технологии изменили традиционную организацию обработки персональных данных: сведения могут одновременно находиться под техническим контролем нескольких организаций и подпадать под действие разных правопорядков. Это усложняет определение субъекта ответственности и установление причин утечки, однако не отменяет обязанности участников обеспечивать надлежащую защиту данных.

Теоретическое рассмотрение темы позволяет выделить несколько ключевых положений. Во-первых, ответственность должна соотноситься с фактическими функциями и возможностью каждого участника управлять риском. Во-вторых, договорная модель разделённой ответственности не подменяет правовые обязанности перед субъектом данных. В-третьих, эффективная защита требует доступности информации об инциденте, сохранения цифровых доказательств и справедливого распределения доказательственной нагрузки. В-четвёртых, безопасность определяется сочетанием правовых, организационных и технических механизмов, а не одним лишь местом хранения информации.

Таким образом, развитие регулирования трансграничной обработки целесообразно рассматривать через общие принципы подотчётности, соразмерности, прозрачности и эффективного возмещения вреда. Такой теоретический подход позволяет оценивать законодательные решения не только по объёму формальных требований, но и по тому, насколько они обеспечивают реальную защиту прав человека в цифровой среде.

СПИСОК ЛИТЕРАТУРЫ

1. Закон Республики Узбекистан от 2 июля 2019 г. № ЗРУ-547 «О персональных данных».

2. Закон Республики Узбекистан от 15 апреля 2022 г. № ЗРУ-764 «О кибербезопасности».

3. Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. (Общий регламент по защите данных, GDPR).

4. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

5. Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 2018.

6. Judgment of the Court of Justice of the European Union of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18.

7. ISO/IEC 27001. Information security management systems — Requirements.

8. ISO/IEC 27701. Security techniques — Privacy information management.